

zborník

BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2025

Miháliková, Ťažká (zost.)



PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

-
- Visegrad Fund
- •

zborník

Bratislavské právnické fórum 2025

zborník príspevkov z medzinárodnej vedeckej konferencie,
ktorá sa uskutočnila 17. – 19. septembra 2025
na Právnickej fakulte Univerzity Komenského v Bratislave



PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

2025

Bratislavské právnické fórum 2025 / Monika Miháliková, Veronika Ťažká (zost.).
Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2025. 1649 s. ISBN
978-80-7160-772-4.

© Autori

Zostavovatelia: Monika Miháliková, Veronika Ťažká
Návrh obálky: Libuša Nicholson, Jozef Andraško

Všetky príspevky prešli dvojíťm anonymným recenzným konaním.

1. vydanie
Právnická fakulta Univerzity Komenského v Bratislave
2025

ISBN (e-verzia) 978-80-7160-772-4
ISSN 2989-4808



Publikácia je šírená pod licenciou Creative Commons 4.0, Attribution-NonCommercial-NoDerivatives. Dielo je možné opakovanie používať za predpokladu uvedenie mena autorov a len na nekomerčné účely, pričom nie je možné z diela ani jeho jednotlivých častí vyhotoviť odvodené dielo formou spracovania alebo iných zmien.

Obsah

Sekcia teórie práva a filozofie práva, ústavného práva a medzinárodného práva a medzinárodných vzťahov

The Right to Free Speech and the Challenge of Disinformation in a Digital World.. 15

David Schultz

Digitálna suverenita a moderný národný štát: Znovuzískanie kontroly v digitálnom veku 29

Ewa Milczarek

Violence against women and girls in the digital age and Organisation of American States.....40

Edyta Lis

Cybersecurity in the Energy Sector and the Role of the European Union..... 52

Marek Janček

Ústavněprávní aspekty ochrany člověka v elektronickém uživatelském prostoru ... 73

Karel Klíma

New technologies and responsibility for their use in armed conflict 87

Ľudmila Elbert

Právna pomoc vo svete halucinácií..... 100

Boris Balog

Nové výzvy inštitútu zodpovednosti za škodu spôsobenú porušením práva Európskej únie 114

Miroslav Slašťan, Miloš Levrinc

Štát, spoločnosť, kyberpriestor: návrat do minulosti? 126

Branislav Fábry

Náhrada škody za porušenie GDPR – právna úprava medzinárodnej právomoci .. 140

Katarína Burdová

Ochrana práv detí v digitálnom svete 155

Lilla Garayová

International Legal Regulation of Remote Sensing of the Earth from Space and Its Application for Environmental Protection..... 169

Liudmyla Golovko

Vojnová propaganda: jej zákaz v medzinárodnom práve a jeho implementácia v slovenskom právnom poriadku 179

Lukáš Mareček

Limity digitalizácie v kontexte základného práva používať hotovosť	200
Vincent Bujňák	
Je spotrebiteľ ešte slobodný vo svojom rozhodovaní? Právne dôsledky digitálneho ovplyvňovania	213
Lea Mezeiová	
Overenie veku pri pornografii na internete: Argument v prospech verejnej morálky	225
Ján Tomašík	
Balansovanie medzi disciplinárnou zodpovednosťou a nezávislosťou sudcov v kontexte Poľska a Slovenska	237
Ema Mikulová	
Digitálne aktíva v medzinárodnom práve súkromnom.....	252
Dominika Juck	
Kolízne dilemy v digitálnej realite alebo určovanie rozhodného práva pre cezhraničné spory týkajúce sa doménových mien v Metaverze	260
Ema Krkošková	
Medzi formálnymi požiadavkami a skutočnou vykonateľnosťou: analýza nedostatkov Nariadenia o digitálnych službách v slovenskom právnom prostredí	274
Marián Ruňanin, Igor Sloboda	
Ochrana ústavnosti volieb v ére kybernetických hrozieb	291
Peter Matuška	
Zodpovednosť štátu za volebnú legislatívu v kontexte digitálnych hrozieb	308
Branislav Korec	
Zodpovednosť štátu za bezpečnosť v kybernetickom priestore a limity jeho intervenčno-regulačnej právomoci	324
Dávid Židek	
Umelá inteligencia a ľudské práva. Je Európa legislatívne pripravená na technologickú revolúciu?	339
Martin Búran	
Medzinárodnoprávne aspekty využívania technológií pri kontrole a ochrane biodiverzity	353
Petra Paľuchová	

Sekcia správneho práva

Niekoľko úvah o využívaní umelej inteligencie v rozhodovacích procesoch vo verejnej správe 368

Marián Vrabko

Právne aspekty aktov DSA a AIA vo vzťahu k rozhodovaniu vo verejnej správe 378

Anton Martvoň

Administrative and Legal Aspects of the Application of Artificial Intelligence in the Decision-Making Process by Public Authorities In Ukraine 393

Ivan Gabani, Yaroslav Lazur

Inovatívne možnosti využitia umelej inteligencie pri rozhodovaní vo verejnej správe 407

Alan Lengyel

Skúmanie materiálnej stránky priestupku umelou inteligenciou..... 420

Martin Krajčí

Využitie digitalizácie údajov a umelej inteligencie pri ochrane bezpečnostných záujmov štátu 433

Michal Aláč

Výzvy implementácie nástrojov umelej inteligencie vo verejnej správe 443

Stanislava Sopková

Soudní tlumočení a překlad v éře AI: Mezi právem na spravedlivý proces a technologickými možnostmi..... 455

Kamila Balounova

Informačný systém a jeho uplatnenie stavebnými úradmi 467

Viera Jakušová

Automatizovaný systém adresnej energopomoci v Slovenskej republike v kontexte európskeho práva 479

Kristína Slámková

Artificial Intelligence in the Energy Performance Certification of Buildings: Opportunities and Limits of Slovak Public Administration..... 493

Ľudovít Máčaj

Právne aspekty využívania umelej inteligencie pri rozhodovaní vo vodnom hospodárstve 502

Lenka Šutaríková

Kategorizácia podnetov v oblasti životného prostredia pomocou umelej inteligencie
– cesta k efektívnejšiemu rozhodovaniu? 518

Dominika Noskovičová

Možnosti a limity využívania UI pri rozhodovaní o náhrade škody spôsobenej
určenými živočíchmi 531

Viktória Sokolová

Využitie umelej inteligencie pri vybavovaní žiadostí o slobodnom prístupe
k informáciám 544

Lenka Hmírová

Nedostatky digitálnej komunikácie s verejnoprávnym prvkom..... 557

Sandra Konečná

Překážky širšího využití umělé inteligence ve správním rozhodování v České
republice 569

Kateřina Ištaková

Ozbrojený ľud...nie, žandárstvo 583

Tomáš Rulíšek

Sekcia práva informačných technológií a práva duševného vlastníctva

The Risks For Children in the Online Environment and the Role of European
Legislation in their Protection 601

Lucia Rybanová

The Day Political Ads Died: Meta's Ban, EU Regulation and the Lessons from
Romania..... 614

Soňa Juhásová

Rethinking Automated Vehicles Regulation Using the Regulatory Sandbox..... 628

Stela Košťálová

Trestnoprávny presah vybraných zakázaných praktík podľa Aktu o umelej inteligencii
..... 639

Marek Kordík, Petra Dražová

Problematika vzdialeného vodiča z pohľadu trestného činu neposkytnutia pomoci
podľa §178 TZ Slovenskej republiky 652

Zoltán Gyurász

Implementačné výzvy Cyber Resilience Act: 5 dimenzií implementácie..... 661

Miroslav Sorkovský

CRA: Kybernetická bezpečnosť smart hodínok a ochrana detí	675
Silvia Kratochvilová	
Kybernetická bezpečnosť ako nový rozmer súkromnoprávnej zodpovednosti členov orgánov obchodných spoločností.....	689
Dominika Pintérová	
Bezpečnosť obchodného tajomstva v digitálnom prostredí	706
Radka Kopčová	
Zdravotníctvo 2.0: Keď inteligentné hodinky monitorujú a zákon mlčí	720
Soňa Sopúchová	
Vývoj a najnovšie trendy pri aplikácii aktu DSA v pomeroch kolaboratívneho hospodárstva s ohľadom na zodpovednosť platforiem.....	734
Lukáš Macko	
From Content Moderation to User Rights: New Perspectives on Digital Regulation	747
Jana Zigo	
Predmety duševného vlastníctva ako predmet záložného práva - financovanie zabezpečené duševným vlastníctvom.....	761
Albert Priehoda	
Securing Democracy: The Role of EU Cybersecurity Law in Promoting Democratic Sustainability	774
Matúš Mesarčík	
Next-Generation Cybercrime: Artificial Intelligence, Deepfakes, and Financial Fraud	787
Matej Smalik	
Sekcia občianskeho práva	
Právny status umelej inteligencie.....	801
Martin Križan, Svetlana Ficová	
Umelá inteligencia a výzvy zmluvného práva v digitálnej ére: Analýza legislatívneho rámca Slovenskej republiky.....	815
Martina Babušíková	
Dokazovanie v ére digitálnej ilúzie	829
Lucia Mertl	
AI a hypertrofia obsahu podaní v civilnom procese: dôsledky pre princíp procesnej ekonómie a hospodárnosti konania	840
Sandra Meňhartová	

Právo dieťaťa na súkromie a digitálny dohľad rodičov	850
	Lenka Dufalová
Digitálny obsah a jeho právna povaha v občianskoprávných vzťahoch. Komparatívna analýza právnej úpravy Slovenska a Poľska	867
	Karin Raková, Ewa Lewandowska
Artificial Intelligence, Real Problems: Consumer Remedies for Non-conformity ..	881
	Tjaša Kalin
Logické usudzovanie a umelá inteligencia v práve	892
	Marek Čiernik
The Use of Artificial Intelligence in Consumer Trade - an Optimal Model of Legal Regulations	904
	Peter Lewandowski
Využitie digitálnych technológií pri výkone rozhodnutia vo veciach maloletých: pomocné nástroje alebo hrozby pre najlepší záujem dieťaťa?	915
	Tamara Čipková, Romana Smyčková
Zrušenie rozhodcovského rozsudku – niekoľko úvah o (ne)dostatočnosti platnej právnej úpravy	927
	Radoslav Hnilica
Najlepší záujem dieťaťa a umelá inteligencia: Kam môže viesť optimalizácia v rodinnom práve?	940
	Petronela Luprichová Cvengrošová
Sekcia finančného práva	
Daňové exekučné konanie v podmienkach digitalizácie: perspektívy do budúcnosti	950
	Tímea Jančiová
Miestne dane a poplatky na Slovensku – aktuálne trendy	964
	Erika Neubauerová, Tomáš Černěňko
Fiškálna decentralizácia na Slovensku – dopady zmeny financovania materských škôl na rozpočty miestnych samospráv	977
	Tomáš Černěňko, Erika Neubauerová
Daň z finančných transakcií – Danový nexus	988
	Toško Beran
ViDA – DPH v digitálnom veku	1001
	Aneta Kollman Steinhübllová

Finančné právo v digitálnom veku: Ako regulátori čelia nárastu online podvodov	1014
	Peter Beňo
Digitalizácia a datafikácia vykazovania informácií o udržateľnosti	1035
	Katarína Poliaková
Transparentnosť alebo nadbytočné dátové stopy v kyberpriestore v kontexte kryptoaktív.....	1049
	Klaudia Keratová
Digitalizácia v prostredí Crowdfundingu	1063
	Matej Krkoška
Elektronická fakturácia v oblasti DPH z pohľadu orgánov verejnej moci	1073
	Filip Richter
MiCA vs. PSD2: regulačný prienik a aplikačné problémy.....	1084
	Mária Potančoková
Prienik digitalizácie a kybernetickej bezpečnosti v regulačnom sandbuxe	1094
	Dávid Kis
Proč krajská samospráva stále pokulháva? Zhodnocení středoevropské zkušenosti se zaměřením na konkurenceschopnost	1109
	Petr Konečný
Výzvy v daňovom práve v súvislosti s digitalizáciou (fokus na výmenu informácií)	1122
	Andrea Szakács

Sekcia obchodného práva a hospodárskeho práva

Manipulatívne praktiky obchodníkov v digitálnom prostredí – právna kvalifikácia tzv. <i>dark patterns</i>	1133
	Regina Šťastová
Zakladanie spoločností v Európskej únii: aktuálny stav, limity harmonizácie a perspektíva 28. režimu	1152
	Barbora Grambličková
Legal Challenges of Using AI in Business: Liability and Regulation	1175
	Jana Pezlar Selecká
Umelá inteligencia, smart kontrakty a ich vplyv na fiduciárne povinnosti konateľa	1187
	Peter Šikulínek

Etické otázky v používaní AI pri obchodných činnostiach.....	1201
	Andrej Oriňak
Digitalizácia v oblasti insolvenčného práva	1213
	Aneta Kšenzighová
Digitalizácia insolvenčného konania prostredníctvom Insolvenčného registra ...	1229
	Martin Spišák
Práva podnikateľa v postavení predávajúceho vo vzťahu ke škodě spôsobené informáci poskytnutou chatovacím robotom kupujúciemu při nákupe zboží online	1242
	Pavla Tloušťová
AI v službách štatutárneho orgánu: digitálny asistent pre rozhodovanie	1253
	Richard Laura
IT governance: monetizácia údajov a jej výzvy při riadení obchodných spoločností	1266
	Ľubica Kubíková

Sekcia pracovného práva a práva sociálneho zabezpečenia

Analýza rodových a etnických nerovností v algoritmickom náborovom procese na Slovensku.....	1281
	Juraj Hamulák
AI - nástroj nerovnosti alebo garant inklúzie?.....	1296
	Marcel Dolobáč
Neutralita algoritmov a rovnosť príležitostí.....	1308
	Denisa Rudžiková
Algoritmická diskriminácia a rovnaké zaobchádzanie na digitálnom trhu práce: Výzvy a príležitosti pre ženy v zraniteľných situáciách.....	1318
	Barbara Faktor Pavlíková
Digitálna dôstojnosť alebo digitálna diskriminácia v pracovnom práve.....	1337
	Mária Nováková
Rovnaké zaobchádzanie v kontexte virtualizácie miesta výkonu práce.....	1358
	Pavol Rak
Kontrola dodržiavania zásady rovnakého zaobchádzania inšpektorátmi práce v Slovenskej republike.....	1369
	Marián Lizanec

Spravedlivé odměňování (nejen) v digitálním věku z pohledu české legislativy a judikatury 1379

Jakub Morávek

Rodový rozmer skončenia ekonomickej činnosti a jeho reflexia v systéme sociálneho poistenia 1397

Ján Matlák, Silvia Treľová

Právo na odpojenie – ochrana zamestnanca pred digitálnym vyhorením 1413

Lenka Freel, Soňa Kašická

Human enhancement, Robotics and AI: the consequences for the labour market 1426

Massimiliano Delfino

The right to reasonable accommodation in digital environment.....1440

Silvia Capíková

Erotic Labour in the Platform Economy: Challenges of Implementing the EU Directive on Improving Working Conditions in Platform Work in Slovakia.....1468

Juraj Plaza

Sekcia rímskeho práva, kánonického, cirkevného práva a právnych dejín a právnej komparatistiky

Vplyv ústavných zmien na hierarchiu právnych noriem (1939 – 1992) 1479

Terézia Švedová

Pár poznámok k prameňom historického a pozitívneho kánonického práva.....1494

Vojtech Vladár

Je goldplating škodlivý? 1509

Martin Šimkovič

Sekcia cudzojazyčnej právnej komunikácie

Využitie digitálnych nástrojov pri rešerši cudzojazyčnej právnej terminológie. Ako môžu pomôcť právne texty 1523

Jarmila Pátková

Možnosti a limity strojových prekladačov na báze umelej inteligencie pri preklade právnej terminológie 1538

Alexandra Debnárová

Use Of ChatGPT In Teaching and Learning Legal English – Friend or Foe? 1554

Lucia Smolková

AI podporené prístupy k učeniu sa anglického jazyka pre špecifické účely: zameranie na právnu terminológiu 1568

Iva Dudášová

Úradný prekladateľ v digitálnom prostredí: medzi tradíciou a inováciou 1579

Sandra Banková, Sylvia Mičíková

Digitálne technológie vo výučbe právneho prekladu: výzvy a príležitosti 1591

Sylvia Mičíková, Sandra Banková

Umelá inteligencia vo výučbe anglickej právnej terminológie: prínosy a limity ... 1610

Jarmila Brtková

K problematike kolokačného potenciálu vybraných inštitútov dedičského práva v slovenských a anglických judikátoch z oblasti dedičského práva 1624

Andrea Demovičová

Následné dedenie podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z r. 1900 (historická právno lingvistická analýza) 1638

Peter Gergel

**Sekcia teórie práva a filozofie práva, ústavného
práva a medzinárodného práva
a medzinárodných vzťahov**

Zodpovednosť v práve a v spoločnosti –
medzinárodné, ústavné a teoretické aspekty
v dobe kybernetických hrozieb a digitalizácie

Sekcia je súčasťou plnenia úloh projektu VEGA č. 1/0579/23 – Právne
a etické aspekty disciplinárnej zodpovednosti v právnom štáte

THE RIGHT TO FREE SPEECH AND THE CHALLENGE OF DISINFORMATION IN A DIGITAL WORLD

David Schultz¹

Abstract: Among the most important human rights in a democratic society is the right to free speech. But there are several historic problems when it comes to protecting free speech, such as defining what constitutes speech and under what circumstances, how, and by whom it may be expressed. In the last two decades new problems have emerged when it comes to protecting free speech. These include the proliferation of disinformation, propaganda, and hate speech on the Internet/social media, and the rise of artificial intelligence in its ability to rapidly produce deep fakes and other false information. This use of free speech to spread false information had also grown as part of hybrid warfare strategies taking place in cyberspace. This Article examines the new threats to free speech in the new digital world. The Article lays out the historic case for free expression, a summary of the current state of the law in selected countries, and then it provides examples of how the spread of disinformation is currently practiced and the threat its pose to democracy and national security.

Key words: Free speech; Constitutional Law; Disinformation; Artificial Intelligence; Cyber-Space.

Introduction

Among the most important and basic human rights in a democratic society is the right to free speech.² Free speech is critical for the circulation of information, enabling people to gather what they need to make informed choices. It also supports expression, self-development, and civic life in general.³

¹ Hamline University, Saint Paul, Minnesota USA.

² Post, Robert. "Participatory democracy and free speech." *Va. L. Rev.* 97 (2011): 477; Mill, J. S. (1859). *On liberty*. London, England: John W. Parker and Son. ISBN: 978-0486421308; Schauer, F. (1982). *Free speech: A philosophical enquiry*. Cambridge, England: Cambridge University Press. ISBN: 978-0521273831.

³ Steven H. Shiffrin, *The First Amendment, Democracy, and Romance* (Harvard University Press, 1990); C. Edwin Baker, *Human Liberty and Freedom of Speech* (Oxford University Press, 1989); Thomas I. Emerson, *The System of Freedom of Expression* (Random House, 1970); Jürgen Habermas, *Between Facts and Norms* (Polity Press, 1996); Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, 2012).

Yet there is a contrary problem: the same channels that distribute truth can also carry disinformation and falsehood.⁴ As the often-paraphrased battlefield maxim reminds us, truth may be the first casualty of conflict, even as information remains essential to both self-government and security.

Information is vital for democratic accountability. However, the very openness that makes speech valuable also enables propaganda, hate speech, and deception to circulate. The rise of the internet and social media scaled these dynamics beyond anything seen before. Artificial intelligence now accelerates the capacity to produce deepfakes and other false content rapidly and at low cost.⁵ This article briefly lays out the historical case for free expression, summarizes selected freed speech case law, and then examines how digital platforms and AI complicate traditional speech doctrines.

The Historical Case for Free Expression

The rise of free speech as a principle is often traced to Europe from the 15th through 18th centuries. There are at least two sources of this commitment to free speech. The first grows out of the Enlightenment and the rebirth of scientific learning where as Immanuel Kant once expressed the sentiment of questioning with the phrase „Sapere Dare,“ or „Dare to know.“⁶

The second was when religious wars pitted sects against one another.⁷ Competing faiths each claimed orthodoxy and sought to suppress rival interpretations. That violence generated a practical argument for toleration and open discourse. John Milton’s *Areopagitica* offered a powerful early defense of unlicensed printing and argued that censorship corrupts both truth and the censors themselves.⁸ If certain materials are corrupting, Milton asked, who guards those who must read them to ban them.

John Locke’s *A Letter Concerning Toleration* urged respect for disagreement in matters of belief, contending that no authority can claim certainty in interpreting

⁴ Gielow Jacobs, L. (2022). Freedom of speech and regulation of fake news. *The American Journal of Comparative Law*, 70(Supplement_1), i278-i311; Goldman, A. I., & Baker, D. (2019). Free speech, fake news, and democracy. *First Amend. L. Rev.*, 18, 66.

⁵ Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2022). Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. *British Journal of Management*, 33(3), 1238-1253; Benzie, A., & Montasari, R. (2022). Artificial intelligence and the spread of mis- and disinformation. In *Artificial intelligence and national security* (pp. 1-18). Cham: Springer International Publishing.

⁶ Peterson, J. (2008). Enlightenment and freedom. *Journal of the History of Philosophy*, 46(2), 223-244.

⁷ Jacob Mchangama, *Free Speech: A History from Socrates to Social Media*. New York: Basic Books, 2022. ISBN 9781541600492, pp. 93-117.

⁸ John Milton, *Areopagitica*, In *Areopagitica and Other Political Writings*, Indianapolis, Indiana: Liberty Fund, 1999, pp. 11-12.

scripture.⁹ Locke argued that the authority of a religious sect should extend no further than its own membership. In *Two Treatises of Government*, Locke argued that government is an artificial creation grounded in a social contract, and the people retain the right to criticize it—and ultimately to dissolve it—when it fails to secure basic rights and liberties.

By the 18th and 19th centuries, the defense of expression shifted from theology toward limited government, constitutionalism, and individual rights. John Stuart Mill's *On Liberty* tied free speech to democracy, self-development, and the search for truth.¹⁰ Mill argued that even false opinions test dogma and sharpen understanding by forcing orthodoxies to justify themselves. Suppressing dissent, he warned, deprives society of the "collision of adverse opinions" necessary for knowledge.

By the 20th century, especially in the United States, the case for free speech rested on the libertarian "marketplace of ideas" metaphor.¹¹ Quoting Justice Oliver Wendall Holmes, Jr:

Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition. To allow opposition by speech seems to indicate that you think the speech impotent, as when a man says that he has squared the circle, or that you do not care whole heartedly for the result, or that you doubt either your power or your premises. But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.¹²

Let a diversity of views compete, trusting that engagement and the competition of ideas reveals the better argument over time.

The important point to understand here is that the historic origins of the concept of free speech date back nearly 500 years. The constitutional and legal doctrines were developed in what we can call a „horse and buggy“ era. It was a time before the rise of newspapers or the press as we know it. It occurred before any forms of mass

⁹ John Locke, *A Letter Concerning Toleration*, Indianapolis, Indiana: Bobbs-Merrill, 1979, pp. 9-11.

¹⁰ Generally, see chapter II of *On Liberty* for a development of these arguments.

¹¹ Blasi, V. (2004). Holmes and the Marketplace of Ideas. *The Supreme Court Review*, 2004, 1-46; Volokh, E. (2011). In defense of the marketplace of ideas/search for truth as a theory of free speech protection. *Va. L. Rev.*, 97, 595.

¹² *Abrams v. United States*, 250 U.S. 616, 630 (1919).

communication and it was developed when the concept of sovereignty was thought of in physical geographic ways. While falsehoods and political propaganda have always been features of society, the issue will be to what extent the framework of law developed decades if not hundreds of years ago is still viable or able to address the needs and challenges of democracy today.

In effect, it was a framework built for pamphlets and public squares now struggles with algorithmic amplification and AI-generated content.

Core Democratic Functions of Speech

The historic importance of free speech rests on several grounds. First, it enables political criticism and accountability, allowing citizens to question leaders and policies.¹³ Second, it promotes a robust exchange of ideas that supports truth-seeking and scientific progress. Third, it protects self-expression and personal growth, offering space for identity, belief, and conscience. Together these values frame speech as both instrumental to democracy and intrinsic to human dignity.¹⁴

These justifications do not guarantee that all speech is beneficial. They do, however, ground a strong presumption against censorship and in favor of counterspeech, debate, and transparency. The challenge arises in recognizing when certain speech crosses lines that justify regulation without undermining the broader project of democratic freedom. That balance—between liberty and other goods—sits at the heart of modern doctrine.

International and Comparative Legal Protections

In the United States, the First Amendment declares that „Congress shall make no law abridging freedom of speech or of the press.“ That provision, adopted in 1791, has inspired broader global understandings of expression.

Article 19 of the Universal Declaration of Human Rights states: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

¹³ *Handyside v. United Kingdom*, App. No. 5493/72, 1 E.H.R.R. 737 (Eur. Ct. H.R. 1976); *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

¹⁴ *Schmidberger v. Austria*, Case C-112/00, 2003 E.C.R. I-5659 (European Court of Justice 2003); *Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn*, Case C-36/02, 2004 E.C.R. I-9609 (European Court of Justice 2004); *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (South Africa v. Israel)*, Order on Provisional Measures, 2024 I.C.J. __ (Jan. 26, 2024).

Article 10 of The European Convention on Human Rights similarly states: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

Article II of The Charter of Fundamental Rights of the European Union echoes these protections, declaring: „Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

National constitutions often combine strong protections with specified grounds for limitation. Article 26 of the Constitution of Slovakia guarantees

(1) Freedom of expression and the right to information shall be guaranteed. (2) Everyone has the right to express his or her opinion in words, writing, print, images or by other means and also to seek, receive and disseminate ideas and information freely, regardless of the state borders . No approval process shall be required for press publishing.

This Article goes on to state that a right to freedom of expression and information, prohibits censorship, and allows restrictions by law only when necessary to protect rights and freedoms of others, national security, public order, or health and morals.

Finally, Article 34 of Ukraine's Constitution pronounces:

Everyone is guaranteed the right to freedom of thought and speech, and to the free expression of his or her views and beliefs. Everyone has the right to freely collect, store, use and disseminate information by oral, written or other means of their choice.

The point in citing to these various documents is simply to demonstrate the proposition that at least in theory if not formal constitutional thought, free speech is considered an important constitutional right in a democracy.¹⁵ This divergence illustrates that free speech is a shared value but not a uniform one.

Legal Limits and the Problem of Line-Drawing

Different jurisdictions draw lines differently. In the United States, doctrines distinguish between advocacy and incitement, protect most political speech, and permit content-neutral time, place, and manner rules. Courts scrutinize prior

¹⁵ PL. ÚS 26/2019, Constitutional Court of the Slovak Republic, preliminary decision (Dec. 2019) and merit judgment (May 2021) (Slovak); II. ÚS 307/2014, Constitutional Court of the Slovak Republic, decision of Dec. 18, 2014 (Slovak); Constitutional Court of Ukraine. (2016, June 1). *Decision No. 2-rp/2016 in the case on the constitutionality of the third sentence of Article 13(1) of the Law "On Psychiatric Care" (judicial control over hospitalisation of incapacitated persons)*. *Visnyk of the Constitutional Court of Ukraine*, 2016(6), 60–67.

restraints and viewpoint discrimination, while recognizing categories with lowered protection, such as true threats or obscenity. The underlying theme is that public debate should be open and robust, especially on matters of public concern.

In Europe, the right to expression is similarly fundamental but expressly balanced against other interests “necessary in a democratic society.” National systems more commonly penalize certain forms of hate speech or Holocaust denial than the United States. Many European courts weigh expression against dignity and equality concerns, reflecting a different constitutional history and risk assessment. These differences show that while free speech is a shared value, its application reflects culture, history, and institutional design.

Slovakia’s constitutional framework illustrates the pattern of strong protection with tailored limits. It guarantees freedom of expression and information, prohibits censorship, and permits restrictions only when necessary to protect others’ rights, security, public order, or health and morals. Ukraine recognizes the right to collect, store, use, and disseminate information and guarantees free expression of thought and belief. Such texts underscore the recognition that vibrant speech is a democratic necessity, even while states reserve tools to address concrete harms.

Even robust speech regimes recognize limits. As U.S. Justice Oliver Wendell Holmes Jr. famously suggested, no one has a right to falsely shout fire in a crowded theater. Courts around the world wrestle with similar boundary questions. Where is the line between protected advocacy and unlawful incitement or true threats.¹⁶ How much protection, if any, should hate speech receive.¹⁷ What separates pornography, which might be protected, from obscenity, which may not be.¹⁸ These questions test the contours of a right that is powerful but not absolute.

Another recurring question concerns who holds speech rights. Most would argue citizens do, but what about visitors, residents without legal status,¹⁹ or transnational

¹⁶ *Walendy v. Germany*, App. No. 21128/92, Eur. Ct. H.R. (1995); *Honsik v. Austria*, App. No. 25062/94, Eur. Ct. H.R. (1995); *Marais v. France*, App. No. 31159/96, Eur. Ct. H.R. (1996); **Chyba! Len hlavný dokument.** *Brandenburg v. Ohio*, 395 U.S. 444 (1969); **Chyba! Len hlavný dokument.** *Virginia v. Black*, 538 U.S. 343 (2003).

¹⁷ *Gündüz v. Turkey*, App. No. 35071/97, 2003-XI Eur. Ct. H.R. 243.

¹⁸ *Mueller and Others v. Switzerland*, App. No. 10737/84, 13 Eur. H.R. Rep. 212 (Eur. Ct. H.R. 1988); *Otto-Preminger-Institut v. Austria*, App. No. 13470/87, 19 Eur. H.R. Rep. 34 (Eur. Ct. H.R. 1994); *Wingrove v. United Kingdom*, App. No. 17419/90, 24 Eur. H.R. Rep. 1 (Eur. Ct. H.R. 1996); **Chyba! Len hlavný dokument.** *Miller v. California*, 413 U.S. 15 (1973).

¹⁹ *Bridges v. Wixon*, 326 U.S. 135 (1945); *Reno v. American-Arab Anti-Discrimination Committee*, 525 U.S. 471 (1999); *Piermont v. France*, App. No. 15773/89 & 15774/89 (ECtHR, 1995).

actors. Corporations,²⁰ political parties,²¹ and labor unions²² likewise raise complex questions about the scope of expression and campaign activity. Democracies frequently rely on time, place, and manner regulations to manage speech in shared spaces,²³ allowing, for example, protest on public streets while restricting disruptive speech in nonpublic forums.²⁴ The goal is to accommodate expression while protecting competing rights and functions of public life.

Anti-discrimination law adds further complexity. In the US speech cannot be proscribed, but discriminatory conduct may be limited or punished.²⁵ When does speech contribute to subordination or create a hostile environment inconsistent with equal citizenship.²⁶ National security concerns also complicate matters, especially for disclosures of state secrets or sensitive operational information.²⁷ Democratic systems have long struggled to balance these imperatives. As difficult as those balances have been in the past, the digital revolution introduces new challenges that test whether older doctrines remain fit for purpose.

The Digital Age: Scale, Speed, and Manipulation

Traditional doctrines emerged before the internet, social media, and AI. The digital environment places vast amounts of information at people's fingertips and allows speakers to reach global audiences instantly. Social media has become a primary source of news and commentary for many.²⁸ While the internet enables extraordinary circulation of truthful information, it also provides unmatched tools for spreading disinformation, mobilizing harassment, and manipulating public discourse.²⁹ The same networks that power democratic engagement can be used to undermine it.

²⁰ *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010); *Autronic AG v. Switzerland*, App. No. 12726/87 (ECtHR, 1990).

²¹ *California Democratic Party v. Jones*, 530 U.S. 567 (2000); *United Communist Party of Turkey and Others v. Turkey*, App. No. 19392/92 (ECtHR, 1998).

²² *Thomas v. Collins*, 323 U.S. 516 (1945); *Demir and Baykara v. Turkey*, App. No. 34503/97 (ECtHR, 2008).

²³ *Ward v. Rock Against Racism*, 491 U.S. 781 (1989).

²⁴ *Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37 (1983); **Chyba! Len hlavný dokument.** *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939).

²⁵ *Wisconsin v. Mitchell*, 508 U.S. 476 (1993).

²⁶ *Vejdeland v. Sweden*, App. No. 1813/07 (ECtHR, 2012).

²⁷ *Leroy v. France*, App. No. 36109/03 (ECtHR, 2008).

²⁸ Hermida, A. (2016). Social media and the news. *The SAGE handbook of digital journalism*, 1, 81-94.

²⁹ Hilary, I. O., & Dumebi, O. O. (2021). Social media as a tool for misinformation and disinformation management. *Linguistics and Culture Review*, 5(S1), 496-505.

Studies and platform transparency reports repeatedly note that falsehoods often travel faster and farther online than truth.³⁰ Algorithmic systems, optimized for engagement, may amplify sensational, polarizing, or emotionally charged content.³¹ Bots and inauthentic accounts scale these dynamics by simulating consensus or injecting coordinated narratives.³² Anonymous and pseudonymous actors can operate from anywhere, complicating attribution and accountability.³³ Meanwhile, governments increasingly assert “cyber sovereignty,” seeking to control online spaces, mandate content restrictions, or wall off national networks.³⁴

The cross-border nature of the internet facilitates foreign influence operations and information warfare.³⁵ Disinformation can erode trust in institutions, depress turnout, or inflame social divisions. The same tools can be used in wartime to confuse adversaries, disrupt logistics, or shape international opinion. In a borderless digital sphere, propaganda becomes a powerful instrument in both peace and war, and liberal democracies must protect open discourse without surrendering it to manipulation.

Platform Power and Private Governance

A handful of corporations control core infrastructures of contemporary speech, including social-media platforms, app stores, mobile operating systems, search, and cloud services.³⁶ These firms’ choices about moderation, algorithmic ranking, and access can shape public discourse more than many public laws. The decision to downrank or remove content, disable ad monetization, or suspend accounts can have

³⁰ Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *science*, 359(6380), 1146-1151.

³¹ Shah, F. (2025). ALGORITHMIC BIAS AND POLITICAL POLARIZATION: CHALLENGES FOR DEMOCRACY. *Global Media and Social Sciences Research Journal*, 6(1), 24-35.

³² Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2022). Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. *British Journal of Management*, 33(3), 1238-1253.

³³ Soares, H. (2022, April). The spread of fake news by social bots: Perspectives on social bot regulation. In *International Conference on Autonomous Systems and the Law* (pp. 189-204). Cham: Springer International Publishing.

³⁴ Deibert, R. J. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In *Routledge handbook of Internet politics* (pp. 323-336). Routledge.

³⁵ Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: cyber subversion, information operations and ‘deep fakes’. *Australian Journal of International Affairs*, 74(4), 439-454; Topor, L., & Tabachnik, A. (2021). Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies*, 12(1), 112-127; Lanoszka, A. (2019). Disinformation in international politics. *European journal of international security*, 4(2), 227-248.

³⁶ Suraj Khanal, Why and How Is the Power of Big Tech Increasing in the Policy Landscape? *Policy and Society* 44, no. 1 (2025): 52–67, <https://doi.org/10.1093/polsoc/puafo22> ; Umut Aytac, Ergin Bulut, and Todd Makse, What Is the Point of Social Media? Corporate Purpose and Political Participation, *Frontiers in Political Science* 7 (2025): Article 1330349, <https://doi.org/10.3389/fpos.2025.1330349>.

dramatic political effects. The opacity of some systems—combined with the speed of enforcement—fuels public suspicion even when intentions are benign.

The concentration of private power also intersects with geopolitics. Decisions about satellite internet access in conflict zones,³⁷ throttling platform reach, or restructuring moderation teams can change on-the-ground realities for activists, journalists, and governments. This raises difficult questions: how should constitutional values apply in privately owned public squares. What due-process norms, transparency mechanisms, or appeal rights should be required. The answers will influence whether digital spaces align with democratic commitments to accountability and reason-giving. These private choices, though outside formal constitutional law, increasingly function like quasi-constitutional rulings for public discourse.

AI as a Force Multiplier for Disinformation

Artificial intelligence magnifies the problems of scale and plausibility. Generative models can produce fluent text, persuasive images, and realistic audio or video with minimal effort. Deepfakes can place words in a leader’s mouth, fabricate evidence of wrongdoing, or impersonate activists to fracture coalitions. Synthetic personas can run convincing influence campaigns, lacing true facts with strategic falsehoods to evade detection. When combined with micro-targeting, these tools tailor messages to exploit cognitive biases and social fractures.³⁸

Recent cycles illustrate the threat environment. Fabricated videos designed to look like breaking news or official addresses have circulated around elections and conflicts.³⁹ This includes recent or current elections in Romania⁴⁰ and Moldova.⁴¹ False claims amplified by networks of inauthentic accounts have sown confusion after major events, delaying consensus on basic facts. Image-based hoaxes have leveraged the speed of visual virality to outpace corrections. Each of these tactics erodes trust, creating an information fog where citizens struggle to distinguish signal from noise. The danger is not only deception but demobilization, as people disengage when they feel they cannot know what is true.

³⁷ Abels, J. (2024). Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations*, 30(4), 842-866.

³⁸ Nasiri, S., & Hashemzadeh, A. (2025). The Evolution of Disinformation from Fake News Propaganda to AI-driven Narratives as Deepfake. *Journal of Cyberspace Studies*, 9(1), 229-250.

³⁹ Lundberg, E., & Mozelius, P. (2025). The potential effects of deepfakes on news media and entertainment. *AI & SOCIETY*, 40(4), 2159-2170.

⁴⁰ Agata Kleczkowska, *The Russian Disinformation Campaign During the Romanian Presidential Elections: The Perfect Example of a Violation of International Law?* (Opinio Juris, January 27, 2025), <https://opiniojuris.org/2025/01/27/the-russian-disinformation-campaign-during-the-romanian-presidential-elections-the-perfect-example-of-a-violation-of-international-law/>.

⁴¹ *Russian propaganda swamps Moldova ahead of elections*, Euronews (July 25, 2025).

At the same time, AI can help defend the information sphere. Detection systems can flag synthetic media, watermarking can help identify provenance, and content authenticity initiatives can allow verification of legitimate photos and videos. AI can also assist researchers and journalists in tracing networks of coordinated activity. The risk is that defensive tools will lag behind offensive innovation or be unevenly deployed across platforms and languages. Democracies must therefore invest in both technical safeguards and civic resilience.

Policy and Governance Options (Without Abandoning Liberty)

The hardest question is how to respond without compromising the very values free speech protects. Several principles can guide action. First, preserve the presumption for speech and favor counterspeech, transparency, and procedural fairness. Second, tailor interventions to concrete harms—deception in commerce, voter suppression, doxxing, targeted harassment, or true threats—rather than broad viewpoint-based bans. Third, require due-process-like mechanisms in platform governance: clear rules, notice, explanation, and appeal. Fourth, promote media literacy and public-interest journalism so that citizens can better evaluate claims.

Governments can also encourage interoperable transparency: standardized reporting on content moderation, political ads, and coordinated influence operations.⁴² Support for independent researchers to access data—subject to privacy safeguards—can improve shared understanding of what works. Finally, where regulation is necessary, it should be precise, proportionate, and subject to judicial review. The aim is to align incentives toward authenticity and accountability while maintaining generous space for dissent and experimentation.

Conclusion: Protecting Freedom Without Surrendering Truth

The democratic dilemma is stark. Free speech makes self-government possible by enabling criticism, participation, and the pursuit of truth. Yet the same openness can be exploited by bad actors—foreign and domestic—to spread falsehoods, undermine elections, and polarize society. In the digital, AI-driven world, misinformation functions like a new form of aggression that can violate the practical sovereignty of states without crossing a physical border.

The task is to protect and define free speech for new realities without sacrificing democratic values. That requires updated legal doctrines, smarter platform governance, and investment in civic capacity. It also requires humility about what law

⁴² Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of cyber policy*, 5(2), 199-217; Ray, A. (2021). Disinformation, deepfakes and democracies: The need for legislative reform. *The UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL*, 44(3), 983-1013.

alone can do: culture, education, and institutional trust matter. Free speech must remain a shield for liberty, not a sword for dismantling it. Meeting that challenge is among the defining tests of twenty-first-century democracy.

The issue is whether the legal framework developed to support free speech to initially support democracy is still relevant and up to the task for contemporary challenges. The central test is whether democracies can adapt free speech protections to the digital age without hollowing them out in practice.

Bibliography

1. ABELS, J. Private infrastructure in geopolitical: Conflicts The case of Starlink and the war in Ukraine. *European Journal of International Relations*, pp. 842–866.
2. *Abrams v. United States*, 250 U.S. 616, 63 (1919).
3. *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide* (South Africa v. Israel), Order on Provisional Measures, 2024 I.C.J. __ (Jan. 26, 2024).
4. *Autronic AG v. Switzerland*, App. No. 12726/87 (ECtHR, 1990).
5. BAKER, C. Edwin. *Human Liberty and Freedom of Speech*. Oxford: Oxford University Press, 1989. 398 pp. ISBN 978-0195057775.
6. BARAK, Aharon. *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press, 2012. 638 pp. ISBN 978-1107008588.
7. BENZIE, A. *Artificial Intelligence and National Security*. Cham: Springer International Publishing, 2022. 18 pp. ISBN 978-3-031-06708-2.
8. BLASI, V. "Holmes and the marketplace of ideas." *Supreme Court Review*, 1–47 (2004).
9. *Brandenburg v. Ohio*, 395 U.S. 444 (1968).
10. *Bridges v. Wixon*, 326 U.S. 135 (1945).
11. BULUT, Umut Aytac, Ergin, & Todd Makse. What is the point of social media? Corporate purpose and political participation. *Frontiers in Political Science* (2025).
12. *California Democratic Party v. Jones*, 530 U.S. 567 (2000).
13. *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010).
14. DEIBERT, R. J. The geopolitics of internet: Censorship control. In *Routledge Handbook of Internet Politics* (pp. 323–336). New York: Routledge, 2008.
15. *Demir and Baykara v. Turkey*, App. No. 34503/97 (ECtHR, 2008).
16. EMERSON, Thomas I. *The System of Freedom of Expression*. New York: Random House, 1970. 754 pp. ISBN 0394711432.
17. GIELOW, Jacobs, L. Freedom of speech and regulation of fake news. *American Journal of Comparative Law*, 70(Supplement 1), i278–i311 (2022).

18. GOLDMAN, Alvin I., & Daniel Baker. Free speech, fake news, and democracy. *First Amendment Law Review*, 18, 66– (2019).
19. *Gündüz v. Turkey*, App. No. 35071/97, 2003-XI Eur. Ct. H.R. 243.
20. HABERMAS, Jürgen. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge, MA: MIT Press, 1996. 631 pp. ISBN 978-0262082433.
21. *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939).
22. HAJLI, N., Saeed, U., Tajvidi, M., & Shirazi, F. Social bots and the spread of disinformation in social media: The challenges of artificial intelligence. *British Journal of Management*, 33(3), 1238–1253 (2022).
23. *Handyside v. United Kingdom*, App. No. 5493/72, 1 E.H.R.R. 737 (Eur. Ct. H.R. 1976).
24. HERMIDA, Alfred. Social media and the news. In T. Witschge, C. W. Anderson, D. Domingo, & A. Hermida (Eds.), *The SAGE Handbook of Digital Journalism* (pp. 81–94). London/New York: SAGE Publications, 2016. ISBN 978-1473906532.
25. HILARY, I. O., & Dumebi, O. "Social media as a tool for misinformation and disinformation management." *Linguistics and Culture Review*, 5(S1), 496–505 (2021).
26. *Honsik v. Austria*, App. No. 25062/94 (ECtHR).
27. KHANAL, Shaleen, Zhang, Hongzhou, & Taeihagh, Araz. Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, 44(1), 52–69 (2025).
28. KLECZKOWSKA, Agata. The Russian disinformation campaign during the Romanian presidential election: The perfect example of a violation of international law? *Opinio Juris*, January 27, 2025.
29. LANOSZKA, A. Disinformation in international politics. *European Journal of International Security*, 4(2), 227–248 (2019).
30. *Leroy v. France*, App. No. 36109/03 (ECtHR, 2008).
31. LOCKE, John. *A Letter Concerning Toleration*. Indianapolis: Bobbs-Merrill, 1979. ISBN 0-672-60183-4.
32. LUNDBERG, E., & Mozelius, P. The potential effects of deepfakes on news media and entertainment. *AI & Society*, 40, 2159–2170 (2024).
33. *Marais v. France*, App. No. 31159/96 (ECtHR).
34. MCHANGAMA, Jacob. *Free Speech: A History from Socrates to Social Media*. New York: Basic Books, 2022. 528 pp. ISBN 978-1541600492.
35. MILL, J. S. On Liberty. In *On Liberty and Other Writings* (pp. 1–116). New York: Cambridge University Press, 1991. ISBN 0-521-37917-2.
36. MILTON, John. *Areopagitica*. In *Areopagitica and Other Political Writings*. Indianapolis, Indiana: Liberty Fund, 1999. 463 pp. ISBN 0-86597-197-8.

37. *Mueller and Others v. Switzerland*, App. No. 10737/84, 13 Eur. H.R. Rep. 212 (Eur. Ct. H.R. 1988).
38. NASIRI, S., & Hashemzadeh, A. The evolution of disinformation from fake news propaganda to AI-driven narratives as deepfake. *Journal of Cyberspace Studies*, 9(1), 229–250 (2025).
39. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
40. *Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn*, Case C-36/02, 2004 E.C.R. I-9609 (ECJ 2004).
41. *On Psychiatric Care* (judicial control over hospitalisation of incapacitated persons). Constitutional Court of Ukraine. Decision No. 2-rp/2016, June 1, 2016. Visnyk of the Constitutional Court of Ukraine, pp. 60–67.
42. *Otto-Preminger-Institut v. Austria*, App. No. 13470/87, 19 Eur. H.R. Rep. 34 (ECtHR, 1994).
43. PATERSON, T., & Hanley, L. Political warfare in the digital age: Cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs*, 74(4), 439–454 (2020).
44. *Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37 (1983).
45. PETERSON, Jonathan. Enlightenment and freedom. *Journal of the History of Philosophy*, 46(2), 223–244 (2008).
46. *Piermont v. France*, App. No. 15773/89 & 15774/89 (ECtHR, 1995).
47. PL. ÚS 26/2019, Constitutional Court of the Slovak Republic, preliminary decision (Dec. 2019) and merit judgment (May 2021); II. ÚS 307/2014, decision of Dec. 18, 2014.
48. POST, Robert. Participatory democracy and free speech. *Virginia Law Review*, 97(3), 477–489 (2011).
49. RAY, Andrew. Disinformation, deepfakes and democracies: The need for legislative reform. *University of New South Wales Law Journal*, 44(3), 983–1013 (2021).
50. *Reno v. American-Arab Anti-Discrimination Committee*, 525 U.S. 471 (1999).
51. Russian propaganda swamps Moldova ahead of elections. *Euronews*, July 25, 2025.
52. SCHAUER, Frederick. *Free Speech: A Philosophical Enquiry*. Cambridge: Cambridge University Press, 1982. 251 pp. ISBN 978-0521243407.
53. *Schmidberger v. Austria*, Case C-112/00, 2003 E.C.R. I-5659 (ECJ 2003).
54. SHAH, F. Algorithmic bias and political polarization: Challenges for democracy. *Global Media and Social Sciences Research Journal*, pp. 24–35 (2025).
55. SHIFFRIN, Steven H. *The First Amendment, Democracy, and Romance*. Cambridge, MA: Harvard University Press, 1990. 285 pp. ISBN 978-0674302754.
56. *Thomas v. Collins*, 323 U.S. 516 (1945).

57. TOPOR, Lev, & Tabachnik, Alexander. Russian cyber information warfare: International distribution and domestic control. *Journal of Advanced Military Studies*, 12(1), 112–127 (2021).
58. *United Communist Party of Turkey and Others v. Turkey*, App. No. 19392/92 (ECtHR, 1998).
59. *Vejdeland v. Sweden*, App. No. 1813/07 (ECtHR, 2012).
60. VOSOUGHI, S., Roy, D., & Aral, S. The spread of true and false news online. *Science*, 359(6380), 1146–1151 (2018).
61. *Walendy v. Germany*, App. No. 21128/92 (ECtHR).
62. *Ward v. Rock Against Racism*, 491 U.S. 781 (1989).
63. WHYTE, C. Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, 5(2), 199–217 (2020).
64. *Wingrove v. United Kingdom*, App. No. 17419/90, 24 Eur. H.R. Rep. 1 (ECtHR, 1996).
65. *Wisconsin v. Mitchell*, 508 U.S. 476 (1993).
66. *Virginia v. Black*, 538 U.S. 343 (2002).

Contact details

David Schultz
dschultz@hamline.edu
Hamline University, Saint Paul, Minnesota USA

DIGITÁLNA SUVERENITA A MODERNÝ NÁRODNÝ ŠTÁT: ZNOVUZÍSKANIE KONTROLY V DIGITÁLNOM VEKU

DIGITAL SOVEREIGNTY AND THE MODERN NATION-STATE: REGAINING CONTROL IN THE DIGITAL AGE

Ewa Milczarek¹

Abstract : As digital technologies permeate every aspect of public and private life, the question of national sovereignty is no longer limited to borders and institutions—it now extends into the digital realm. This article explores how modern nation-states can reclaim control over their digital infrastructure, data governance and informational autonomy. A key focus will be placed on the structural opacity of dominant digital platforms, often operating as “black boxes” with proprietary algorithms and non-transparent decision-making systems that elude public oversight. Furthermore, we will critically examine how the prevailing business model of the attention economy, where user engagement is monetized through surveillance and behavioral targeting, undermines democratic governance and challenges state authority. Through case studies and policy analysis, this article will assess whether and how states can reassert digital sovereignty without retreating into techno-nationalism or compromising fundamental rights. Ultimately, it will address the urgent question: What does meaningful digital sovereignty look like in an age of platform dominance and algorithmic control?

Keywords: Digital Sovereignty, digital constitutionalism, Attention Economy, Surveillance Capitalism, democracy

Introduction

The internet, originally designed as an open and pluralistic space for the exchange of information, has transformed into an ecosystem managed by a complex network of entities, ranging from nation states and global technology corporations to non-governmental organizations and the community. The architecture of digital communication is based on infrastructure that, although technically decentralized, is

¹ University of Szczecin, Faculty of Law and Administration

in practice subject to increasingly strong processes of concentration of influence², node or server operators, and entities financing the development of protocols.

Originally, it was expected that the Internet would be able to resist commodification or colonization by any single government or company³. In practice, however, the development of the digital economy has led to the dominance of a few powerful entities, such as Microsoft, Google, Amazon, and Meta, which have taken control of key segments of the network. Currently, the technical and content layers of the network remain under their control. They impose policies and regulations on their users, often detached from the norms of the offline world, thus creating a kind of legal system⁴. This is a new form of infrastructural power is exercised by digital corporations.

The dominance of private corporations in the digital sphere raises questions about the state's ability to exercise political power independently of other entities, about Foucault's power and knowledge⁵. In this context, the research aim of the article the answer to the research question posed: What does meaningful digital sovereignty look like in an age of platform dominance and algorithmic control?

The article is based on a qualitative analysis of the literature and policy documents, covering both theoretical sources and case studies of selected countries and international organizations. The approach taken is desk research, focusing on a critical reconstruction of the concept of digital sovereignty and on identifying differences in its interpretation in different political and geographical contexts. The scope of the study is exploratory and comparative, allowing for the identification of major trends and models, but does not include a full empirical analysis of all state and corporate practices.

Sovereignty gap

From a technological point of view, the Internet is a precisely defined infrastructure—a network of connected devices, protocols, cables, and code⁶. It should be treated as

² LIVITCKAIA, Kristina – PAPOUTSOGLU, Iordanis – KONSTANTINOS, Iordanis – REVOLIDIS, Ioannis – ELLUL, Joshua – FERREIRA DA SILVA, Catarina – SZEGÖ, Daniel – JOSHI, Amit. Decentralised Social Media, 2023, Retrieved from : <http://dx.doi.org/10.2139/ssrn.4636894> (1.8.2025)

³ GIMMLER Antje. Deliberative Democracy, the Public Sphere and the Internet. In: Philosophy & Social Criticism vol. 27 no. 4 (2001), pp. 21-39, <http://doi/10.1177/019145370102700402>

⁴ MILCZAREK, Ewa. Warunki zastosowania pakietów zero-rating w świetle zasady neutralności sieci. In. Acta Universitatis Lodziensis. Folia Iuridica no. 105 (2024,) pp. 221-231 <https://doi.org/10.18778/0208-6069.105.14>

⁵ FOUCAULT, Michel. Power/Knowledge; Selected Interviews and Other Writings 1972-1977. Pantheon Books: New York, 1980, ISBN 0-394-51357-6, p. 52.

⁶ GEIGER, R. Stuart. Does Habermas Understand the Internet? The Algorithmic Construction of the Blog/Public Sphere. In A Journal of Communication, Culture, and Technology vol 10, no. 1 (2009), p.24

public infrastructure⁷ that enables the existence of various communication spaces, both public and private. The network is used to perform traditional state functions, including public debate, information gathering, public services, as well as consultation, education, and administrative processes, which are increasingly moving into the digital sphere. However, this technology does not function within the borders of a single country, but is a global ecosystem whose structure and rules of operation are shaped by a multitude of entities: state, private, and supranational. Algorithms that manage the organization of digital space are neither neutral nor technically impartial. Contrary to the commonly held assumption that they operate objectively and automatically, these algorithms implement a specific logic of platform owners' interests, subordinated to commercial and strategic goals⁸. By taking control of the flow of information, platforms disrupt traditional mechanisms of communication between the state and its citizens, leading to a weakening of the authority of public institutions. The goal is to expropriate public attention and sell it commercially⁹. Attention becomes a symbolic currency¹⁰. The dominant business model of the attention economy, in which user engagement is monetized through surveillance and behavioral targeting, undermines democratic governance and undermines the authority of the state.

The operation of algorithms and technologies that determine the implementation of these state functions remains largely hidden in the so-called black box. This is a metaphor describing the lack of transparency and comprehensibility of the mechanisms that determine the selection and presentation of content. It refers to a situation in which both users and independent observers do not have access to information about how algorithms work, what data is processed, and what logic guides the decisions made¹¹. We see the input and output data, but we do not know how the algorithm moves from one to the other¹². The literature distinguishes three

⁷ RASMUSSEN, Terje. Internet and the Political Public Sphere. In *Sociology Compass* no 8(12) (2014), p. 1315.

⁸ VAN DIJCK, Jose. *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press: New York, 2013, ISBN 9780199307425 p. 29.

⁹ HOTELLING, Harold. The general welfare in relation to problems of taxation and of railway and utility rates. In *Econometrica* vol. 6 no. 3 (1938), p. 257.

¹⁰ HEITMAYER, Maxi. The Second Wave of Attention Economics. Attention as a Universal Symbolic Currency on Social Media and beyond. In *Interacting with Computers* vol. 37 no. 1 (2025), pp. 18–29, <https://doi.org/10.1093/iwc/iwae035>

¹¹ GRZY, Jarek – ROJSZCZAK, Marcin. Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem. In *Internet Policy Review* vol. 10 no. 2 (2021). <https://doi.org/10.14763/2021.2.1564>

¹² BUNGE, Mario. A General Black Box Theory. In *Philosophy of Science* vol. 30 no. 4 (1963), p.346-358. <https://doi.org/10.1086/287954>

barriers to algorithm transparency¹³: intentional concealment whose objective is the protection of intellectual property; lack of technical literacy on the part of users; intrinsic opacity which arises from the nature of machine learning methods.

These strategic unknowns are a tool that allows technology companies to avoid responsibility for the effects of their systems. It is also part of a communication strategy that allows them to mask the actual decision-making mechanisms behind a veil of supposed technical complexity or inaccessibility of knowledge¹⁴. Furthermore, maintaining such opacity supports the achievement of key corporate goals within the attention economy, all without having to disclose the specific means by which these goals are achieved. In this way, opacity becomes a strategic resource and a form of infrastructural power. As a result, it is difficult to assess the social, political, and economic consequences of current data practices in the public and private sectors¹⁵. Technology creates new hierarchies of power/knowledge between those who possess the economic, political, and intellectual capital needed to design algorithmic models and communities subject to unregulated algorithmic decisions¹⁶.

In view of the growing crisis in online information management and the inadequacy of existing models, there are increasing calls for a new approach to Internet governance. This requires a nuanced understanding of the relationship between the Internet and nation states¹⁷. As Timmers points out, these global threats, ranging from geopolitical tensions, through the expansion of digital technologies and the power of transnational corporations, to cybercrime, pandemics, and the climate crisis, operate beyond national jurisdictions¹⁸. This creates a sovereignty gap—a gap between the formal right to sovereignty and the real possibility of exercising it. In the digital context, this means that states and societies are unable to fully control the

¹³ GRYZ, Jarek – ROJSZCZAK, Marcin. Black box algorithms and the rights of individuals: no easy solution to the “explainability” problem. In Internet Policy Review vol. 10 no. 2 (2021). <https://doi.org/10.14763/2021.2.1564>; BURELL, Jenna. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. In. Big Data & Society vol 3 no 1 (2016). <https://doi.org/10.1177/2053951715622512>

¹⁴ NGUYEN, Dennis – BEIJNON, Bjorn. The data subject and the myth of the ‘black box’ data communication and critical data literacy as a resistant practice to platform exploitation. In. Information, Communication & Society vol. 27 no. 2 (2023), pp. 333–349. <https://doi.org/10.1080/1369118X.2023.2205504>

¹⁵ Ibidem

¹⁶ PŁONOWSKA-ZIAREK, Ewa. Rządy ludzkie czy algorytmiczne. In. Teksty drugie vol 6 (2021), pp. 247–248 <https://doi.org/10.18318/td.2021.6.15>

¹⁷ MUELLER, Milton L. Networks and states: the global politics of Internet governance. The MIT Press: Cambridge 2013, ISBN: 9780262289665. <https://doi.org/10.7551/mitpress/9780262014595.003.0001>

¹⁸ TIMMERS, Paul. Sovereignty in the Digital Age. Introduction to Digital Humanism. WERTHNER, Hannes – GHEZZI, Carlo – KRAMER, Jeff - NIDA-RÜMELIN, Julian – NUSEIBEH, Bashar – PREM, Erich-STANGER, Allison ed. Springer: Cham, Switzerland, 2024, ISBN 978-3-031-45303-8, p. 572, <https://doi.org/10.1007/978-3-031-45304-5>

digital space because the actual power is exercised by transnational technology platforms.

Digital sovereignty

The issue of state sovereignty is complex, multidimensional, and subject to change over time¹⁹. It generally refers to the ability to exercise political power over a specific territory or group of people independently of other entities. However, the development of digital technologies has introduced new dimensions to this category that go beyond traditional territorial and jurisdictional boundaries. Contemporary states are forced to face the question of how to exercise power and control in an environment that operates transnationally and is largely influenced by private actors. Digital sovereignty is a concept that refers to the overall ability of individuals, organizations, and states to exercise control over technological infrastructure, data, and digital systems²⁰. It covers issues such as data ownership (data sovereignty), infrastructure independence (e.g., clouds, servers), control over the flow of information and online communication, and regulatory sovereignty over digital platforms and the digital market. The essence of digital sovereignty assumes the need to control the digital realm at the physical layer (resources, infrastructure, devices), the code layer (standards, rules, design), and the information layer. Control means the ability to influence and limit production (including the extraction and processing of necessary raw materials), design, use, and production of digital technologies²¹.

Significant digital sovereignty in an era where platforms dominate the flow of information and algorithms determine the visibility of content means much more than just “control over one's own data.” Rather, it is a comprehensive set of conditions that allow individuals, organizations, and states to maintain real influence over their presence, functioning, and security in the digital space—without dependence on the arbitrary decisions of private entities. In order to govern, to be

¹⁹ NÚÑEZ, Jorge E. State Sovereignty: Concept and Conceptions. In. *International Journal for the Semiotics of Law* no. 37 (2024), pp. 2131–2150. <https://doi.org/10.1007/s11196-024-10170-y>

²⁰ JAISWAL, Rituka - SCHAATHUN, Hans G. On Human Sovereignty in a Digital Age. In. *Procedia Computer Science* no 254 (2025), pp. 157–163; CELESTE, Eduardo. Digital Sovereignty in the EU: Challenges and Future Perspectives. *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, FABBINI, Federico - CELESTE, Eduardo – QUINN, John. Oxford: Hart, 2021, ISBN 978-1-50994-066-0, pp 211–228; Federal Ministry for Economic Affairs and Energy (BMWi), ‘Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem’ (n 2) 7.

²¹ FALKNER, Gerda - HEIDEBRECHT, Sebastian - OBENDIEK, Anke - SEIDL, Timo. Digital sovereignty - Rhetoric and reality. In *Journal of European Public Policy* vol. 31 no 8 (2024), pp. 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>

sovereign, it is needed to possess knowledge, and in order to possess knowledge, you must first gain access to the information that enables its production—to the black box. Signifies the inextricable link between power and knowledge, where power is not merely repressive but also productive, shaping what is considered knowledge and how it is produced and disseminated²².

The goals that countries pursue through digital sovereignty are vary and depend on the political context. In China's case, policy in this area focuses on strengthening control over information, protecting the political order, and building an internal digital ecosystem independent of the influence of global technology corporations. Algorithms are subordinated to the goals of surveillance, social prevention, and shaping ideologically desirable attitudes among citizens.

The United States sees digital sovereignty primarily as an element of geopolitical and economic competition. The aim is to secure technological dominance, protect the national innovation ecosystem, and control strategic data resources²³. The priority is not so much the direct regulation of the internet in the public interest as maintaining the advantage of global digital platforms in the world economy.

The debate on the achievement and goals of digital sovereignty is reflected in the different political practices of other countries. In India, digital public infrastructure has become a key instrument for building digital sovereignty, not only enabling control over key data resources and digital services, but also serving as a tool for strengthening social inclusion and economic development. In South Africa the strategy focuses on balancing dependence on foreign technology providers with the development of local solutions and policies, which indicates a pragmatic approach to the issue, based on adaptation to global conditions²⁴. These examples show that digital sovereignty goals can serve very different models of government, from authoritarian to neoliberal, which makes the question of how states will use their newly gained control over digital systems crucial. The mere achievement of digital sovereignty by a state is not sufficient for the full realization of public goals, such as improving the quality and functioning of the public sphere, although it remains an absolutely essential condition.

Against this backdrop, a European approach is emerging. In France, the concept of digital sovereignty refers to the classical understanding of sovereignty, linking it to the principles of democracy, the rule of law, and territoriality. This concept was

²² FOUCAULT, Michel. *Power/Knowledge; Selected Interviews and Other Writings 1972-1977*. Pantheon Books: New York, 1980, ISBN 0-394-51357-6, p. 52.

²³ WRANGEL, Claes T. The biopolitics of algorithmic governmentality: How the US military imagines war in the age of neurobiology and artificial intelligence. In. *Security Dialogue* vol. 55 no. 4 (2024), pp. 49–367, <https://doi.org/10.1177/09670106241226622>

²⁴ JIANG, Min. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. In. *Policy & Internet* vol. 16, no. 4 (2025), pp. 1–20.

developed mainly as a response to the perceived dominance of American digital technology providers and the resulting dependence of the French state on foreign entities. In Germany, research on “digital sovereignty” focuses on independent digital infrastructures and the protection of data flows and the ability of individuals to exercise control in the digital sphere²⁵. The European Union defines it as “a capability that Europe must have to make its own choices, based on its own values, respecting its own rules”²⁶.

Fratini et al.²⁷, based on a combination of values and descriptive codes, distinguish three models of digital sovereignty. The rights-based model views digital regulation as a tool for strengthening fundamental rights and democratic principles, emphasizing a balance between the protection of rights and market benefits, and assuming a decisive regulatory approach towards the private sector. The market-oriented model is based on the values of laissez-faire, the priority of economic benefits and competition-driven innovation, and treats state regulation as an obstacle, leading to its minimization or complete avoidance. The centralization model, on the other hand, assumes a restructuring of the digital order based on strongly centralized state control, which in practice means excluding non-state actors from decision-making processes and concentrating full regulatory power in the hands of state institutions. Previous approaches to digital sovereignty show its complexity and the multitude of possible applications, but they do not fully reflect the dynamics of this concept in political practice. Therefore, as Pohle et al.²⁸ point out, the perspective of digital sovereignty must be both relational and historical—it must take into account the relationships between regions of the world, the dynamics between individuals, groups, and institutions, and not just between governments. Digital sovereignty is not a static state, but a dynamic discourse shaped by power struggles involving both state and non-state actors. Digital sovereignty is redefined

²⁵ POHLE, Julia – NANNI, Riccardo – SANTANIELLO, Mauro. Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. In. Policy & Internet vol. 16 no. 4 (2025). pp. 666-671 <https://doi.org/10.1002/poi3.437>

²⁶ VON DER LEYEN, Ursula. State of the Union Address by President von der Leyen. European Commission (2020, September 16). https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (1.8.2025)

²⁷ FRATINI, Samuele - HINE, Emmie - NOVELLI, Claudio, HUW, Roberts – FLORIDI, Luciano. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. In DISO vol 3 no. 59 (2024). <https://doi.org/10.1007/544206-024-00146-7>

²⁸ POHLE, Julia – NANNI, Riccardo – SANTANIELLO, Mauro. Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. In. Policy & Internet vol. 16 no. 4 (2025). pp. 666-671 <https://doi.org/10.1002/poi3.437>

in different political contexts and through numerous conflicts²⁹. As Falkner et al.³⁰ point out, it can be used in politics in different ways depending on the context. In some areas, it only plays a supporting role, while in others it becomes a central element of regulatory strategy. It can serve to build coalitions and strengthen international cooperation, but also to deepen divisions by emphasizing conflicting interests. It can be used both to consolidate and strengthen existing institutional competences and to legitimize actions taken in new areas of regulation that have not previously been covered by the traditional scope of state authority.

Conclusions

The analysis shows that digital sovereignty is not a homogeneous or static construct, but rather a dynamic political discourse shaped by global competition for power and resources. The internet, originally conceived as a decentralized space for the exchange of information, has in practice been subordinated to the logic of concentration of influence, both by transnational technology corporations and by states seeking to strengthen their control over digital infrastructure. This phenomenon leads to the emergence of a sovereignty gap—a gap between the formal right of states to act sovereignly and their real ability to exercise power in the context of a global digital economy and algorithmic control.

Digital sovereignty is therefore becoming one of the key areas of struggle and competition between nation states, corporations, epistemic communities, and social groups³¹, shaping the contemporary constitutional and democratic order and the ability of states to build resilience and independence³². The new asymmetry of power, resulting from the dominance of private entities and algorithmic opacity, forces states to redefine their role as guarantors of civil rights and freedoms³³. In this context, the challenge for the future remains to strike a balance between effective

²⁹ POHLE, Julia. Digital Sovereignty—A New Key Concept of Digital Policy in Germany and Europe. Konrad Adenauer Stiftung, 2020. <https://www.kas.de/en/single-title/-/content/digital-sovereignty> (1.8.2025)

³⁰ FALKNER, Gerda - HEIDEBRECHT, Sebastian - OBENDIEK, Anke - SEIDL, Timo. Digital sovereignty - Rhetoric and reality. In Journal of European Public Policy vol. 31 no 8 (2024), pp. 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>

³¹ SANTANIELLO, Mauro. Attributes of Digital Sovereignty: A Conceptual Framework. In. Geopolitics (2025), pp. 1–22. <https://doi.org/10.1080/14650045.2025.2521548>

³² MISRA, Sanjay - Barik, KOUSIK – KVALVIK, Petter. Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities. In. Procedia Computer Science Vol. 254 (2025), pp. 108-117, <https://doi.org/10.1016/j.procs.2025.02.069>.

³³ FRATINI, Samuele - HINE, Emmie - NOVELLI, Claudio, HUW, Roberts – FLORIDI, Luciano. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. In DISO vol 3 no. 59 (2024). <https://doi.org/10.1007/544206-024-00146-7>

digital regulation, ensuring transparency and accountability, and openness to technological innovation and social change.

Examples of policies in individual countries show that this concept is highly contextual. It can be used both to consolidate power in authoritarian models and to defend fundamental rights and shape a more pluralistic digital order.

It should be emphasized that this analysis is limited. It concerns selected cases and does not cover the full spectrum of practices of states and non-state actors. The topic of digital sovereignty remains a developing issue that requires further empirical research and in-depth theoretical reflection. With the rapid development of technology, changing geopolitical conditions, and the growing role of data in social life, this concept will evolve and its importance for democracy, the state, and the global information order will continue to grow.

Bibliography

1. BUNGE, Mario. A General Black Box Theory. In. *Philosophy of Science* vol. 30 no. 4 (1963), p.346-358. <https://doi.org/10.1086/287954>
2. BURELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. In. *Big Data & Society* vol 3 no 1 (2016). <https://doi.org/10.1177/2053951715622512>
3. CELESTE, Eduardo. Digital Sovereignty in the EU: Challenges and Future Perspectives. *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, FABBRINI, Federico - CELESTE, Eduardo – QUINN, John. Oxford: Hart, 2021, ISBN 978-1-50994-066-0, pp 211–228;
4. FALKNER, Gerda - HEIDEBRECHT, Sebastian - OBENDIEK, Anke - SEIDL, Timo. Digital sovereignty - Rhetoric and reality. In *Journal of European Public Policy* vol. 31 no 8 (2024), pp. 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>
5. Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2) 7.
6. FOUCAULT, Michel. *Power/Knowledge; Selected Interviews and Other Writings 1972-1977*. Pantheon Books: New York, 1980, ISBN 0-394-51357-6, p. 52.
7. FRATINI, Samuele - HINE, Emmie - NOVELLI, Claudio, HUW, Roberts – FLORIDI, Luciano. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. In *DISO* vol 3 no. 59 (2024). <https://doi.org/10.1007/s44206-024-00146-7>
8. GEIGER, R. Stuart. Does Habermas Understand the Internet? The Algorithmic Construction of the Blogosphere/Public Sphere. In *A Journal of Communication, Culture, and Technology* vol 10, no. 1 (2009), p.24

9. GIMMLER Antje. Deliberative Democracy, the Public Sphere and the Internet. In: *Philosophy & Social Criticism* vol. 27 no. 4 (2001), pp. 21-39, <http://doi/10.1177/019145370102700402>
10. GOLDBERGER, Michael H. The attention economy and the Net. In: *First Monday* vol. 2 no 4, (1997) <https://doi.org/10.5210/fm.v2i4.519>
11. GRYZ, Jarek – ROJSZCZAK, Marcin. Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem. In *Internet Policy Review* vol. 10 no. 2 (2021). <https://doi.org/10.14763/2021.2.1564>
12. HEITMAYER, Maxi. The Second Wave of Attention Economics. Attention as a Universal Symbolic Currency on Social Media and beyond. In: *Interacting with Computers* vol. 37 no. 1 (2025), pp. 18–29, <https://doi.org/10.1093/iwc/iwae035>
13. HOTELLING, Harold. The general welfare in relation to problems of taxation and of railway and utility rates. In *Econometrica* vol. 6 no. 3 (1938), p. 257.
14. JAISWAL, Rituka - SCHAATHUN, Hans G. On Human Sovereignty in a Digital Age. In: *Procedia Computer Science* no 254 (2025), pp. 157–163;
15. JIANG, Min. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa. In: *Policy & Internet* vol. 16, no. 4 (2025), pp. 1–20.
16. LIVITCKAIA, Kristina – PAPOUTSOGLU, Iordanis – KONSTANTINOS, Iordanis – REVOLIDIS, Ioannis – ELLUL, Joshua - FERREIRA DA SILVA, Catarina – SZEGÖ, Daniel – JOSHI, Amit. Decentralised Social Media, 2023, Retrieved from : <http://dx.doi.org/10.2139/ssrn.4636894> (1.8.2025)
17. MILCZAREK, Ewa. Warunki zastosowania pakietów zero-rating w świetle zasady neutralności sieci. In: *Acta Universitatis Lodzensis. Folia Iuridica* no. 105 (2024,) pp. 221-231 <https://doi.org/10.18778/0208-6069.105.14>
18. MISRA, Sanjay - Barik, KOUSIK – KVALVIK, Petter. Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities. In: *Procedia Computer Science* Vol. 254 (2025), pp. 108-117, <https://doi.org/10.1016/j.procs.2025.02.069>.
19. MUELLER, Milton L. *Networks and states: the global politics of Internet governance*. The MIT Press: Cambridge 2013, ISBN: 9780262289665. <https://doi.org/10.7551/mitpress/9780262014595.003.0001>
20. NGUYEN, Dennis – BEIJNON, Bjorn. The data subject and the myth of the 'black box' data communication and critical data literacy as a resistant practice to platform exploitation. In: *Information, Communication & Society* vol. 27 no. 2 (2023), pp. 333–349. <https://doi.org/10.1080/1369118X.2023.2205504>
21. NÚÑEZ, Jorge E. State Sovereignty: Concept and Conceptions. In: *International Journal for the Semiotics of Law* no. 37 (2024), pp. 2131–2150. <https://doi.org/10.1007/s11196-024-10170-y>
22. PŁONOWSKA-ZIAREK, Ewa. Rządy ludzkie czy algorytmiczne. In: *Teksty drugie* vol 6 (2021), pp. 247-248 <https://doi.org/10.18318/td.2021.6.15>

23. POHLE, Julia – NANNI, Riccardo – SANTANIELLO, Mauro. Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. In. *Policy & Internet* vol. 16 no. 4 (2025). pp. 666-671 <https://doi.org/10.1002/poi3.437>
24. POHLE, Julia. Digital Sovereignty—A New Key Concept of Digital Policy in Germany and Europe. Konrad Adenauer Stiftung, 2020. <https://www.kas.de/en/single-title/-/content/digital-sovereignty> (1.8.2025)
25. RASMUSSEN, Terje. Internet and the Political Public Sphere. In *Sociology Compass* no 8(12) (2014), p. 1315.
26. RÖSSLER Beate. *Der Wert des Privaten*, Suhrkamp: Frankfurt am Main 2001, ISBN 978-3-518-29130-6, p. 23-24
27. SANTANIELLO, Mauro. Attributes of Digital Sovereignty: A Conceptual Framework. In. *Geopolitics* (2025), pp. 1–22. <https://doi.org/10.1080/14650045.2025.2521548>
28. TIMMERS, Paul. Sovereignty in the Digital Age. Introduction to Digital Humanism. WERTHNER, Hannes – GHEZZI, Carlo – KRAMER, Jeff - NIDA-RÜMELIN, Julian – NUSEIBEH, Bashar – PREM, Erich- STANGER, Allison ed. Springer: Cham, Switzerland, 2024, ISBN 978-3-031-45303-8, p. 572, <https://doi.org/10.1007/978-3-031-45304-5>
29. VAN DIJCK, Jose. *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press: New York, 2013, ISBN 9780199307425 p. 29.
30. VON DER LEYEN, Ursula. State of the Union Address by President von der Leyen. European Commission (2020, September 16). https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 (1.8.2025)
31. WRANGEL, Claes T. The biopolitics of algorithmic governmentality: How the US military imagines war in the age of neurobiology and artificial intelligence. In. *Security Dialogue* vol. 55 no. 4 (2024), pp. 49–367, <https://doi.org/10.1177/09670106241226622>

Contact details

De Ewa Milczarek

Ewa.milczarek@usz.edu.pl

University of Szczecin, Faculty of Law and Administration

VIOLENCE AGAINST WOMEN AND GIRLS IN THE DIGITAL AGE AND ORGANISATION OF AMERICAN STATES¹

Edyta Lis²

Abstract: Online violence against women and girls (VAWG) is a form of gender-based violence (GBV), and like all forms of GBV, it is based on stereotypes and prejudice. Technological advances have also given rise to new forms of cyber VAWG, which also constitute a breach of human rights and fundamental freedoms, posing a serious threat to women's and girls' freedom of expression and right to privacy. For a long time, states and international organisations, including the Organisation of American States (OAS), have concentrated on eliminating or at least mitigating the adverse effects of VAWG online. This paper aims to demonstrate the links between gender and different types of cyberviolence. It indicates that digital technologies are not gender-neutral and that women and girls are more exposed to GBV in cyberspace. Hence, the method of legal analysis is applied to concisely explore the concept of cyberviolence and its basic forms, as well as examining the legal instruments and measures taken by OAS bodies to prevent and combat online VAWG. This article contributes to the discussion on technology-facilitated VAWG within the Inter-American system. It also raises public awareness of the risks that information and communication technologies (ICT) pose to women and girls.

Keywords: cyberviolence; gender-based violence; Organisation of American States, technology; women and girls.

Introduction

GBV is a complex, yet not new, phenomenon. However, thanks to rapid technological progress, this form of violence has also emerged in the digital world and disproportionately affects women and girls. It manifests itself in various ways and hurts women's and girls' public and private lives, including within the family. The statistics are truly alarming. At least one in three women has experienced physical and/or sexual violence at some point in their life. Between 16% and 58% of women

¹ The Polish National Agency for Academic Exchange, Zawacka NAWA Programme – travel offer for 2025–2026, application no. BPS/ZAW/2024/1/00010.

² Maria Curie-Skłodowska University in Lublin, Department of Public International Law, Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland.

and girls have experienced online violence³. It intensified during the COVID-19 pandemic. This paper discusses the various forms of violence against women and girls that occurs online, the measures implemented by the OAS to prevent and combat such violence, and the steps taken to enhance the safety of women and girls. It illustrates the links between gender and different types of cyber violence. It also attempts to show that digital technologies are not gender-neutral, i.e., that women and girls are more vulnerable to their adverse effects because of their gender. Furthermore, they face additional obstacles in cyberspace. This article is divided into eight sections. First, it provides an overview of the definition and forms of cyber VAWG. Then, discusses the instruments adopted in the Inter-American system to combat GBV against women and girls, including the Follow-up Mechanism to the Belém do Pará Convention (MESECVI). Next, it analyses the actions and measures taken by OAS bodies and specialised organisations to prevent and combat online VAWG. Finally, it contains concluding remarks. This article does not refer to the case law of the Inter-American Court of Human Rights (IACtHR)⁴.

The concept and main forms of cyberviolence

So far, the Inter-American human rights system has not adopted a definition of technology-facilitated VAWG (technology-facilitated GBV, online violence, cyberviolence and digital violence)⁵. However, such a definition was developed by a group of experts, according to which it is 'any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms'⁶. Like other forms of GBV, it has originated in misogyny, patriarchy and discrimination, including structural discrimination among others⁷. This kind of violation is partly or wholly committed using ICT such as mobile phones, smartphones, the internet, social media platforms, email, geolocation tracking devices, drones and non-internet-

³ Available at: nwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-infographic-and-recommendations-en.pdf. Accessed: 20.09.2025.

⁴ See e.g., LIS, Edyta: Gender Perspective in the Recent Case Law of the Inter-American Court of Human Rights. In: *International Community Law Review*, vol. 26, no. 6 (2024), pp. 579-635.

⁵ See OAS and Canada: Combating Online Violence Against Women: A Call for Protection. In: *White Papers Series*, no. 7 (2019), p. 7; A/77/302, 18 August 2022, para 7.

⁶ Technology-facilitated Violence Against Women: Towards a Common Definition, Report of the Meeting of the Expert Group, 15-16 November 2022, New York, p. 4.

⁷ A/79/500, 8 October 2024, para 3.

connected recording devices, as well as AI⁸. Basic forms of cyber VAWG include: online harassment, image-based abuse (IBA), including doxxing, sextortion, cyberstalking; deepfake pornography, gender-based hate speech and cyberflashing. The first, involves the use of ICT to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse individuals⁹. IBA is a term used for a diverse abusive behaviour involving non-consensually taken or shared nude or sexual images (revenge pornography)¹⁰. Doxxing is a form of online harassment and contains the non-consensual disclosure of personal information e.g., phone number, home and e-mail address¹¹. The term 'sextortion' is a subset of IBA and has many different definitions. It refers to online blackmail, threats and intimidation made by strangers, or by intimate partners, to extort on victim sharing more nude or sexual images, and/or to pay money, and/or to engage in any unwanted act¹². Cyberstalking is closely related to online harassment and involves using ICT to stalk or harass someone. This behaviour is repetitive, lasts some time and is unwanted, and it can make the victim feel afraid¹³. Deepfake pornography is a form of AI that creates images of someone seemingly saying or doing things they never actually did¹⁴. Although there is no uniform accepted definition of gender-based hate speech in international law, it covers a broad range of hateful expression¹⁵ directed against individual or/and members of minority group¹⁶ based on race, gender, colour, religion, nationality among others¹⁷. The term cyberflashing can be described as the unsolicited and unwanted transmission of sexual images and/or videos via ICT and

⁸ The Digital Dimension of Violence Against Women as Addressed by the Seven Mechanisms of the EDVAW Platform, Thematic Paper adopted by the EDVAW Platform at its 14th Meeting on 17 November 2022, p. 8.

⁹ Available at: <https://sherloc.unodc.org/cld/zh/education/tertiary/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html>. Accessed: 20.09.2025.

¹⁰ HENRY, Nicola — FLYNN, Asher — JOHNSON, Kelly — POWELL, Anastasia — SCOTT, Adrian J.: Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery. London and New York: Routledge, 2021, pp. 4-6.

¹¹ A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), United Nations Office on Drugs and Crime, October 2022, p. 42

¹² SHAPIRO, Lauren R.: Cyberpredators and Their Prey. London, New York: CRC Press, 2022, pp. 273-274.

¹³ See e.g., WILSON, Chanelle — SHERIDAN, Lorraine — GARRATT-REED, David: What is Cyberstalking? A Review of Measurements. In: Journal of Interpersonal Violence, vol. 37, no. 11-12 (2022), pp. NP9763–NP9783.

¹⁴ PASCALE, Emily: Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse. In: Syracuse Law Review, vol. 73 (2023), pp. 337-338.

¹⁵ A/76/258, 30 July 2021, para 69.

¹⁶ POWELL, Anastasia - HENRY, Nicola: Sexual Violence in a Digital Age. London: Palgrave Macmillan, 2017, pp. 167-170.

¹⁷ United Nations Strategy and Plan of Action on Hate Speech, 18 June 2019, p. 2.

could be classified as a form of IBA¹⁸. Grooming is deliberate acts by an adult to approach a minor to initiate a relationship and secure emotional control to facilitate sexual abuse, undertake virtual relationships, obtain child pornography, or engage in the trafficking of minors¹⁹.

Legal Framework

Since its establishment, the OAS has adopted several key legally binding documents that protect women's and girls' rights. These include the American Convention on Human Rights (ACHR) adopted on 22 November 1969²⁰ and the Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women (Convention Belém do Pará - CBP) adopted on 9 June 1994²¹. Article 1 of the ACHR requires State Parties (SP) to respect and guarantee the rights of all persons within their jurisdiction, as set out in the ACHR, regardless of their race, colour, sex, language, or any other characteristics. This list of prohibited grounds of discrimination is not exhaustive. For instance, gender is not expressly mentioned as a reason for discrimination. However, according to the IACtHR's case law, the SP are obliged to eradicate and prevent GBV against women and girls²². The Court emphasised that gender stereotypes can lead to structural discrimination, posing a risk to women and girls' full enjoyment of human rights²³. The CBP is the first international instrument to address combating violations against women and set out a list of women's rights²⁴. Article 1 of the CBP contains definition of violence against women i.e., 'any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere'. However, at the time when the CBP was adopted, the private sphere

¹⁸ BLEAKLEY, Paul – KELLY, Danielle – SHORT, Emma: What's the Harm? Gender and Age Differences in Acceptance of Cyberflashing, Reporting Intentions, and Perceived Prevalence. In: *Current Issues in Criminal Justice*, June 2025, pp. 1-2.

¹⁹ Online Gender-Based Violence Against Women and Girls: Guide of Basic Concepts, Digital Security Tools and Response Strategies, OAS/CITE/CIM/ MESECVI, October 2021, p. 44.

²⁰ OAS Treaty Series No. 36.

²¹ OAS A-61.

²² See e. g., FALCÓN, Julissa Mantill: The Inter-American Human Rights System and Its Impact on the Human Rights of Women: The Issue of Sexual Violence. In: *The Impact of the Inter-American Human Rights System: Transformations on the Ground*. Oxford, New York: Oxford University Press, 2024, pp. 268–284.

²³ See HENNEBEL, Ludovic – HÉLÈNE, Tigroudja: The American Convention on Human Rights: A Commentary. Oxford, New York: Oxford University Press, 2022, pp. 59-67.

²⁴ CARMONA, Encarnación: Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women. In: *Elgar Encyclopedia of Human Rights*. Cheltenham, Northampton: Edward Elgar Publishing, vol. 1 (2022), para 7.

did not envisage the online environment²⁵. Furthermore, in 2004 the MESECVI was created to examine SP implementation of the CBP. The Mechanism consists of four pillars: the Conference of SP, which is composed of competent national authorities; the Committee of Experts, a technical body responsible for preparing analyses on implementation of the CBP; the Technical Secretariat, which deals with administrative and strategic issues; and Civil Society²⁶. Since 2008 the MESECVI issued fourth Hemispheric Report on the Implementation of the CBP and the last concerning access to justice, truth, and reparation in cases of GBV against women and girls²⁷. Regrettably, the Inter-American system has not yet prepared a document dedicated to the protection of children's rights. However, several conventions concerning private international law have been adopted. In the ACHR, there is only one provision, i.e., Article 19, which addresses this issue, stating that children are entitled to protection due to their immaturity. The responsibility for ensuring this protection lies with the child's family, society, and the state²⁸.

Inter-American Commission on Human Rights

According to Articles 53 and 106 of the OAS Charter, the IACHR is main body of the Organisation whose fundamental function is to promote the observance and protection of human rights. Under Articles 34–37 of the ACHR, the IACHR consists of seven members who are elected for four years. The functions of the IACHR are listed in Articles 41–47 and include raising awareness of human rights, conducting research and producing reports, transferring cases to the IACtHR, and reviewing petitions. In order to protect women's rights the IACHR in 1994 created the Office of the Rapporteur on the Rights of Women and is composed of one Commissioner and human rights experts²⁹. The Rapporteur analyses whether OAS member states (MS) comply with obligations set forth in the OAS human rights instruments, address the issues concerning women's rights, participate in preparation of reports on cases involving the rights of women and supports Commission during country visits among others³⁰. In 1998, the IACHR established the Office of the Rapporteur on the Rights of Children to protect and promote the rights of children and adolescents. The Rapporteur advises the IACHR on individual petitions, cases and requests for

²⁵ OAS and Canada: Combating Online Violence, p. 7.

²⁶ Available at: https://belemdopara.org/cim_mesecvi/structure. Accessed: 20.09.2025.

²⁷ OEA/Ser.L/II/7.10, MESECVI/CEVI/doc.290/24.rev1, 24 January 2025.

²⁸ HENNEBEL, Ludovic – HÉLÈNE, Tigroudja: The American Convention, pp. 547–598.

²⁹ DUHAIME, Bernard – TORRADO TAPIAS, Nancy R.: Contributions of the Inter-American Jurisprudence to the Protection of Women's Human Rights. In: Journal of Law and Equality, vol. 20 (2025), pp. 115–116.

³⁰ Available at: <https://www.oas.org/en/iachr/jsForm/?File=/en/IACHR/r/DMujeres/mandato.asp>. Accessed: 20.09.2025.

precautionary and provisional measures relating to these rights³¹. Furthermore, the IACHR produced a report on violence and discrimination against women and girls that addressed the issue of online violence. The report has stated that the use of ICT is extremely dangerous for women and girls. Perpetrators use new technologies to plan sexual assaults and human trafficking, as well as to recruit victims³². ICT also perpetuate gender stereotypes and the subordination of women and girls. The report emphasised that most GBV occurs in private, which is why educating girls on how to use these technologies safely is crucial. In the case of children, it stressed that those belonging to minority groups are particularly vulnerable to such violations³³.

Inter-American Commission of Women

During the Sixth International Conference of American States, a resolution was adopted creating the CIM³⁴. According to Article 1 of the Statute³⁵ and Chapter of XVIII of the Charter of OAS³⁶, it is a specialised organisation. The CIM is composed of 34 Delegates designated by their government of the OAS MS. Under Article 2 of the Statute, the CIM is a forum for discussion and forming policy concerning women rights and gender equality in region and to support MS in implementation of their national and international obligations concerning women's rights. The Commission functions are listed in Article 3, including to support MS, on their request, in the implementation of national and international obligations on women's rights and gender equality, and to advice the OAS in all matters concerning women's rights among others. The CIM made a lot of efforts to established standards of protection of women rights such as: drafting conventions³⁷, adopting Strategic Plan of Action for 1995-2000³⁸. Furthermore, thanks to support from the CIM, the OAS Assembly adopted the Inter-American Program on the Promotion of Women's Human Rights and Gender Equity and Equality (IAP) which brought about significant changes to the way the Commission operates³⁹. Under Article 10 of the CBP, the SP are obliged to

³¹ Available at: <https://www.oas.org/en/iachr/jsForm/?File=/en/iachr/r/DN/default.asp>. Accessed: 20.09.2025.

³² See e.g., OEA/Ser.L/V/II., Doc. 51/23, 16 February 2023, para 109.

³³ OAS/Ser.L/V/II., Doc. 233, 14 November 2019, paras 303-308.

³⁴ BUSTAMANTE, Antonio S. de - MAÚRTUA, Victor M. - BROWN SCOTT, James: The Inter-American Commission of Women. In: Bulletin of the Pan American Union, vol. 63, no. 5 (1929), p. 478.

³⁵ Available at: <https://www.oas.org/en/cim/docs/CIMStatute-2016-EN.pdf>. Accessed: 20.09.2025.

³⁶ OAS Treaty Series, Nos. 1-C and 61.

³⁷ See e.g., the Inter-American Convention on Granting of Political Rights to Women, adopted on 2 May 1948, Colombia, OAS Treaty Series, No. 3; MEYER, Mary, K.: Negotiating International Norms: The Inter-American Commission of Women and the Convention on Violence Against Women. In: Aggressive Behavior, vol. 24 (1998), no. 2, pp. 135-146.

³⁸ Resolution adopted at the fifth plenary session, held on 11 November 1994.

³⁹ AG/RES. 1732 (XXX-O/00), 5 June 2000.

present reports to CIM on implementation measures. Moreover, in line with Article 11 of the CBP, CIM is empowered to request advisory opinions from the IACtHR on interpretation of the Convention. Furthermore, the CIM prepared two documents entitled 'Covid-19 in Women's Lives: Reasons to Recognize Differential Impacts'⁴⁰ and 'Cyber-violence and Cyber-bullying against Women and Girls in the Framework of the Belém Do Pará Convention'. The former addresses the issue of the COVID 19 and online GBV. First of all, the pandemic has revealed that women and girls have more limited access to the ICTs. Secondly, they lack the necessary digital skills⁴¹. Thirdly, various forms of GBV, including domestic violence, have increased. Colombia experienced the most significant rise, with an increase of around 130 per cent, followed by Chile with around 70 per cent⁴². Furthermore, other forms of online GBV also increased such as sextortion, grooming and sexual harassment among others⁴³. Fourthly, online GBV has led to a reduction in digital interactions and self-censorship in anticipation of potential attacks. It violates their human rights, including the freedoms of expression and privacy, as well as the right to digital security⁴⁴. Therefore, the CIM requested the implementation of the three so-called 'S' measures: (i) sensitisation: preventing cyber VAWG and girls by promoting changes in attitudes and social behaviours through training, education, awareness campaigns and community development; (ii) safeguards: establishing safeguards to supervise and maintain responsible internet infrastructure and robust user care practices; (iii) enforcement: enforcing sanctions through laws, regulations, and governance mechanisms. Furthermore, ICT should facilitate the reporting of GBV crimes⁴⁵. The latter tackles online GBV issue from a human rights perspective, among other things⁴⁶. Moreover, in 2022, the CIM adopted Strategic Plan of the CIM 2022-2026⁴⁷, which addresses issues such as gender equality, cybersecurity, online education and online political violence against women, and the Panama Declaration 'Building Bridges for a New Social and Economic Pact Led by Women', emphasises the importance of strengthening legal frameworks to promote the digital inclusion

⁴⁰ CIM, 29 April 2020.

⁴¹ Cyber Security for Women during COVID-19: Experiences, Risk, and Self-care Strategies in the New Normal Digital Era. In: White Paper (March, 2022), pp. 11-13, 18.

⁴² Available at: <https://www.statista.com/statistics/1113975/gender-violence-growth-coronavirus-latin-america/>. Accessed: 20.09. 2025.

⁴³ Cyber Security for Women during COVID-19, pp. 21-23.

⁴⁴ Ibid., p. 15.

⁴⁵ COVID-19 in Women's Lives, pp. 10-11.

⁴⁶ Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará, OEA/CIM, MESECVI y ONU MUJERES, 2022.

⁴⁷ Available at: https://www.oas.org/en/cim/docs/plan_estragico ENG 22-26.pdf, pp. 17-21. Accessed: 20.09. 2025.

of women. It includes closing the gender digital divide, promoting women's access to ICT and digital education, and reducing cyber violence against women⁴⁸.

Inter-American Children's Institute

The Institute was created in 1927 in response of initiative of the Fourth Pan American Child Congress of 1924⁴⁹. According to Article 5 of Statute MS of the OAS are members of the Institute. Under Article 1 of its Statute it is a specialised organisation of the OAS intended to promote the study of motherhood, children, adolescents among others, and to adopt integral protection measures⁵⁰. Its functions are enlisted in Article 3 of the Statute, which are carried by the Institute's bodies: the Directing Council, the Pan American Congress on Child and the Secretariat of the Institute (Article 4). In 2007, the Directing Council approved the establishment of the Inter-American Cooperation Programme for the Prevention and Eradication of the Sexual Exploitation, Trafficking, and Smuggling of Children and Adolescents (ANNAObserva)⁵¹. The programme aims to systematise and disseminate key information on the sexual exploitation, trafficking and smuggling of children and adolescents, with a particular focus on information produced in the region. It also provides tools for addressing these issues, as well as technical assistance and training⁵². As part of the programme, a report was prepared in 2024, containing data on the prevalence of online child sexual exploitation, associated practices, national regulations, the international cooperation of OAS MS and the role of the private sector in preventing and combating such violations⁵³. The Institute has also issued a report on the commercial sexual exploitation of boys and girls through the internet and the measures taken by Latin American states to prevent such violence and protect children and adolescents, including national legislation⁵⁴. Furthermore, as part of the Public Policy Discussions for the Safe Use of the Internet by Children and Adolescents, the Institute first submitted a questionnaire to participating states in 2023 regarding the safe use of the internet by children and adolescents. The outcome of this consultation is the 'Decalogue for the Safe Use of the Internet', divided into two volumes. The first volume contains recommendations aimed at strengthening this area, in addition to other initiatives carried out by the Promotion and Protection

⁴⁸ CIM/DEC. 17 (XXXIX-O/22), 26 May 2022, para 17.

⁴⁹ OEA/Ser.GCP/doc. 3278/00, 9 March 2000, para I.

⁵⁰ CD/RES. 06 (79-04), 25 al 26 de Octubre de 2004; amended by CD-RES 1-2021.

⁵¹ CD/RES 04 (87- R/12), 27 September 2012.

⁵² CD/RES.10 (82-R/07), 27 July 2007.

⁵³ Abordaje de la explotación sexual de niñas, niños y adolescentes en los Estados de la región, 2024.

⁵⁴ Explotación Sexual Comercial de Niños, Niñas y Adolescentes e Internet, Febrero 2011; Regional Report, Guidelines for Empowering and Protecting Child and Adolescent Rights on the Internet in Central America and the Dominican Republic, January 2018.

of Rights in the Virtual Environment Programme. It is aimed at an audience aged 12 and over⁵⁵. Volume two covers topics including state online protection policies and legislation, reporting and addressing mechanisms for cases of inappropriate content, digital education and awareness programmes, prevention initiatives, psychological support, and cooperation with the private sector, among others⁵⁶. Moreover, a document was issued outlining regional consensus on conceptual approaches to issues faced by children and adolescents in the digital environment, along with best practices. It addresses three digital phenomena: grooming, cyberbullying and sexting. It also sets out preventive measures⁵⁷.

Inter-American Committee Against Terrorism

To combat cybercrime, the OAS set up the CICTE. Established after the Second Specialised Conference on Terrorism in Mar del Plata in 1998, and based on a resolution of the OAS General Assembly, CICTE aims to promote collaboration among OAS MS to prevent, combat and eliminate terrorist acts and activities⁵⁸. All OAS MS are part of CICTE, which holds an annual regular session. In 2002, CICTE's implementation body, the Executive Secretariat of the Committee, was established, which is the part of the Secretariat of Multidimensional Security⁵⁹. Moreover, the CICTE Cybersecurity Program (CSP), launched in 2003, aims to support OAS MS in building technical and policy capacities to prevent, combat and recover from cyberattacks, enhance cooperation and information sharing, and improve access to knowledge and information on cyber threats and risks for relevant entities. To date, the CICTE's CSP has helped MS develop eighteen national cybersecurity strategies and publish two regional reports on levels of cybersecurity capacity within the OAS. Furthermore, over 2,000 women have participated in cybersecurity exercises, and more than 20 publications on regional cybersecurity issues have been launched, including those addressing cyber violence against women and girls⁶⁰. These publications were prepared in collaboration with the OAS, CICTE, CIM and MESECVI. It considers the impact of the pandemic on the digital environment and various cyber risks associated with it, paying particular attention to those affecting women and

⁵⁵ Decálogo para el uso responsable y seguro de Internet, Volumen I (2024).

⁵⁶ Ibid., Volumen II (2025).

⁵⁷ Consenso regional sobre enfoques conceptuales y problemáticas, enfoques conceptuales problemáticas y mayores prácticas, Volumen I (2022).

⁵⁸ See e.g., LEONARD, Thomas M. (eds.): Inter-American Committee Against Terrorism (CICTE). In: Encyclopedia of U.S.-Latin American Relations. Los Angeles, London, New Delhi, Singapore, Washington DC: CQ Press, vol. 2 (2012), p. 480.

⁵⁹ Available at: <https://www.oas.org/ext/en/main/oas/our-structure/gs/sms/cicte>. Accessed: 20.09.2025.

⁶⁰ Available at: <https://www.oas.org/ext/en/security/prog-cyber>. Accessed: 20.09.2025.

girls and measures in response to such threats⁶¹. Furthermore, the publication examined online GBV against women and girls which was divided on two sub-publication⁶², such as basic concepts⁶³ and digital security tools and response strategies⁶⁴. Moreover, as a joint effort of the Cybersecurity Section of the OAS and the Gender and Disarmament Programme of the Institute for Disarmament Research (UNIDIR), the CICTE published a report on gender-responsive cybersecurity policy, different types of gender-based cyber threats, and best practices. The report clearly emphasises that cyber violence affects different genders differently. Therefore, it is crucial to consider gender when addressing cyber threats⁶⁵. In 2024, the CSP launched the Women in Cybersecurity Empowerment (WiCE) Network as part of the 'Closing the Gender Gap in the Cybersecurity Agenda of the Americas and the Caribbean' project. The latter project is from 2022 and established the three-year CYNDER initiative, which aims to increase female participation in cybersecurity and promote an understanding of the gender perspective in this field⁶⁶.

Conclusion

At first sight, one could think that rapid digitalisation could provide women and girls with an opportunity to escape prejudice and gender stereotypes. Regrettably, in the vast majority of cases, it has become a weapon against them. Victims of such violations suffer physical, psychological, economic and social harm. They are often stigmatised, humiliated and isolated by society. Therefore, in recent years, the OAS and its MS have taken measures in combating online VAWG. These efforts have intensified significantly since the start of the pandemic. During this period, there has been a substantial increase in online traffic, resulting in a surge in online VAWG. A particular issue has been 'zoombombing', whereby intruders disseminate obscene, pornographic, sexist, racist and homophobic content during video conferences without consent⁶⁷. But, first and foremost, cyber VAWG has become a complex and widespread human rights issue. It violates their right to live free from violence, both

⁶¹ Cyber security for women during COVID-19.

⁶² Online Gender-based Violence Against Women and Girls: Guide of Basic Concepts, Digital Security Tools and Response Strategies.

⁶³ Online Gender-based Violence Against Women and Girls: Guide of Basic Concepts, OAS/CICTE/MESECVI, October 2021.

⁶⁴ Online Gender-based Violence Against Women and Girls: Practical Self-protection Handbook: Digital Security Tools and Response Strategies, OAS/CICTE/MESECVI, October 2021.

⁶⁵ A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation, Washington, DC: Organization of American States; Geneva: UNIDIR, 2025, pp. 17-21.

⁶⁶ Press Releases, E-038/24, 12 June 2024.

⁶⁷ Cyber Security for Women during COVID-19, p. 41.

online and offline, and their right to non-discrimination based on gender⁶⁸. However, such discrimination affects women and girls not equally, because some groups of them are at greater risk, e.g., poor, indigenous, Afro-descendant or LGBTI+. Therefore, the ACHR and the CBP SP are obliged to prevent these violations and adhere to their commitments under the conventions⁶⁹. To sum up, analyses of OAS activities demonstrate the need for closer collaboration among international organisations, the private sector, and society to combat or mitigate the adverse effects of online GBV. National legislation must adapt to evolving cyber threats. It is also crucial to raise public awareness of the risks associated with ICT use, particularly among vulnerable groups. Ultimately, we are our own best defenders against GBV online.

Bibliography (selected)

1. BLEAKLEY, Paul – KELLY, Danielle – SHORT, Emma: What's the Harm? Gender and Age Differences in Acceptance of Cyberflashing, Reporting Intentions, and Perceived Prevalence. In: *Current Issues in Criminal Justice*, June 2025, pp. 1-19.
2. BUSTAMANTE, Antonio S. de - MAÚRTUA, Victor M. - BROWN SCOTT, James: The Inter-American Commission of Women. In: *Bulletin of the Pan American Union*, vol. 63, no. 5 (1929), pp. 478-479.
3. CARMONA, Encarnación: Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women. In: *Elgar Encyclopedia of Human Rights*. Cheltenham, Northampton: Edward Elgar Publishing, vol. 1 (2022). 2348 pp. ISBN 9781789903614.
4. DUHAIME, Bernard – TORRADO TAPIAS, Nancy R.: Contributions of the Inter-American Jurisprudence to the Protection of Women's Human Rights. In: *Journal of Law and Equality*, vol. 20 (2025), pp. 111-144.
5. FALCÓN, Julissa Mantill: The Inter-American Human Rights System and Its Impact on the Human Rights of Women: The Issue of Sexual Violence. In: *The Impact of the Inter-American Human Rights System: Transformations on the Ground*. Oxford, New York: Oxford University Press, 2024. 704 pp. ISBN 9780197744192.
6. HENEBEL, Ludovic – HÉLÈNE, Tigroudja: The American Convention on Human Rights: A Commentary. Oxford, New York: Oxford University Press, 2022, pp. 20-94. 1648 pp. ISBN 9780190222345.
7. HENRY, Nicola – MCGLYNN, Clare – FLYNN, Asher – JOHNSON, Kelly – POWELL, Anastasia – SCOTT, Adrian J.: Image-based Sexual Abuse: A Study on

⁶⁸ Third Hemispheric Report on the Implementation of the Belém do Pará Convention, 2017, para 49.

⁶⁹ Ciberviolencia y ciberacoso, pp. 96, 115-120.

the Causes and Consequences of Non-consensual Nude or Sexual Imagery. London and New York: Routledge, 2021. 200 pp. ISBN 9781351135153.

8. LEONARD, Thomas M. (eds.): Inter-American Committee Against Terrorism (CICTE). In: Encyclopedia of U.S.-Latin American Relations. Los Angeles, London, New Delhi, Singapore, Washington DC: CQ Press, vol. 2 (2012). 1120 pp. ISBN 9780872897625.
9. LIS, Edyta: Gender Perspective in the Recent Case Law of the Inter-American Court of Human Rights. In: International Community Law Review, vol. 26, no. 6 (2024), pp. 579-635.
10. MEYER, Mary, K.: Negotiating International Norms: The Inter-American Commission of Women and the Convention on Violence Against Women. In: Aggressive Behavior, vol. 24 (1998), no. 2, pp. 135-146.
11. SHAPIRO, Lauren R.: Cyberpredators and Their Prey. Boca Raton, London, New York: CRC Press, 2022. 382 pp. ISBN 9781003092292.
12. PASCALE, Emily: Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse. In: Syracuse Law Review, vol. 73 (2023), pp. 335-366.
13. POWELL, Anastasia - HENRY, Nicola: Sexual Violence in a Digital Age. London: Palgrave Macmillan, 2017. 317 pp. ISBN 9781137580474.
14. WILSON, Chanelle – SHERIDAN, Lorraine – GARRATT-REED, David: What is Cyberstalking? A Review of Measurements. In: Journal of Interpersonal Violence, vol. 37, no. 11-12 (2022), pp. NP9763–NP9783.

Contact details

Prof. Edyta Lis, PhD, Dr. Habil. (Professor at UMCS)

edyta.lis@mail.umcs.pl

Maria Curie-Skłodowska University in Lublin

Department of Public International Law

Faculty of Law and Administration

Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland.

CYBERSECURITY IN THE ENERGY SECTOR AND THE ROLE OF THE EUROPEAN UNION

Marek Janček¹

Abstract: The notion of energy security has traditionally been associated with the security of oil and gas supplies exemplified mainly by oil crises of the 1970s. In recent years, however, the cybersecurity dimension of the energy sector has been gaining increasing prominence, particularly within the EU. This growing importance is closely linked to the ongoing energy transition, which aims to ensure clean, homegrown, and secure energy for all Europeans. Put simply, molecules are being replaced by electrons. Yet the shift from centralized fossil-fuel-based systems - such as coal- and gas-fired power plants - to decentralized, digitalized and renewable-driven energy models relying on photovoltaic parks, wind farms and smart grid technologies, creates both opportunities and vulnerabilities. While decentralization can enhance the resilience of energy systems, as demonstrated in Ukraine, it simultaneously opens new avenues for hostile actors to carry out cyberattacks against critical energy infrastructure. Against this background, this paper seeks to examine the role of the EU in addressing cybersecurity threats in the energy sector by analyzing the existing legal frameworks and by proposing further actions to be undertaken by the EU at both the international and European levels to strengthen the security and resilience of critical energy infrastructure.

Key words: Cybersecurity, Energy Transition, Cyberattack, Critical Energy Infrastructure, Energy Security

Introduction

Traditionally, the notion of energy security was associated primarily with the physical security of supplies of key energy sources such as gas or oil. Classic examples of such threats include the oil crisis of the 1970s and, more recently, the 2022 energy crisis following the full-scale invasion of Ukraine by the Russian Federation. Although multiple definitions of energy security exist, the most widely cited remains the one formulated by the International Energy Agency (hereinafter referred to as the "IEA"): *"Energy security means the uninterrupted availability of energy sources at an affordable*

¹ Comenius University in Bratislava, Faculty of Law, Department of International Law and International Relations

price".² This definition emphasizes two core aspects of energy security: availability, meaning whether sufficient volumes of energy can be supplied, and affordability, meaning whether energy prices remain stable and accessible for households and businesses. Even though this definition was originally developed in the 1970s, it continues to be highly relevant today, since it does not specify what has to trigger unavailability or unaffordability.

When considering traditional threats to critical energy infrastructure, one might recall visible images such as the massive gas leak on the surface of the Baltic Sea caused by explosives planted on the Nord Stream pipelines, whereby about 35% of all Russian gas imports to Europe were transported.³ This incident is a typical example of how security threats against energy infrastructure were once understood. A physical kinetic attack or sabotage on a gas or oil pipeline. Yet, such a view has become increasingly narrow in today's digitized world. With the advancing energy transition towards climate neutrality, new vulnerabilities are emerging such as the need for system flexibility, the necessity to ensure diverse and resilient clean energy supply chains or the requirement to foster the climate resilience of energy infrastructure.⁴ Beyond these challenges, however, the currently changing geopolitical landscape has brought another critical dimension to the forefront. The cybersecurity of critical energy infrastructure, with its potential to trigger massive cascading disruptions across multiple sectors and countries in a matter of seconds. Cyberattacks against energy infrastructure are by no means a novel phenomenon. Already in 1982, the Siberian pipeline explosion is believed to be the first cyber incident against energy infrastructure, when malware was introduced into SCADA systems.⁵ Subsequent high-profile cases include the 2010 Stuxnet cyberattack on Iranian nuclear installations, and the large-scale cyberattack on the control system of a power grid, which took place in Ukraine on 23 December 2015, when nearly 225.000 customers endured hours of blackout.⁶

The European Union (hereinafter referred to as the "EU") finds itself particularly exposed to cybersecurity threats in the context of its energy transition towards climate neutrality, requiring electrification and digitalization of energy systems, as

² IEA. *World Energy Outlook 2022* [online] 2022. Retrieved from: <https://www.iea.org/reports/world-energy-outlook-2022> [cited 28/8/2025]

³ BBC. *Nord Stream 1: How Russia is cutting gas supplies to Europe* [online] 2022. Retrieved from: <https://www.bbc.com/news/world-europe-60131520> [cited 28/8/2025]

⁴ IEA. *World Energy Outlook 2022* [online] 2022. Retrieved from: <https://www.iea.org/reports/world-energy-outlook-2022> [cited 28/8/2025]

⁵ ALANAZI M., MAHMOOD A., CHOWDHURY M. *SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues*. Issued in *Computers & Security*, Volume 125, 2023. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S0167404822004205> [cited 28/8/2025]

⁶ COMMISSION STAFF WORKING DOCUMENT Accompanying the document Commission Recommendation on cybersecurity in the energy sector {C(2019) 2400 final}

well as due to rising geopolitical tensions, especially *vis-à-vis* the Russian Federation, which possesses formidable cyber warfare capabilities. As underlined in Eurelectric's report "*A Snapshot of Cybersecurity in the EU*":

*"Cyberattacks are on the rise. In the energy sector, a doubling was observed from 2020 to 2022. Countries in the EU are more frequently becoming the target of these attacks, and the majority of global attacks are currently performed by Russian actors."*⁷

As the numbers indicate, the EU is to a great extent exposed to cybersecurity threats against its energy infrastructure. Given the strategic importance of the energy sector for the EU's economy and society, reinforcing cybersecurity has become an urgent priority.

Against this backdrop, the purpose of this paper is to examine and reflect on the role of the EU in addressing cybersecurity threats in the energy sector, both at the international and European levels. In this regard, the paper is structured into three main chapters. The first chapter explores the broader context in which cybersecurity threats arise. The second analyses the international legal framework relevant for the protection of critical energy infrastructure against cyberattacks. Eventually, the third chapter deals with the EU legal framework designed to mitigate and respond to increasing cybersecurity threats against its energy sector.

For the sake of clarity, this paper limits its scope to the protection of critical energy infrastructure against cyberattacks, leaving aside other sectors of critical infrastructure such as transport, health, banking, drinking water or public administration.⁸ The reason for this particular focus is the fact that the energy sector requires a tailored cyber security approach due to three specific characteristics, namely: a) cascading effects, b) real-time requirements, and c) the need to jointly manage new and old technologies.⁹

An additional unique characteristic of the energy sector is its function as a cornerstone of modern societies and economies, upon which virtually all other sectors depend. The recent blackout in Spain serves as a striking example. It produced cascading effects across other sectors such as transport or health, while

⁷ EURELECTRIC. *A snapshot of Cybersecurity in the EU* [online] 2024. Retrieved from: <https://www.eurelectric.org/publications/eurelectric-short-paper-a-snapshot-of-cybersecurity-in-the-eu/> [cited 29/8/2025]

⁸ Annex I of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

⁹ COMMISSION STAFF WORKING DOCUMENT Accompanying the document Commission Recommendation on cybersecurity in the energy sector {C(2019) 2400 final}

also spreading beyond national borders hitting Portugal and southern France.¹⁰ It is a stark reminder of how deeply our societies are dependent on stable and secure supply of energy. Within the EU, in the context of its endeavour for carbon neutrality and changing geopolitical landscape, the threat of cyberattacks on the energy sector is only about to rise.

Context – Energy Transition and Energy Security

The energy trilemma requires policymaker to strike a balance between three sometimes competing objectives of energy policy: energy security, sustainability, and affordability. The EU's answer to this challenge is clear - an accelerated deployment of renewable energy sources, delivering clean, homegrown, secure, and affordable energy for all Europeans.

In the face of accelerating climate change, or nowadays more often referred to as the climate crisis, the EU has embarked on an ambitious mission to achieve its climate neutrality by 2050 through a number of binding and non-binding commitments. At the international level, the EU has pledged to the goals of the Paris Agreement and actively promotes them particularly under the UNFCCC platform, urging other states to follow suit.¹¹ At the European level, the European Green Deal, unveiled in 2019 by Commission President Ursula von der Leyen, has set the political direction for the Old continent. This was subsequently strengthened by the adoption of the European Climate Law, which enshrines the 2050 neutrality target into legislation and is currently under intense negotiation regarding 2040 greenhouse gas reduction goals.¹²

As part of these commitments, the EU has resolved to phase out fossil fuels and substitute them with clean technologies, most notably wind turbines and solar panels. Since these renewable sources are intermittent and dependent on weather conditions, Europe's transmission and distribution grids require substantial modernization to accommodate fluctuating supply. As a result, the entire energy system is undergoing a profound transformation. Electricity is supposed to no longer flow in a simple one-way direction from a few centralized producers to millions of small consumers. Instead, the rise of prosumers - consumers who also generate

¹⁰ CNN. *Spain says April blackout was caused by grid failures and poor planning, not a cyberattack* [online] 2024. Retrieved from: <https://edition.cnn.com/2025/06/17/europe/spain-april-blackout-not-cyberattack-intl-hnk> [cited 28/8/2025]

¹¹ EEAS. *Call for urgent global action to mitigate climate crisis - the external dimension of the European Green Deal* [online] 2021. Retrieved from: https://www.eeas.europa.eu/eeas/call-urgent-global-action-mitigate-climate-crisis-external-dimension-european-green-deal_en [cited 28/8/2025]

¹² POLITICO. *Vote on 2040 climate target canceled after big EU countries block decision* [online] 2025. Retrieved from: <https://www.politico.eu/article/vote-on-eus-2040-climate-target-canceled-after-biggest-countries-block-decision/> [cited 28/8/2025]

electricity and feed it back into the grid - illustrates the decentralization of the sector.¹³ Similarly, the installation of smart meters enables real-time measurement of electricity use, thereby supporting demand-side response. This allows consumers to shift their energy consumption to off-peak hours, reducing costs while contributing to grid stability.¹⁴ All of this, however, relies heavily on digitalization and the deployment of modern automated systems and smart metres to ensure the smooth functioning of electricity networks. Yet with growing digitalization comes increased vulnerability to cybersecurity incidents, as malicious actors can compromise system operability with far greater efficiency than through conventional means.¹⁵

Whereas the EU has relied (and to a great extent still relies) predominantly on large centralized gas-fired or coal-fired power plants, today's and mainly future's energy mix increasingly includes distributed generation, such as rooftop solar panels, wind farms, and battery storage.¹⁶ Transmission and distribution system operators now depend on modern digital technologies to manage real-time electricity flows across interconnected grids. Simply put, the integration of variable renewable energy sources requires smart and digitalized electricity grids. However, these same technologies are more exposed to malicious interference. Common threats include ransomware, phishing, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, as well as supply chain attacks.¹⁷

At the same time, cyberattacks occur against the backdrop of intensifying geopolitical tensions, directly affecting the EU's energy security. It is a very well-known fact that the EU has limited domestic reserves of fossil fuels and is the largest energy importer in the world, with nearly 60% of its primary energy consumption dependent on imports, predominantly oil, coal, and natural gas.¹⁸ For natural gas in

¹³ FILHO W. AND COLL. *Prosumers and sustainable development: An international assessment in the field of renewable energy*, Issued in Sustainable Futures, Volume 7, 2024. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S266618882400008X>

¹⁴ UK PARLIAMENT. *Demand side response: A tool for lowering household energy bills* [online] 2024. Retrieved from: <https://post.parliament.uk/research-briefings/post-pn-0715/> [cited 28/8/2025]

¹⁵ EURELECTRIC. *Cybersecurity in the power sector* [online] 2025. Retrieved from: <https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/> [cited 28/8/2025]

¹⁶ [ibid]

¹⁷ [ibid]

¹⁸ EUROSTAT. *EU imports of energy products - latest developments* [online] 2024. Source: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU imports of energy products - latest developments](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_imports_of_energy_products_-_latest_developments) [cited 28/8/2025]

particular, the EU's import dependency in 2023 stood at approximately 90%.¹⁹ The long-term solution for both energy security and carbon neutrality might be the electrification of the EU's economy and society, powered by low-carbon sources as wind, solar, and - though politically more contentious - nuclear energy.²⁰

The urgency of this transformation has been further reinforced by the full-scale invasion of Ukraine by the Russian Federation on 24 February 2022. Russia's weaponization of energy supplies starkly exposed Europe's dependence on external providers and underscored the need to accelerate the scale-up of renewable energy. Thus, renewable sources are not only indispensable in combating climate change but also serve as a strategic tool to reduce reliance on imports from unreliable states and regimes. To this end, the EU is committed to maximizing its most abundant domestic resources, particularly solar, hydro, and wind power.

In this context, the REPowerEU initiative has prioritized the rapid expansion of renewable energy capacity, with offshore wind farms in Northern Europe and solar parks in Southern Europe being central elements. Yet, once again, the integration of these variable sources depends on the development of smart, digitalized grids capable of ensuring secure cross-border electricity flows across the internal market. Moreover, the ongoing international armed conflict in Ukraine has demonstrated the benefits of decentralized energy production. For over three years, Ukraine's energy infrastructure has been targeted by Russian forces. According to the IEA: "*As of November 2024, Russia had occupied, damaged or destroyed nearly two-thirds of Ukraine's dispatchable power generation capacity.*"²¹ By deploying decentralized renewable energy sources, such as solar panels and wind turbines, Ukraine has strengthened its energy security by reducing the vulnerability associated with large centralized production facilities like gas-fired or coal-fired power plants.²² At the same time, however, as previously mentioned, this decentralization increases reliance on digital systems, thus exposing the sector to a different category of risks - cyberattacks. Consequently, the EU has been compelled to develop a robust legislation framework that would address these evolving threats.

In addition, the EU should also seek to explore the role of international law in safeguarding critical energy infrastructure. This is particularly relevant in light of the

¹⁹ EUROSTAT. *Energy statistics - an overview* [online] 2024. Source: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_statistics_-_an_overview [cited 28/8/2025]

²⁰ EURONEWS. *Europe is divided on nuclear power: Which countries are for and against it?* [online] 2024. Source: https://commission.europa.eu/topics/energy/repower.eu_en [cited 28/8/2025]

²¹ IEA. *Empowering Ukraine Through a Decentralised Electricity System* [online] 2024. Source: <https://www.iea.org/reports/empowering-ukraine-through-a-decentralised-electricity-system> [cited 12/9/2025]

²² [ibid]

surge in state-sponsored cyberattacks, a considerable share of which has been directed against European critical infrastructure. Such attacks have ranged from ransomware incidents to deliberate attempts at disrupting electricity grids, illustrating the severity and complexity of the threats confronting the EU.²³ In this context, the EU should make greater use of international legal instruments to promote clarity regarding the rights and obligations of states in cyberspace, thereby strengthening the protection of its own energy sector against malicious activities.

Cyberattacks against Critical Energy Infrastructure from the Perspective of International Law

The changing geopolitical landscape has created a fertile ground for growing cybersecurity threats, particularly in the energy sector. The ongoing international armed conflict in Ukraine has demonstrated the vulnerability of critical energy infrastructure, which has repeatedly been targeted by cyberattacks.²⁴ According to the study published in 2021, 61 United Nations member states had created a cyber force by 2018, including a number of European states.²⁵ While states remain the primary actors capable of conducting such operations, they are not the only ones. Numerous other players, including state-related groups, cybercriminals, private sector offensive actors, and so-called hacktivists, pose significant risks.²⁶ In this fragmented environment, attribution of legal responsibility becomes highly complex, especially in the context of “hybrid warfare,” where states often rely on non-state actors with blurred links to conceal their involvement and maintain “plausible deniability”. Against this backdrop, it is of utmost importance for the EU to strive for greater legal clarity at the international level regarding the rights and obligations of states in cyberspace.

Ongoing debates focus in particular on the applicability and interpretation of international humanitarian law (hereinafter referred to as “IHL”) norms to cyber operations. Given that several EU member states have established their own cyber forces, a clear understanding of the relevant legal framework is essential for military

²³ LE MONDE. *Cyberattacks on the rise in Europe amidst the war in Ukraine* [online] 2024. Source: https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html [cited 28/8/2025]

²⁴ GOVERNMENT OF CANADA. *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine* [online] 2022. Retrieved from: <https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine>

²⁵ BLESSING J. *The Global Spread of Cyber Forces, 2000–2018*. 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2021, pp. 233-255, doi: 10.23919/CyCon51939.2021.9467807

²⁵ EUROPEAN COUNCIL. *Cyber threats in the EU: facts and figures* [online] Retrieved from: <https://www.consilium.europa.eu/en/policies/top-cyber-threats/> [cited 30/8/2025]

²⁶ [ibid]

planners and legal advisers, especially should armed conflict become reality.²⁷ Consensus among EU member states would not only strengthen legal certainty but also improve the chances of wider compliance with IHL by third states. With the clear understanding of applicable legal rules, it would be possible to hold states responsible for their misconduct as well as to establish individual criminal responsibility for potential war crimes committed through cyberattacks.

However, the first precondition is the recognition that international law applies to cyberspace. At the expert level, already in 2013, the UN Group of Governmental Experts (hereinafter referred to as the "GGE") managed to achieve a consensus on the applicability of international law to cyberspace.²⁸ At the political level, for instance, in November 2024, the EU adopted a declaration on a common understanding of application of international law to cyberspace, whereby reaffirmed that:

*"...respect for and adherence to the UN framework of responsible state behaviour in cyberspace remain essential to maintaining international peace, security, and stability... [and] that international law, particularly the UN Charter, international human rights law, and international humanitarian law, fully applies to cyberspace."*²⁹

However, application of IHL norms is triggered only in situations of armed conflict - either international³⁰, between two or more states, or non-international³¹, involving states and organized armed groups. The key legal question, therefore, is whether a cyberattack can be considered a "resort to armed force"³² that initiates an armed conflict.

Two scenarios illustrate the dilemma. If a cyberattack is conducted in a conjunction with a kinetic attack against another state, it clearly triggers an international armed conflict. By contrast, if a cyberattack occurs independently, the legal threshold

²⁷ As of 2018: Belgium Croatia Czechia Denmark Estonia France Germany Greece Hungary Italy Luxembourg Netherlands Norway Poland Portugal Romania Slovakia Spain. Source: BLESSING J. *The Global Spread of Cyber Forces, 2000–2018*. 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2021, pp. 233–255, doi: 10.23919/CyCon51939.2021.9467807

²⁸ MAČÁK K., RODENHÄUSER T. *Towards common understandings: the application of established IHL principles to cyber operations* [online] 2023. Retrieved from: <https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/>

²⁹ EUROPEAN COUNCIL. *Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace* [online] 2023. Retrieved from: <https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/> [cited 23/9/2025]

³⁰ Article 2 Common to the Geneva Conventions

³¹ Article 3 Common to the Geneva Conventions

³² ICRC ORG. *International armed conflict* [online] Retrieved from: https://casebook.icrc.org/a_to_z/glossary/international-armed-conflict

remains unsettled. Many states as well as the ICRC argue that cyber operations producing effects equivalent to kinetic force - such as those comparable to a missile strike - should trigger the application of IHL. Others disagree, particularly where an attack merely causes a loss of functionality without physical damage as such.³³ This disagreement raises pressing questions, for example: "Would a cyber operation disabling a nuclear power plant that supplies millions of households constitute an unlawful attack under IHL principles of distinction, proportionality, and necessity, or would it be treated as a legitimate target simply because no physical destruction occurred?"

This is only one of many questions related to the application of IHL norms to cyber operations. It is, however, outside the scope of this paper to deal with all of them. What is important is to emphasize the role of the EU in clarifying how the principles and norms of IHL should be applied to cyber operations. Given that the EU member states themselves possess formidable cyber operation capabilities, and the same applies to their potential adversaries, it is in the EU's interest to have these rules clearly settled.

The situation gets even more complex given the number of actors active in cyber operations blurring the lines between armed conflicts and peacetime creating the so-called "hybrid warfare". However, if a cyberattack does not constitute an armed attack within the meaning of IHL, at least the rules of general international law on state responsibility still apply. Yet, there is still a great number of questions to be asked, such as: "Who is responsible for the conduct of non-State actors in cyberspace? What are obligations of states *vis-à-vis* such non-State actors operating from their territories?"

In this regard, the UN has identified and developed specific norms through reports from the UN Group of Governmental Experts on responsible state behaviour in cyberspace (hereinafter referred to as the "GGE"). General Assembly Resolution 70/237³⁴ endorsed the 2015 GGE report, which set out 11 voluntary, non-binding norms with three being directly relevant to the protection of critical infrastructure, including energy.³⁵ First and foremost, states should not conduct or knowingly support information and communication technology (hereinafter referred to as the

³³ MAČÁK K., RODENHÄUSER T. *Towards common understandings: the application of established IHL principles to cyber operations* [online] 2023. Retrieved from: <https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/> [cited 20/9/2025]

³⁴ Resolution A/RES/70/237 adopted by the General Assembly on 23 December 2015. Available at: <https://docs.un.org/en/A/res/70/237> [cited 20/9/2025]

³⁵ Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: <https://docs.un.org/en/a/70/174>

“ICT”) activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.³⁶ Secondly, states should take appropriate measures to protect their critical infrastructure from ICT threats, while taking into account relevant General Assembly resolutions.³⁷ And finally, states should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty.³⁸

Yet, because these norms are non-binding, compliance remains at the discretion of states. Given the EU’s exposure to cyber threats in the context of its energy transition and heightened geopolitical tensions, it is in the EU’s strategic interest to transform these voluntary commitments into binding obligations. This would require the negotiation of a new international treaty on the protection of critical infrastructure against cyberattacks, building on the existing GGE norms. Such a treaty should establish clear rights and obligations of states, incorporate a robust dispute settlement mechanism, and create an implementation body capable of monitoring compliance, including through mechanisms such as “naming and shaming.”³⁹ This would help establish state responsibility for internationally wrongful acts, including those committed by non-state actors operating within the territory of specific states, which is particularly a problem for the EU.⁴⁰

The EU is uniquely positioned to lead such an initiative, owing to its strong diplomatic power and existing experience in global cyber governance. It has already played a decisive role in securing international consensus on establishing a permanent UN mechanism to promote responsible state behaviour in cyberspace, grounded in

³⁶ Point 13f) of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: <https://docs.un.org/en/a/70/174> [cited 20/9/2025]

³⁷ Point 13 g) of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: <https://docs.un.org/en/a/70/174> [cited 20/9/2025]

³⁸ Point 13f) of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: <https://docs.un.org/en/a/70/174> [cited 20/9/2025]

³⁹ PAWLAK P., GÉRY A. *Why the World Needs a New Cyber Treaty for Critical Infrastructure* [online] 2024. Retrieved from: <https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en>

⁴⁰ EURELECTRIC. *A snapshot of Cybersecurity in the EU* [online] 2024. Retrieved from: <https://www.eurelectric.org/publications/eurelectric-short-paper-a-snapshot-of-cybersecurity-in-the-eu/>

international law, human rights, and multilateralism. This mechanism builds on the 2020 proposal by the EU and its member states for a “UN cyber Programme of Action”.⁴¹ Therefore, in its future work, the EU should champion for the adoption of a comprehensive new international treaty on the protection of critical infrastructure against cyberattacks - an objective directly linked to safeguarding its critical energy infrastructure.

Alternatively, given the current state of international affairs, it is true to admit that it is very unlikely that the international community would adopt any new comprehensive treaty, especially on such a sensitive topic as the protection of critical infrastructure against cyberattacks. Therefore, it might be worth taking note of a proposal by the German Council on Foreign Relations urging states to sign political declarations whereby they would refrain from conducting any cyber operations against select critical infrastructure – early warning satellites, nuclear command and control systems, electrical grids – of the parties involved during peacetime.⁴² In this paper, even more ambitious proposals are made urging states to sign bilateral agreements based upon the example of the 1988 Agreement on the Prohibition of Attack Against Nuclear Installations and Facilities concluded between India and Pakistan. In this agreement both parties agreed to completely and explicitly prohibit this type of attacks which is the only one of its kind.⁴³ The same would be possible to conclude only with a difference being the protection of select critical infrastructure against cyberattacks during peacetime.

Having outlined the international dimension, the next chapter will briefly present the EU’s internal legal and regulatory framework for protecting critical energy infrastructure against cyberattacks. It will also address mechanisms for ensuring the necessary international cooperation in this field, given the cross-border nature of such threats and the risk of cascading effects originating from third states.

⁴¹ EEAS. *UN Member States agree to establish a global mechanism to advance responsible state behaviour in cyberspace* [online] 2024. Retrieved from: https://www.eeas.europa.eu/delegations/un-new-york/un-member-states-agree-establish-global-mechanism-advance-responsible-state-behaviour-cyberspace_en?s=63

⁴² WEBER V. *How German (Cyber)diplomacy Can Strengthen Norms in a World of Rule-Breakers* [online] 2023. Retrieved from: <https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms> [cited 20/9/2025]

⁴³ NEOG R. *Targeting Nuclear Facilities During War: What Does International Law Have to Say?* [online] 2024. Retrieved from: <https://www.apln.network/analysis/commentaries/targeting-nuclear-facilities-during-war-what-does-international-law-have-to-say> [Cit. 24/10/2024]

Protection of Critical Energy Infrastructure at the EU Level and International Cooperation

Over the past decade, the EU has adopted a broad set of legislative acts to strengthen the cybersecurity of critical infrastructure, including the energy sector. These consist of either horizontal instruments such as the EU Cyber Solidarity Act⁴⁴, the Cyber Resilience Act⁴⁵, and the NIS2 Directive⁴⁶, as well as sector-specific legislations like the Network Code on Cybersecurity⁴⁷, or the Regulation on Risk Preparedness in the Electricity Sector⁴⁸ or the Regulation on Safeguarding the Security of Gas Supply⁴⁹. Taken together, at the EU level, these legislative acts form a comprehensive framework. The key challenge, however, lies in ensuring consistent and harmonised implementation across all member states. Despite the high degree of interconnection of Europe's energy systems, national differences persist, complicating cooperation and increasing the risk of cyber incidents. For this reason, the EU should allow sufficient time for member states to fully implement existing rules before adopting new legislation. At the same time, any future regulatory initiatives should be introduced only when strictly necessary and after careful validation to avoid overlap with existing instruments thereby avoiding unnecessary bureaucratic complexity.⁵⁰

Another essential dimension of resilience is sustained investment in the cybersecurity of energy infrastructure, particularly electricity grids. Here, the TEN-E

⁴⁴ Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)

⁴⁵ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

⁴⁶ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

⁴⁷ Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

⁴⁸ Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

⁴⁹ Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010

⁵⁰ EURELECTRIC. *A snapshot of Cybersecurity in the EU* [online] 2024. Retrieved from: <https://www.eurelectric.org/publications/eurelectric-short-paper-a-snapshot-of-cybersecurity-in-the-eu/> [cited 20/9/2025]

Regulation⁵¹ plays a crucial role, as it defines Projects of Common Interest (PCIs) and Projects of Mutual Interest (PMIs)⁵² which are key cross-border projects that enhance the interconnection of European and neighbouring third states energy systems.⁵³ Projects included on the Union list of PCI/PMI benefit from accelerated permitting procedures⁵⁴ and access to funding under the Connecting Europe Facility (CEF).⁵⁵ Notable examples include Projects of Common Interest with participation of the Slovak transmission and distribution system operators ACON⁵⁶ or Danube Ingrid⁵⁷, which focus on integrating renewable energy sources through smart grid technologies. However, as already mentioned, the increased use of new digital technologies go hand in hand with an increased exposure to cyberattacks. Therefore, these projects also invest in enhancing resilience of smart grids against cyberattacks. The latest example from our region is the candidate Project of Common Interest in priority thematic area smart electricity grids deployment – SELENA, which aims to enhance operational security, cybersecurity, infrastructure resilience, and cross-border data exchange.⁵⁸

The TEN-E Regulation also enables investments in projects with third countries, the so-called PMIs. These are important given that European network is synchronized with also electricity grids of third states. As an example, Ukrainian and Moldovan electricity grids were synchronized with European network in less than 3 weeks after the Russian full-scale invasion, despite initial plans foreseeing more than a year.⁵⁹ This development not only ensured stability for Ukraine and Moldova but also demonstrated the strategic importance of interconnected networks. In this context,

⁵¹ Regulation (EU) 2022/869 of the European Parliament and of the Council of 30 May 2022 on guidelines for trans-European energy infrastructure, amending Regulations (EC) No 715/2009, (EU) 2019/942 and (EU) 2019/943 and Directives 2009/73/EC and (EU) 2019/944, and repealing Regulation (EU) No 347/2013

⁵² Article 3 of the TEN-E Regulation

⁵³ EC. *Key cross-border infrastructure projects* [online] Retrieved from: https://energy.ec.europa.eu/topics/infrastructure/projects-common-interest-and-projects-mutual-interest/key-cross-border-infrastructure-projects_en [cited 20/9/2025]

⁵⁴ Article 10 of TEN-E Regulation

⁵⁵ EC. *Connecting Europe Facility* [online] Retrieved from: https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en [cited 20/9/2025]

⁵⁶ ACON. *ACON: Project of common interest* [online] Retrieved from: <https://www.acon-smartgrids.cz/> [cited 20/9/2025]

⁵⁷ DANUBE INGRID. *Danube InGrid Smart grid Project of Common Interest of the European Union* [online] Retrieved from: <https://danubeingrid.eu/> [cited 20/9/2025]

⁵⁸ SELENA. *Candidate Project Of Common Interest Priority Thematic Area Smart Electricity Grids Deployment* [online] Retrieved from: <https://www.selena-smartgrid.eu/> [cited 20/9/2025]

⁵⁹ EC. *2 years since Ukraine and Moldova synchronised electricity grids with EU* [online] Retrieved from: https://energy.ec.europa.eu/news/2-years-ukraine-and-moldova-synchronised-electricity-grids-eu-2024-03-15_en [cited 20/9/2025]

the CESEC High-Level Group⁶⁰, which coordinates efforts to facilitate cross-border and trans-European energy infrastructure projects in central-eastern and south-eastern Europe⁶¹, plays a vital coordinating role, bringing together EU Member States⁶² and Energy Community Contracting Parties. One of the competences of this platform is to compile a list of priority projects for building an interconnected regional electricity market.

However, given the risk of cascading effects in the energy sector, harmonised legislation on the protection of critical infrastructure against cyberattacks is indispensable. In this regard, the Energy Community provides a key international organization for bridging the EU and nine neighbouring EU candidate or potential candidate countries, to create an integrated regional energy market based on a legally binding framework.⁶³ Its Contracting Parties are obliged to adopt the EU energy *acquis* and enforce EU rules across a wide range of areas, including electricity, gas, infrastructure, renewables, energy efficiency, climate policy, and - most relevant in this context - cybersecurity.⁶⁴ In 2019, the Energy Community published its Final Report on Cyber Security in the Energy Sector of the Energy Community, which assessed gaps between the Contracting Party legislation and EU-wide energy sector cybersecurity legislation and standards. Moreover, Energy Community-wide and Contracting Party-specific cybersecurity risk assessments were addressed.⁶⁵ The report further stressed that eliminating regulatory gaps and harmonising cybersecurity measures across the integrated market is crucial for building a resilient energy system.

At the same time, the EU must rely on strategic international cooperation to protect critical infrastructure from hybrid threats, including cyber operations. In January 2023, the President of the European Commission and the Secretary General of NATO announced the establishment of a dedicated NATO-EU Task Force on the Resilience of Critical Infrastructure. The Task Force issued its final report in June 2023, recommending concrete measures to enhance resilience and underlining the shared interest of both organizations in preventing disruptions. In light of these recommendations, cooperation between the EU and NATO should be designed as

⁶⁰ Central and South-Eastern Europe Energy Connectivity

⁶¹ EC. *Central and South-Eastern Europe Energy Connectivity* [online] Retrieved from: https://energy.ec.europa.eu/topics/infrastructure/high-level-groups/central-and-south-eastern-europe-energy-connectivity_en [cited 20/9/2025]

⁶² Austria, Bulgaria, Croatia, Greece, Hungary, Italy, Romania, Slovakia and Slovenia.

⁶³ EC. *Energy Community* [online] Retrieved from: https://energy.ec.europa.eu/topics/international-cooperation/international-organisations-and-initiatives/energy-community_en [cited 20/9/2025]

⁶⁴ [ibid]

⁶⁵ ENERGY COMMUNITY. *Final Report - Study on cyber security in the energy sector of the Energy Community* [online] 2019 Retrieved from: https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf [cited 20/9/2025]

complementary and mutually reinforcing, with a focus on preparedness and coordinated crisis management.⁶⁶

This partnership approach has been mirrored and further reinforced by the EU Preparedness Union Strategy, adopted in March 2025, which identifies integration of preparedness and resilience into NATO cooperation as one of its key priorities in the area of “Resilience through external partnerships”. The strategy stresses the importance of building mutual resilience with partners, particularly in addressing cyber threats against energy systems, given their central role in both national security and societal stability.⁶⁷

Concluding remarks

Cybersecurity of critical energy infrastructure is becoming increasingly important as the energy sector transitions from centralized power generation to decentralized, renewable-based models such as photovoltaic parks and wind farms. This profound transformation, driven by the deployment of intermittent renewable energy sources, has accelerated both electrification and digitalization of the entire system. While these developments bring significant advantages for energy security in terms of decentralization, they also create new vulnerabilities. Among the most serious belong cyber operations targeting this critical energy infrastructure.

The EU is particularly exposed to these threats due to its ambitious climate objectives and the rising geopolitical tensions. Its commitment to becoming the first climate-neutral continent by 2050 requires large-scale deployment of renewable energy sources. To integrate intermittent, weather-dependent generation, modernization of transmission and distribution grids is indispensable. However, this modernization simultaneously increases exposure to cyber risks. Moreover, with the international armed conflict in Ukraine at its doorstep and the rise of hybrid threats, the EU has witnessed a sharp increase in cyberattacks on its critical energy infrastructure. In such a hostile environment, where state-related groups, cybercriminals, private sector offensive actors, and so-called hacktivists are all active, the EU has to use all available legal tools whether at the international or European level to counter these threats and enhance cybersecurity and resilience of its critical energy infrastructure.

At the international level, the EU should take a leading role in clarifying the rights and obligations of states in cyberspace, especially regarding the protection of critical energy infrastructure against cyber operations. The international armed conflict in

⁶⁶ EC. *EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report* [online] 2019 Retrieved from: https://commission.europa.eu/document/34209534-3c59-4b01-b4fo-b2c6ee2df736_en [cited 20/9/2025]

⁶⁷ EC. *EU preparedness union strategy* [online] Retrieved from: https://commission.europa.eu/topics/preparedness_en [cited 20/9/2025]

Ukraine has particularly highlighted the contentious issue of applying and interpreting IHL norms to cyberattacks. Given its diplomatic and soft-power strengths, the EU is well positioned to push this agenda, building on its success in securing international consensus for a permanent UN mechanism to promote responsible state behavior in cyberspace. Ideally, this would culminate in a comprehensive international treaty on the protection of critical infrastructure against cyberattacks, building on the work of the UN GGE and its 11 voluntary norms. However, given the current geopolitical landscape, the EU and its member states should also persuade other states to conclude at least bilateral agreements, modeled on the 1988 Agreement between India and Pakistan prohibiting attacks on nuclear facilities during armed conflict, but adapted to cyberattacks on critical energy infrastructure in peacetime.

At the European level, the EU has already established a comprehensive regulatory framework combining horizontal and sector-specific legislation. The key priority now is to ensure that member states fully transpose and implement these existing rules before introducing new legislative acts.⁶⁸ Equally important is sustained investment in the resilience of energy infrastructure, particularly electricity grids. Projects of Common Interest (PCIs) and Projects of Mutual Interest (PMIs) eligible for funding through the Connecting Europe Facility (CEF) and accelerated permitting procedures, play an essential role in strengthening cybersecurity in cross-border infrastructure. In this regard, the CESEC High-Level Group is an important platform where identification of priority projects for building an interconnected regional electricity market is conducted at the political level. Moreover, because of the risk of cascading effects in the energy sector, international cooperation is indispensable. In this context, the Energy Community helps candidate and neighboring countries to align their legal frameworks with the EU energy *acquis*, including in the field of cybersecurity, thereby extending resilience beyond EU borders. Finally, in the face of hybrid threats, cooperation with NATO remains crucial to ensure the physical and military protection of EU's critical energy infrastructure.

All in all, the EU will certainly face a significant increase in cyberattacks against its critical energy infrastructure. Therefore, the EU has to address these threats through enhanced international cooperation with its allies and partners using all available international platforms and organizations, while taking a leading role in initiatives at

⁶⁸ This statement is somewhat amusing, as the European Commission has at the time of writing of this paper published a call for evidence for revision of the EU's energy security architecture in order to adapt to the new geopolitical, energy and climate situation and prepare for a more decarbonised, electrified and integrated energy system. Available at: EC. *EU energy security framework (revision)* [online] 2025 Retrieved from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14695-EU-energy-security-framework-revision_en [cited 20/9/2025]

the international level aimed at clarifying and developing rules for the protection of critical energy infrastructure against cyberattacks.

Bibliography:

1. ACON. *ACON: Project of common interest* [online] Retrieved from: <https://www.acon-smartgrids.cz/>
2. ALANAZI M., MAHMOOD A., CHOWDHURY M. *SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues*. Issued in *Computers & Security*, Volume 125, 2023. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S0167404822004205>
3. BBC. *Nord Stream 1: How Russia is cutting gas supplies to Europe* [online] 2022. Retrieved from: <https://www.bbc.com/news/world-europe-60131520>
4. BLESSING J. *The Global Spread of Cyber Forces, 2000–2018*. 2021 13th *International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2021, pp. 233-255, doi: 10.23919/CyCon51939.2021.9467807
5. CNN. *Spain says April blackout was caused by grid failures and poor planning, not a cyberattack* [online] 2024. Retrieved from: <https://edition.cnn.com/2025/06/17/europe/spain-april-blackout-not-cyberattack-intl-hnk>
6. Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows
7. COMMISSION STAFF WORKING DOCUMENT Accompanying the document Commission Recommendation on cybersecurity in the energy sector {C(2019) 2400 final}
8. DANUBE INGRID. *Danube InGrid Smart grid Project of Common Interest of the European Union* [online] Retrieved from: <https://danubeingrid.eu/>
9. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
11. EC. *2 years since Ukraine and Moldova synchronised electricity grids with EU* [online] Retrieved from: https://energy.ec.europa.eu/news/2-years-ukraine-and-moldova-synchronised-electricity-grids-eu-2024-03-15_en

12. EC. *Central and South-Eastern Europe Energy Connectivity* [online] Retrieved from: https://energy.ec.europa.eu/topics/infrastructure/high-level-groups/central-and-south-eastern-europe-energy-connectivity_en
13. EC. *Connecting Europe Facility* [online] Retrieved from: https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en [cited 20/9/2025]
14. EC. *Energy Community* [online] Retrieved from: https://energy.ec.europa.eu/topics/international-cooperation/international-organisations-and-initiatives/energy-community_en
15. EC. *EU energy security framework (revision)* [online] 2025 Retrieved from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14695-EU-energy-security-framework-revision-_en
16. EC. *EU preparedness union strategy* [online] Retrieved from: https://commission.europa.eu/topics/preparedness_en
17. EC. *EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report* [online] 2019 Retrieved from: https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en
18. EC. *Key cross-border infrastructure projects* [online] Retrieved from: https://energy.ec.europa.eu/topics/infrastructure/projects-common-interest-and-projects-mutual-interest/key-cross-border-infrastructure-projects_en
19. EEAS. *Call for urgent global action to mitigate climate crisis - the external dimension of the European Green Deal* [online] 2021. Retrieved from: https://www.eeas.europa.eu/eeas/call-urgent-global-action-mitigate-climate-crisis-external-dimension-european-green-deal_en
20. EEAS. *UN Member States agree to establish a global mechanism to advance responsible state behaviour in cyberspace* [online] 2024. Retrieved from: https://www.eeas.europa.eu/delegations/un-new-york/un-member-states-agree-establish-global-mechanism-advance-responsible-state-behaviour-cyberspace_en?s=63
21. ENERGY COMMUNITY. *Final Report - Study on cyber security in the energy sector of the Energy Community* [online] 2019 Retrieved from: https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf
22. EURELECTRIC. *A snapshot of Cybersecurity in the EU* [online] 2024. Retrieved from: <https://www.eurelectric.org/publications/eurelectric-short-paper-a-snapshot-of-cybersecurity-in-the-eu/>
23. EURELECTRIC. *Cybersecurity in the power sector* [online] 2025. Retrieved from: <https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/>

24. EURONEWS. *Europe is divided on nuclear power: Which countries are for and against it?* [online] 2024. Source: https://commission.europa.eu/topics/energy/repowereu_en
25. EUROPEAN COUNCIL. *Cyber threats in the EU: facts and figures* [online] Retrieved from: <https://www.consilium.europa.eu/en/policies/top-cyber-threats/>
26. EUROPEAN COUNCIL. *Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace* [online] 2023. Retrieved from: <https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/>
27. EUROSTAT. *Energy statistics - an overview* [online] 2024. Source: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy statistics - an overview](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_statistics_-_an_overview)
28. EUROSTAT. *EU imports of energy products - latest developments* [online] 2024. Source: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU imports of energy products - latest developments](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_imports_of_energy_products_-_latest_developments)
29. FILHO W. AND COLL. *Prosumers and sustainable development: An international assessment in the field of renewable energy*, Issued in Sustainable Futures, Volume 7, 2024. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S266618882400008X>
30. Geneva Conventions
31. GOVERNMENT OF CANADA. *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine* [online] 2022. Retrieved from: <https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine>
32. ICRC ORG. *International armed conflict* [online] Retrieved from: https://casebook.icrc.org/a_to_z/glossary/international-armed-conflict
33. IEA. *Empowering Ukraine Through a Decentralised Electricity System* [online] 2024. Source: <https://www.iea.org/reports/empowering-ukraine-through-a-decentralised-electricity-system>
34. IEA. *World Energy Outlook 2022* [online] 2022. Retrieved from: <https://www.iea.org/reports/world-energy-outlook-2022>
35. LE MONDE. *Cyberattacks on the rise in Europe amidst the war in Ukraine* [online] 2024. Source: https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html
36. MAČÁK K., RODENHÄUSER T. *Towards common understandings: the application of established IHL principles to cyber operations* [online] 2023. Retrieved from: <https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common->

[understandings-the-application-of-established-ihl-principles-to-cyber-operations/](#)

37. NEOG R. *Targeting Nuclear Facilities During War: What Does International Law Have to Say?* [online] 2024 Retrieved from: <https://www.apln.network/analysis/commentaries/targeting-nuclear-facilities-during-war-what-does-international-law-have-to-say>
38. PAWLAK P., GÉRY A. *Why the World Needs a New Cyber Treaty for Critical Infrastructure* [online] 2024. Retrieved from: <https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en>
39. POLITICO. *Vote on 2040 climate target canceled after big EU countries block decision* [online] 2025. Retrieved from: <https://www.politico.eu/article/vote-on-eus-2040-climate-target-canceled-after-biggest-countries-block-decision/>
40. Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010
41. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC
42. Regulation (EU) 2022/869 of the European Parliament and of the Council of 30 May 2022 on guidelines for trans-European energy infrastructure, amending Regulations (EC) No 715/2009, (EU) 2019/942 and (EU) 2019/943 and Directives 2009/73/EC and (EU) 2019/944, and repealing Regulation (EU) No 347/2013
43. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)
44. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)
45. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: <https://docs.un.org/en/a/70/174>
46. Resolution A/RES/70/237 adopted by the General Assembly on 23 December 2015. Available at: <https://docs.un.org/en/A/res/70/237> [cited 20/9/2025]
47. SELENA. *Candidate Project Of Common Interest Priority Thematic Area Smart Electricity Grids Deployment* [online] Retrieved from: <https://www.selena-smartgrid.eu/>

48. UK PARLIAMENT. *Demand side response: A tool for lowering household energy bills* [online] 2024. Retrieved from: <https://post.parliament.uk/research-briefings/post-pn-0715/>
49. WEBER V. *How German (Cyber)diplomacy Can Strengthen Norms in a World of Rule-Breakers* [online] 2023. Retrieved from: <https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms> [cited 20/9/2025]

Contact details

Mgr. Marek Janček

jancek16@uniba.sk

Comenius University in Bratislava, Faculty of Law, Department of International Law and International Relations

ÚSTAVNĚPRÁVNÍ ASPEKTY OCHRANY ČLOVĚKA V ELEKTRONICKÉM UŽIVATELSKÉM PROSTORU

CONSTITUTIONAL ASPECTS OF HUMAN PROTECTION IN THE ELECTRONIC USER SPACE

Karel Klíma¹

Abstrakt: Společenské prostředí života obyvatel a jednotlivců zvláště je ovlivňováno řadou elektronizačních procesů. Jedná se především o pokračující digitalizaci veřejnoprávní komunikace a umělou inteligenci, jako schopnost počítačů napodobovat lidské myšlení. Občan zvláště se tak stává objektem digitalizace, a to v jeho nejpřirozenější hodnotě, již je právo na život, nedotknutelnost osoby, právo na soukromí a jeho garance, svoboda myšlení, slova, projevu apod. Příspěvek řeší nezbytnost udržitelnosti lidského faktoru zejména v komunikaci s orgány veřejné správy a v postupující digitalizaci veřejnoprávního rozhodování. Zkoumá tak zejména ústavněprávní dopady digitalizace veřejnoprávních vztahů a současně zachování lidské přirozenoprávnosti, jakož i digitalizační limity při vrchnostenské nadřazenosti státní moci.

Klíčové slová: elektronizace, digitalizace, umělá inteligence, udržitelnost lidského faktoru, základní lidská práva, právo na život, ochrana soukromí, digitalizační limity, ústavněprávní odpovědnost státní moci

Abstract: The social environment of the lives of residents and individuals is particularly influenced by several electronic processes. This concerns primarily the ongoing digitalization of public law communication and artificial intelligence, as the ability of computers to imitate human thinking. The citizen thus becomes an object of digitalization, in its most natural value, which is the right to life, the inviolability of the person, the right to privacy and its guarantees, freedom of thought, speech, expression, etc. The contribution addresses the necessity of sustainability of the human factor, especially in communication with public administration bodies and in the progressive digitalization of public law decision-making. It examines the constitutional legal impacts of the digitalization of public law relations and at the same time

¹ Katedra právních disciplín a veřejné správy, Metropolitní univerzita v Praze.

the preservation of human natural law, as well as the limits of digitalization in the event of the supremacy of state power.

Key words: electronization, digitization, so-called artificial intelligence, sustainability of the human factor, fundamental human rights, right to life, protection of privacy, digitalization limits, constitutional responsibility of state power

Úvod

Veřejnost může být postupně překvapována, zděšena, fascinována, zneklidňována, ale i uklidňována expanzí stylu komunikace veřejné správy, který je více a více založen na takovém způsobu elektronické komunikace, jež nazýváme digitalizací. Jedná se o nezvratný proces, způsob a tím i ovlivňování společenských vztahů, na který se musí reagovat, neboť sice „*cesta do pekel, je dlážděna (předpokládáme) dobrými úmysly*“, ale vyžaduje se její trvalé sledování jakož i přiměřená reagence.²

Zvolené a zde diskutované téma má v sobě apriorně pocitový „náboj“ rezistence člověka vůči expanzi elektronizace určitých společenských komunikačních procesů, uživatelského charakteru, ba i rozhodovacího efektu, neboť se týká veřejnoprávní komunikace. Čili, týká se vztahů, kde člověk (firma) vstupuje do „povinné“ komunikace s veřejnou správou (např. žádá o vydání určitého průkazu, o vydání stavebního povolení, přijetí na určitou školu, o registraci živnosti apod.). Jiná situace nastává tehdy, kdy dokonce musí reagovat na zásahy veřejné moci (subjekt obdržel rozhodnutí o přestupku, s nímž nesouhlasí, odmítnutí žádosti apod.).

Konstatujeme tedy: je třeba akceptovat společenský vývoj a k věci se postavit tak, že když lidé něco vymyslí, musí být schopni dostát zásadě udržitelnosti lidského faktoru v tomto postupně se rozvíjejícím vztahu. Je nutno se tedy řídit zásadou, že každá etapa digitalizace (elektronizace, modernizace) musí být lidská.³

² V současnosti je obtížné najít právní definici umělé inteligence. Evropská komise se o ní pokusila v dubnu roku 2018 s následujícím textem: „Umělá inteligence, dále AI, (případně dle kontextu autonomní systémy) odkazuje na systémy, které vykazují inteligentní chování tím, že analyzují své prostředí a jednají s jistou mírou autonomie tak, aby dosáhly určitých specifických cílů. Systémy založené na AI mohou mít čistě softwarovou povahu a jednat ve virtuálním světě nebo mohou mít být vestavěny do hardwarové zařízení...“, srov. k tomu in: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>.

³ Pramenná literatura, která by zohledňovala a samozřejmě poskytovala poznatky k problematice vztahu práva a jeho užívání na straně jedné a problematiky umělé inteligence na straně druhé je očekávaně skoupá a mimořádná. Tradiční konzervatismus právnické obce je zatížen zřejmě „vyčkáváním“ na poznatky elektronizačního vývoje v této sféře. Tak se objevují varování směřující do zásahů do lidských práv, kdy se ve vztahu k digitalizaci hovoří až jako o nástrojích úředního, resp. digitálního teroru, srov. k tomu J. Navrátil in: ŠTĚDRŮŇ, B. a kol. *Právo a umělá inteligence*. Plzeň: Aleš Čeněk, 2020, ISBN 978-80-7380-803-7, s.16 a násl.

Jako stěžejní hypotetické konstatování tohoto řešitelského pojednání klademe tezi, podle níž expanze elektronizace se výrazně dotýká lidské existence jak ve vztahu k lidstvu, tak ve vztahu k jednotlivcům. Ústavněprávní odpovědnost veřejné moci tak spočívá v trvalé udržitelnosti lidského faktoru, zejména jeho tvůrčí nezastupitelnosti, ale také ochraně.

Ústavně zaručené právo na život jako výchozí sféra ochrany člověka

Při zkoumání fenoménu, jímž je vývoj elektronizace a jeho využití ze strany veřejné moci při komunikaci zejména s fyzickou osobou, se musíme pohybovat na základech ústavního práva na život. V konceptu Rady Evropy, Evropského soudu pro lidská práva, naší Listiny základních práva a svobod a samozřejmě samotného Ústavního soudu ČR je to hmotně-právně přirozenoprávní doména.⁴

To znamená, že zasahování státní moci do této sféry může být založeno jenom zákonem. Vycházejme takto z té hypotézy, že digitalizace bude zachovávat zákonem stanovená pravidla, a jde tedy o to, aby se v zásadě technologický způsob a vývoj této komunikace nestal nesrozumitelným, nejasným, neovladatelným, ba i odpudivým. Ze strany státní moci tak nastupuje požadavek očekávání sebereflexe, v realizačních důsledcích pak šetrnosti a opatrnosti a případně zvýšené ochrany *erga omnes*.

Přirozenoprávní přístup je tak bariérou proti svévoli, kterou vyvolává expanze technicko-modernizačních procesů. Přirozenoprávní přístup totiž ukazuje na autentické lidské hodnoty, které by digitalizace neměla ohrožovat, potlačovat, ba i ničit. Jedině totiž svoboda myšlení je svobodou absolutní, potenciálně zvnějšku ohrožovanou, a to jak ze strany okolí ve vztazích horizontálních, tak bohužel takto ovlivňovanou možná častěji ze strany státu. A tím ohrožením může být jak explozivní digitalizace, plošného charakteru tak i nespoutaná tzv. „umělá inteligence“ (dále jen AI).⁵

Přirozenoprávní přístup nám dává jistotu, že někde musí státem vnucený způsob elektronické komunikace narazit, a to je soukromí člověka, jeho svědomí, čest a pocit osobní jistoty, jakož i ochrana rodiny. Identita člověka je založena na osobitosti každého individua a zejména na intelektuálních schopnostech, uvažování, hodnocení

⁴ J. Navrátil k tomu trefně poznamenává, že: „Pokud bychom pro u fungování umělé inteligence zvolili směr ryze přirozenoprávní, bylo by riziko vymknutí se umělé inteligence a lidskosti zřejmě nejvyšší, přitom přirozenoprávní přístup má nesporné výhody a při správné aplikaci může právě on být důležitou bariérou proti svévoli umělé inteligence“, srov. in: *Právo a umělá inteligence*, ... tamtéž, s. 19.

⁵ Vývoj informačních a komunikačních technologií přinesl taktéž do práva takové množství zásadních formálních proměn, že z toho vyplynula potřeba specificky zaměřeného specifického přístupu, a tudíž i počátky formulace nového právního odvětví – práva informačních technologií, k tomu zejména srov. POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, ISBN, 978-80-75-98045-8.

jevů a psychice. Shora vnucený způsob elektronické komunikace je sice stejný (rovný) pro všechny lidské bytosti, ale s ohledem na odlišné, a přitom přirozené schopnosti lidí je schopen různým způsobem vědomí jednotlivých lidí degradovat, ponížít, i jinak negativně ovlivnit. Ani způsob aplikace zákonů jakož i jejich výklad právních předpisů nesmí být „odlidštěn“, a to zvláště při jejich procesní aplikaci.

Zvlášť sledovanou otázkou je digitalizace a veřejná subjektivní práva. Vycházíme z premisy, podle níž užití určitého práva občanem jej „dostává“ do komunikace s úřadem.⁶ Tento, na základě posouzení splnění zákonných podmínek rozhoduje o povolení, souhlasu, o registraci a podobně. Smysl digitalizace je v zásadě a logicky pozitivní – urychlit, zjednodušit, sumarizovat dokumenty, podklady, argumenty, a případně i připravit ve věcech (jednoduchých opakovacích, nesporných) i rozhodnutí. Zřejmě komplikací může být elektronická náročnost podání. Narážíme tak na problém předpokládané vstupní kontroverze mezi profesionalitou aparátu státu a schopností soukromého subjektu požadavky návrhu splnit ve všech formalizovaných údajích. Je zřejmé, že je odpovědností orgánů veřejné správy technicko-formální způsob podání připravit maximálně srozumitelně. Je také zřejmé, že komplikovanost takových podání je schopna realizaci veřejných subjektivních práv znesnadňovat. V té souvislosti se může významně uplatnit systém správního soudnictví, které by mělo nastoupit a s citem pro spravedlnost komplikovanost tohoto sporu vyřešit.

Klíčovou otázkou jsou tedy problémy technicko-komunikační. V té souvislosti je jasné, že se musí zachovat osobní dostupnost fyzické osoby do úřadu. Přitom by neměla ztížit rychlost řešení věci. Problémy s technickou a elektronickou či digitalizovanou komunikací nesmějí zahltovat opravné prostředky.

Aktuální elektronizační trendy a jejich vztah ke společenskému prostředí zejména veřejno-mocenskému charakteru

Vycházejme z předpokladu, že více než třicetiletí modernizace společenské komunikace přeneslo podstatnou část mezilidských vztahů do roviny elektronicky a virtuálně telefonicky zprostředkovaných kontaktů. Ve vztahu ke zpracování informací potom nastoupily digitalizační trendy, které na jedné straně postupně vytlačily odbornou učebnicovou literaturu, a na straně druhé umožnily zpracování dat přenést na elektronické nosiče. Jestliže se v posledním desetiletí do této modernizace dostává tzv. umělá inteligence, posouvá se elektronizační servis do podstatně vyšší úrovně kvalitativní činnosti, a sice do roviny nahrazující lidské myšlení. Jedná se tak zejména o cílové zhodnocování faktů, které by mělo sledovat objektivitu, věrohodnost, logičnost, a dokonce i kreativnost. Zřejmě, především zde

⁶ Zde máme na mysli právní situace, kdy na jedné straně fyzická či právnická osoba žádá o „přivolení státu“ (například povolené, souhlas, vydání průkazu apod), a na straně druhé, kdy fyzická nebo právnická osoba je objektem (adresátem) rozhodnutí orgánu veřejné správy.

uvedené se dá profesionálně naprogramovat, neboť technické poznatky ze světového vývoje robotizace mají určité časově vysoký a vývojově mnohačetný posun.⁷

Výše uvedené ve sféře, kterou zkoumáme, tedy veřejnoprávní rozhodování ve vztahu k soukromoprávnímu adresátovi, apriorně naráží na nezastupitelnost lidského faktoru. Týká se to jak toho subjektu, který rozhoduje (úřední osoba, komise, soudce, senát soudu apod.), tak toho subjektu, který je objektem rozhodování. V respektu k nezastupitelnosti lidského faktoru zjišťujeme tudíž různou úroveň přijatelného i nepřijatelného subjektivismu. Hledejme zejména jeho výhody, neboť každé profesionální (veřejnoprávní) rozhodování musí mít v sobě potřebnou úroveň diskrece – přirozeného lidského uvažování. Výsledně totiž sledujeme zásady spravedlnosti, humanismu, rovnoprávnosti, pružnosti, etičnosti. Je zapojení „umělé inteligence“ do rozhodovacích procesů tyto požadavky v potřebných dimenzích uplatňovat? Zhodnotí náležitě například smysl tzv. polehčujících, nebo naopak tzv. přitěžujících okolností? Elektronizační procesy jsou tedy součástí dodržování a uplatňování etiky komunikace veřejné moci s člověkem.

Každé „právo na život“ je naplňováno subjektivně, čímž vyvolává nároky na objektivní prostředí. Toto objektivní prostředí je v zásadě co do komunikace člověka se státní mocí zákonem dané, vymezené, ovlivňované. Musí však obsahovat garance v oblasti právních a mocenských nástrojů, a tedy mocnou a sofistikovanou ochranu ze strany společnosti. Zvláštním požadavkem na toto prostředí je etika komunikace veřejné moci s individuálním člověkem. Zahrňme tedy digitalizaci do rámce požadavků na etiku rozhodování, samozřejmě ze strany moci veřejné.⁸

V čem spatřovat „nebezpečnost“ digitalizace (a případně potažmo) při jejím užívání veřejnou mocí z hlediska etiky tohoto rozhodování. Moderní technologie v podobě elektronizace, digitalizace a zejména „umělá inteligence“ již dávno expandovaly z etapy efektivního účelového využívání, a to jak do náhrady (zastoupení) člověka, tak do možného ohrožení člověka schopnostmi, které mají výjimečně výjimeční geniové (rychlost rozhodování, komplexnost zhodnocení faktorů a systémové rozhodování, mechanizace forem rozhodování na základě užívaných vzorců apod.). Ale, co je horší – digitalizace odosobňuje „lidské“ vztahy, a to zejména vztahy úředníka a

⁷ Z hlediska aktuálních elektronizačních trendů se tedy aktuálně věnujeme, respektive spíše bereme v potaz: internet, práva k „datům“ a software, elektronické dokumenty (jako například elektronický podpis, elektronickou poštu, datové schránky, domény a doménová jména, pojetí informací ve veřejném prostoru.

⁸ Samozřejmě nastupuje otázka nejen etiky rozhodování, ale i zásadní problémy právní odpovědnosti (například ochrana spotřebitele při uzavírání smluv na internetu, ochrana osobních údajů apod., jakož i trestněprávní odpovědnost za kyberkriminalitu, srov. k tomu in: *Právo informačních technologií, ...*, tamtéž, s. 307 a násl., resp. 432 a násl., resp. s. 541 a násl.

soukromého žadatele. Tyto vztahy formalizuje, přenáší je do modelové (vzorové) symboliky, a navíc i zjednodušování.⁹

Přístup k digitalizaci sledujme tedy v jejích pozitivích a negativích. Modernizační výše uvedený vývoj a situace má (ostatně jako všechno spojené s elektronizací) určité dvě stránky:

- a) pozitivní, tedy očekávanou, plánovanou, programovanou, což znamená modernizaci rozhodovacích procesů, zrychlení rozhodování, racionalizaci pracovních sil a prostředí, menší počet úředníků apod.
- b) negativní, tedy spíše neočekávanou, sice monitorovanou, ale trpěnou, nebo i nekontrolovatelnou: počítačovou negramotnost, nepochopitelnost lakonických formulářových požadavků, složitost elektronických operací, v důsledcích i nebezpečí diskriminace lidí apod.

Řešením výše uvedených dilemat je tak zajištění určité rovnováhy mezi těmito stránkami. Předpokládejme tudíž, že tento požadavek apriorně směřuje k řešení především ze strany veřejné moci.

Do jaké veřejnoprávní oblasti právní úpravy je nutné (možné) zařadit digitalizaci jako součást mocenského rozhodování. Stavíme na takové hypotéze, že apriorně jde o účelovou technickou modernizaci jako akceleraci profesionalizace a racionalizace, a jejich dopadu na chování lidského faktoru. V postupném technologickém zjednodušování rozhodovacích procesů jde z hlediska práva zejména o zásadní vliv tohoto vývoje na administraci procesů, neboť:

- digitalizace i užití „umělé inteligence“ má společensky komunikační charakter vztahu moci veřejné a subjektů v zásadě zcela soukromých, tedy subjektů na jedné straně jménem veřejné moci rozhodovacích a subjektů, jejichž práva jsou předmětem rozhodování, na straně adresátů,
- společenským důsledkem tohoto vývoje je zesilování „vrchnostenského“ (nadřazenostního) charakteru veřejnoprávního rozhodování (administrativního typu),
- nastupuje tím však i problém, jak zvýšeně chránit člověka, zacházet s ním co nejšetrněji, srozumitelně a lidsky vysvětlovat od člověka očekávané chování,
- uplatňování digitalizace a aplikace AI má z hlediska subjektu užívajícího tyto způsoby převážně resortní, odvětvově ministerský charakter, včetně digitalizace i užití AI v oblasti justice,

Při zkoumání této problematiky je třeba se přednostně zabývat digitalizací veřejné správy a postavením soukromého subjektu vzhledem k dopadu jejích rozhodnutí.

⁹ K tomu zřejmě triviálním příkladem je nadužívání dotazníkové formulářové formy komunikace, která je případně i formálně omezována počtem slov, počtem řádků, a dokonce i počtem písmen (zkušenost autora tohoto článku ze současné formalizované komunikace při koncipování stížností k Evropskému soudu pro lidská práva, a to včetně jejího formálního vymezení „bodů“ jejího obsahu).

Stěžejní nasměrování našeho řešení stavíme na takové hypotéze, podle níž elektronizace včetně digitalizace veřejné správy, případně využívající umělou inteligenci, je schopna uvést soukromý subjekt (člověka zejména) do situace až ohrožující jeho přirozenoprávní svobodu. Potom je možné dospět k určitému i klíčovému názoru, jímž se konstatuje, že ve vývoji uvedených zkoumaných procesů je nutno trvale sledovat, zda se v jednotlivých a různorodých svým správným charakterem odvětvích veřejné správy zachovává lidský faktor. Je tím myšleno, zda přirozenoprávní osobnost a individuální osobitost lidí není natolik ovlivňována, potlačována, manipulována a podobně, že lze konstatovat až ohrožení udržitelnosti lidského faktoru. Je třeba to takto testovat právě na kontaktech veřejnoprávních rozhodovacích procesů, jejichž adresátem je člověk, občan, a to zejména při realizaci veřejných subjektivních práv, kdy soukromá osoba je obvykle návrhatelem k následné realizaci žádosti orgánem veřejné moci.

Tato udržitelnost lidského faktoru má zvláštní požadavky v prostředí rozhodování soudu. Týká se totiž nezastupitelnosti činitele, který rozhoduje o spravedlnosti a jejím užití v individuálních kauzách, nastupuje tedy otázka diskrece soudce, jeho objektivního a nestranného hodnocení sporu nebo viny, včetně spravedlivého rozhodnutí o sankci. To nevylučuje samozřejmě efektivní užití elektronických prostředků digitalizovaných zdrojů, servisních informací a názorů zprostředkovaných umělou inteligencí. Jedině justiční resort je oprávněn sféru nezastupitelnosti soudce řešit a hájit.

Při přístupu k řešení vztahu elektronizace-digitalizace-umělá inteligence zejména v komunikačním a rozhodovacím užívání veřejnou správou na straně jedné a soukromého subjektu (fyzické osoby) na straně druhé jako hraniční kritérium nastavujeme tedy základní lidská práva. Jde totiž o to, aby mnohočetné a ve formách velmi rozmanité elektronizační zpracování tohoto vztahu zachovalo jistou garanci, že podstata základního lidského práva nebude porušena natolik, že potlačí lidskou osobnost v její přirozenosti.¹⁰ V této souvislosti se naším testovacím kritériem stává konsolidované pojetí přirozenoprávnosti spočívající v kompozici lidských hodnot chráněných na bázi klíčového základního lidského práva, tedy práva na život. Dopady výše uvedené trojice tak sledujeme ve vztahu k dominantám jako jsou nedotknutelnost osoby, svoboda myšlení, svoboda lidského projevu, svoboda lidské činnosti a ochrana soukromí včetně rodinného života a rodinných vztahů.¹¹

S právem na život především souvisí princip nedotknutelnosti osoby. Když vyjdeme ze skutečnosti, že užití umělé inteligence v zásadě není schopno porušit fyzickou

¹⁰ Autor ve shodě s koncepcí autorů publikace, srov. in: *Právo informačních technologií, ..., tamtéž, s. 395 a násl., tomu blíže in: KLÍMA, K. Listina a její realizace v systému veřejného a nového soukromého práva.* Praha: Wolters Kluwer, 2014, ISBN 978-80-7478-647-1, s. 84 a násl.

¹¹ K evropskému pojetí základních lidských práv a svobod viz autor in: KLÍMA, K. *Ústavní právo srovnávací.* Praha: Metropolitan University Prague Press, Wolters Kluwer ČR, 2020, s. 107 a násl.

integritu člověka, jde o to, jakým způsobem může zasáhnout do integrity psychické, potažmo do roviny morální ochrany osobnosti, včetně rodinných vztahů a soukromí vůbec.

Nedílnou součástí přirozenoprávnosti člověka je svoboda myšlení. Svoboda myšlení je absolutní přirozené právo. To znamená, že je nedotknutelná ze strany jakéhokoli vnějšího subjektu včetně orgánů veřejné moci (správy). Jestliže ji tedy nelze omezit ani zákonem, je otázkou, čím a jak ji mohou atakovat požadavky zprostředkované digitalizačním kontaktem určitý názor omezující nebo dokonce vymezující až příkazující (například ve formulářích formulací otázek kapciózních či sugestivních). Digitalizovaná elektronická komunikace by neměla nahrazovat metody takzvaného detektoru lži.

Svoboda lidského projevu je založena tom, že vůle člověka se projeví v možnosti sdělit navenek myšlenku nebo její ztvárnění. Svoboda projevu je i svobodou neprojevovat se. Dotazníková forma zejména je totiž schopná k projevu nutit. Je možné diskutovat s umělou inteligencí? Určitě ano. Je schopna umělá inteligence pochopit, reagovat, připustit názor a následně jej zhodnotit, ba dokonce opravit (upravit) svůj názor? Zcela specifickou otázkou svobody lidského projevu je autorskoprávní ochrana, která analyzuje limity práva na svobodu projevu ve vztahu k umělé inteligenci.

Další důležitou problematikou je ochrana svobodné činnosti. Jakákoliv formulářová forma zintenzivňuje manipulativnost nestátního subjektu orgány veřejné správy. Jestliže je subjekt podle zákona povinen něco činit nebo se zdržet činností, tato povinnost nesmí být akcelerovaná nadbytečnými povinnostmi fakticky svobodnou činností, dále omezující činnostními povinnostmi. Důležitým aspektem digitalizace je ochrana soukromí, neboť každá forma elektronické komunikace je schopna vstupovat do soukromí. V souvislosti s výkonem veřejné správy, a tudíž veřejnoprávních funkcí, respektive i ze zákona povinné komunikace, navíc případně sankcionované ignoranci ze strany, adresáta vysloveně stresuje, případně zatěžuje finančně i poškozují.¹²

Elektronizace, digitalizace a umělá inteligence, a právo

Zásadní otázky jsou především spojeny s právní regulací systému umělé inteligence.¹³ Právní řád by především měl zachytit regulační nutnost ve vztahu k

¹² Systém takzvaných datových stránek měl nepochybně racionalizační charakter urychlující komunikaci ve veřejné správě, ale i svým způsobem byl „donucovací akcí“ *sui generis*. Elektronická komunikace určitě od adresátů vyžaduje i vlastnictví tiskárny třeba jen k osobní dokumentaci.

¹³ V tomto článku se nezabýváme umělou inteligencí jako produktem, který má nárok na registraci, a tudíž i právní ochranu. Ale předmětem naší pozornosti je umělá inteligence jako použitelný autonomní systém.

vývoji autonomních systémů, a to včetně rizik s tím spojených. To se také může projevit v určitých omezujících prvcích právní úpravy obsažených v právní regulaci. Obsahu právních norem je taktéž imanentní zakotvení právní odpovědnosti, která může nastoupit v užití jednotlivých těchto autonomních systémů.

Z pohledu práva a právní vědy je umělá inteligence velmi nesnadno uchopitelná. Není to snad jenom kvůli její univerzální využitelnosti a širokému uplatnění. Inteligentní systémy totiž dokážou fungovat relativně nezávisle na člověku, dokonce bez jeho dohledu a mají při svém rozhodování určitou míru autonomie. Lze vyvolat i pochybnost o tom, zda je možné spolehnout se na tyto systémy při řešení důležitých problémů. Relativní nepředvídatelnost, a tedy i snížená kontrola člověka nad těmito systémy je jedním z dalších důvodů, proč právo začalo umělou inteligenci zkoumat. I komplikovanost právního řádu a zejména jeho jednotlivých právních odvětví zdůvodňuje, proč aplikační otázky realizace jednotlivých odvětví tuto výzkumnou nutnost vyvolávají.

Problematika, umělé inteligence a směrů výzkumu a vývoje včetně jejího využívání představují jednu z aktuálních priorit Evropské unie. I Evropská unie vidí v umělé inteligenci ohromný potenciál, který je nutné a účelné využít. Hlavním dokumentem, který započal tento vývoj úvah a bádání o umělé inteligenci a autonomních robotech, bylo usnesení Evropského parlamentu ze dne 16. 2. 2017 s názvem „Občanskoprávní pravidla pro robotiku“. Evropský parlament v tomto dokumentu nastínil hlavní právní a etické problémy týkající se robotů a umělé inteligence, přičemž na prvním místě doporučil vytvořit obecně přijatelnou definici robota a umělé inteligence, která bude pružná a nebude bránit inovacím. Hlavním problémem, který vyplývá z celého usnesení je snaha poukázat na problematické momenty v přístupu k odpovědnosti ve vztahu k užívání umělé inteligence. Jde zejména pak o možnou ztrátu kontroly člověka na technologií, která se chová do jisté míry autonomně a nemůže být tak považována za pasivní nástroj, ale je vzhledem ke své schopnosti interakce s okolím spíše připodobňována k aktivnímu aktérovi.¹⁴ Autonomní systémy tohoto druhu jsou totiž schopny samostatně se učit a jsou tudíž nepředvídatelné. Nastupuje tak otázka, zda právní řád je schopen se vyrovnat s případy škod způsobených autonomními systémy.

Jaké jsou v současnosti možné směry užití umělé inteligence v právu? Jaké směry jsou v tomto smyslu zatím detekovány, respektive vyvolávány? Je všeobecně známo, že umělá inteligence je užitečná ve vyhledávání informací, jakož i pro analýzu a syntézu informací z judikatury. Odkazuje se na možnosti užití umělé inteligence při právní argumentaci. Nelze opomenout, že umělá inteligence je použitelná ve výuce práva pro simulaci právních problémů nebo při systémové analýze práva. Může umělá inteligence nahradit právníky a soudce? Je samozřejmě třeba se zabývat i užitím

¹⁴ K tomu srov. in: *Právo a umělá inteligence, ...*, tamtéž, s. 35.

umělé inteligence při zpracování právních informací, při přípravě právní argumentace při vytváření smluv a dalších dokumentů. Důležitou otázkou je kodifikace práva, plánování řešení soudních sporů, předcházení vzniku sporů a porušování práva. A samozřejmě i rozhodování v soudnictví, respektive při dalším vynucování práva.

Jakým způsobem nasměrovat právní regulaci umělé inteligence? Každá právní regulace totiž má tradičně určitý prvek statiky, respektive stability, včetně rigidity ve smyslu své předvídatelnosti, právní jistoty a také transparentnosti. Právní regulace by však měla mít i určitou vnitřní dynamiku, jež musí umožnit pružné reagování na existující poptávku po nové právní regulaci či její transformaci. Právo je v této souvislosti totiž velmi výrazně konfrontováno s rozvojem techniky a technologickým pokrokem. Úvahy o potřebnosti nové právní regulace by však měly být vedeny nejprve v rovině identifikace konkrétní potřeby která potvrdí do jaké míry dosavadní právní regulace postačuje.

Důležité pro odpovědné hledání relevantních řešení je především celkový interdisciplinární záběr, což znamená získat potřebnou znalost řady jiných relevantních technologických oborů, jako je kybernetika či informatika. Každopádně při aplikaci nových technologií je klíčovým vodítkem otázka ochrany, podpory a rozvoje pozitivních stránek těchto technologií, jakož i současné vytváření efektivních překážek a regulace všech jejích negativních důsledků pro společnost či jednotlivce. Je třeba zdůrazňovat zachování minimálních standardů existující míry právní ochrany adresáta (soukromoprávních osob) ve světle možných faktických důsledků aplikace konkrétní technologie v novém právním prostředí.

Pro každou novou právní úpravu zde totiž nastupuje důležitá otázka schopnosti práva, respektive nové právní regulace předvídat. Aktuálním právním problémem aplikace těchto nových zákonných ustanovení týkajících se digitalizace a nové inteligence je totiž určitá základní vlastnost autonomních systémů v podobě relativní či dokonce absolutní nezávislosti jejich fungování. Jde totiž o nezávislost na člověku včetně osob, jež tyto autonomní systémy vytvořily. V tomto kontextu lze hovořit o tom, že autonomní systém není z povahy věci naprogramován pouze k výkonu nějaké konkrétní činnosti, ale především k tomu, aby se výkon takové činnosti naučil, případně aby se dále samostatně to je bez další pomoci člověka kvalifikovaně při výkonu této činnosti konal, tvořil, a dokonce rozhodoval (a to s následnou závazností, včetně vynutitelnosti rozhodnutí). Autonomie takového systému tak nespočívá pouze v tom, že systém tyto činnosti vykonává automatizovaně ve smyslu své nezávislosti na člověku, ale především v tom, že zcela nezávisle na svém tvůrci člověku svůj program rozvíjí, vyvíjí, zlepšuje a podobně.¹⁵

¹⁵ Odkazujeme takto na velmi kvalifikovaný rozbor právního přístupu k problematice in: *Právo a umělá inteligence, ...*, tamtéž, s. 43 a násl.

Možné ústavněprávní dopady digitalizace a podstata ústavněprávní odpovědnosti

Jak již řečeno, z hlediska subjektivního jakákoliv digitalizace a elektronizace společenských procesů se týká zejména základních lidských práv, tedy (svým způsobem) nedotknutelnosti osobnosti, svobody myšlení, vstupuje do soukromých vztahů člověka, jeho osobnosti a důstojnosti. Digitalizace však vstupuje i do oblasti těch ústavně zaručených práv jako jsou (zejména): právo na práci, právo podnikat, právo na sociální zabezpečení, právo na ochranu zdraví, právo na vzdělání, právo na zdravé životní prostředí, právo na informace apod.

Je nutné, aby platný ústavní pořádek České republiky reagoval na elektronizační vývoj rozhodování státu a veřejné moci vůbec? Jak ústavně zaručená práva základní, tak jiná práva garantovaná českou Listinou základních práv a svobod, jsou práva, jejichž nezbytná konkretizace vytváří rozsáhlý legislativní prostor, který ve zde sledovaném vztahu veřejné moci a fyzických či právnických osob celkově dostatečně garantuje ochranu člověka.

Ústavní pořádek České republiky je stabilizovaným a obsahově sofistikovaným systémem. Různé elektronické modernizace veřejnoprávním rozhodovacích procesů by neměly dopadat na hmotněprávní podstatu ústavněprávní materie, zde zejména na obsah Listiny základních práv a svobod. Ústavu je třeba chránit před dobovými a účelovými textovými pokyny, zákazy i deklarativními zvoláními (typu jako: právo nosit zbraň, právo na platbu „cash“, apod.). Proto i název tohoto příspěvku je s otazníkem, a otazník je tudíž pochybností, a tedy pro potenciální úvahy *de constitutione ferenda* i jednoznačným odmítnutím jakýchkoliv účelových zásahů do ústavní materie.¹⁶

Digitalizace je v realizační fázi různorodá v odlišnosti rozhodování jednotlivých resortů. Digitalizace má sice globalizační charakter, ale vzhledem k jejímu dopadu na různá práva fyzických a právnických osob, je třeba její charakter sledovat v jednotlivých sférách veřejné správy. Nelze totiž nastavit vzhledem k výše uvedenému celospolečenskému problému generalizující kritéria hodnocení. Existuje různorodost kompetencí, typů rozhodování, zákonných požadavků pro různorodé rozhodování, obsahových požadavků pro obsah žádostí. Komunikační systém zejména veřejné moci administrativní se pohybuje mezi návrhy, žádostmi a stížnostmi soukromých subjektů na straně jedné, a dopady rozhodnutí, včetně sankcí na trajektorii zcela opačné.

¹⁶ Elektronické technologie jsou typem komunikace, které se v rovině ústavní materie zásadně i potažmo týkají prakticky všech lidských práv a svobod. V tom směru zřejmě neovlivňují rozsah jejich užívání a spíše jde o to, kdy by mohly soukromoprávnímu sektoru škodit, znesnadňovat jejich užívání a realizaci. Vzhledem k vývoji právní úpravy tak půjde spíše o otázky *de lege ferenda*, a tedy budoucího prováděcího zákonodárství.

Zvlášť sledovanou otázkou je digitalizace soudnictví a taktéž soudního rozhodování. Spisová soudní dokumentace je velmi komplikovaná záležitost založená především na záznamech protokolů svědeckých výpovědí, důkazů, argumentů z vyšetřovacích spisů a podobně. Spisová dokumentace se přirozeně liší podle typu soudního procesu (civilní, trestní, správní). Dále pak podle rozhodování věcí samé, respektive nebo v rozhodování ve věcech procesních a podobně. Navíc vzhledem k zásadnímu principu soudcovské nezávislosti je soudní proces plně v rukou soudu, senátu, soudce zpravodaje, samosoudce. Shromáždění potřebných podkladů má tudíž velmi subjektivní charakter z řady všeobecně dostupných poznatků odborně zkušenostního charakteru vyplývá, že digitalizace justice jako součást rozhodovacího procesu v zásadě neexistuje. Právo na spravedlivý proces však obsahuje nároky nejen na regulérní postup směřující k dosažení rozhodnutí (v soukromoprávním sporu, v obraně v trestním procesu, ve vztahu k rozhodnutí ve správním soudnictví a podobně). Toto v zásadě procesní právo neřeší výsledný efekt a sice objektivní spravedlnost. A k té se spravedlnost v konkrétní věci může (asi většinou) přibližovat. Spravedlnost v soudním rozhodování je totiž ad hoc, a tudíž vždy konkrétní a subjektivní, včetně pocitového dojmu žalobce. Je tak otázkou, kde je procesní limit digitalizace v rozhodování věcí samé, tedy kdy začíná být nezastupitelnou procesní zjištění, vyvozené konstatování, formulace materiální pravdy, nároků, potvrzení, usvědčení pachatele a podobně. Navíc, rozhodnutí soudu (soudce) má často stanovené sankční důsledky (ex lege, ze žaloby), polehčující či přitěžující okolnosti. V tom smyslu je osobitost soudce, odborná zkušenost, psychologická a další zcela nezastupitelná podpořená zásadami nestrannosti, kontradiktornosti a rovnosti zbraní a celkově tedy diskreční (úvahové) úlohy soudcovské.¹⁷

Evropsky v současné době pojímané právo na spravedlivý proces, tak podněcuje nezbytnost střežit spravedlnost finálního rozhodnutí a dovádí tak k možnému limitu racionální digitalizace soudního systému a soudního rozhodování, a tudíž i k nezastupitelnosti profesionálního lidského faktoru.

Zvláštním vztahem, jímž se hodláme zabývat, je vztah k umělé inteligence a autorské tvorby. Vycházíme z takové premisy, podle níž je umělá inteligence způsoben tvořivého myšlení, schopného rychlostí, metodologickou instruktivností nahrazovat lidské myšlení. Je zřejmě zatím potvrditelné, že úkol, respektive řešení závisí na

¹⁷ Nezastupitelná úloha soudce totiž spočívá ve výkonu spravedlnosti, přičemž tento výkon spravedlnosti chápeme širěji, než je pojímán v článku 6. Úmluvy o lidských právech a základních svobodách systému Rady Evropy. I judikatura Evropského soudu pro lidská práva rozvíjí koncept práva na spravedlivý proces jak právo „na proces bezvadný“, tedy dodržující principiální zásady soudního řízení, jakož i ze zákona vyplývající soudní postup (řízení). Pojetí spravedlivého rozhodnutí je obtížně definovatelné a musí mít vždy kauzálně konkrétní i subjektivně soudcovskou povahu, a to včetně precedenčního dosahu. K tomu autor v kapitole „Jurisdikce Evropského soudu pro lidská práva jako pramen evropské lidskoprávní ústavnosti“, in: *Ústavní právo srovnávací*, ..., tamtéž, s. 180.

formulaci otázky. A k úkolu, jež komunikační nositel tohoto pramenného druhu inteligence obdrží, je zřejmě podmiňující, že ke zpracování tohoto úkolu potřebuje přitom získávání informací potřebných k sumarizaci, k hodnocení, k dedukcím, k informacím.

V čem tedy spočívá pozitivum kreativity umělé inteligence?

- ve vyhledávání informací, v jejich syntetizaci, případně i hodnocení faktů,
- v komparaci vyhledaných informací dle stanovených kritérií, nároků a zadání,
- v možnostech formulovat hodnotící závěry, včetně výběru zákonných sankcí apod.,

Je zde zřejmě hodné otázky, zda je (bude) umělá inteligence schopna sama nastavovat hodnotící (testovací) kritéria, neboť ta musejí být součástí rozhodování. Určitě nevýhodou užití umělé inteligence je obtížná (i nemožná) identifikace autorství, ale i věrohodnosti názorů, závěrů apod.

Záver

Jaká možná veřejnoprávní řešení posuzovaného společenského problému? Digitalizace spojená případně s „umělou inteligencí“ je nezvratným, nezastavitelným procesem, jehož vývoj je z právního hlediska třeba monitorovat, vyhodnocovat, případně i do něho regulativně zasahovat. Vzhledem k tomu, že má komunikačně převážně resortní charakter, celospolečenská kontrola musí být specifikována směrem k jednotlivým resortům. K tomu vybrané příklady: přihlašování se na střední školy, vedení zdravotní dokumentace zdravotnickými zařízeními, rozhodování v jakémkoliv přestupkovém řízení, komunikace úřadů práce s veřejností, komunikace úřadů sociálního zabezpečení s veřejností, provoz systému veřejného pojištění apod. Zvláštní oblastí je komunikace obecních a městských úřadů v tzv. přenesené působnosti, a to například v oblasti matriční agendy, osobní občanského statutu, řidičských průkazů a jiných oprávnění, stavebního řízení, užívání energetických zdrojů, odpadového hospodářství, základního školství, středního školství apod. Vzhledem k tomu, že uvedený proces má globální společenský charakter, nastupuje tak nutnost i sofistikované parlamentní kontroly, typu speciální kontroly resortních výborů jim odpovídajících odvětví státní správy, neboť jediné parlamentní kontrola je schopna efektivního vstupu do rezortů.

Elektronizační pokrok bude mít vždy náskok. Přirozená rezistence člověka bude vždy existovat a je sociálně-psychologicky pochopitelná. Je samozřejmě otázkou, jaký myšlenkový styl nastavit vůči elektronickému progresu. Digitalizace je jako metoda poznatelná, její využití otevřené a nepředvídatelné ani ve výhodách, na natož pak v nevýhodách. Z teoretického hlediska tak jedna z možných metod je ochrana člověka v jeho přirozenoprávnosti. Jde totiž o to, aby aplikační a z hlediska veřejně mocenského užití elektronizace, digitalizace a umělá inteligence neohrožovaly

materiální rovinu zejména základních lidských práv. Reálná ochrana ze strany veřejné moci tak musí být aplikační, konkrétní a efektivní.

Zoznam použitej literatúry

1. KLÍMA, K. Listina a její realizace v systému veřejného a nového soukromého práva. Praha: Wolters Kluwer, 2014, ISBN 978-80-7478-647-1.
2. KLÍMA, K. Ústavní právo. 5. aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2016, ISBN 978-80-7380-606-4.
3. KLÍMA, K. Ústavní právo srovnávací. Praha: Metropolitan University Prague Press, Wolters Kluwer ČR, 2020, ISBN 978-80-7598-883-6.
4. KRAUSOVÁ, A. Status elektronické osoby v evropském právu v kontextu českého práva. *Právní rozhledy*, 2017, č.20.
5. POLČÁK, R. Internet a proměny práva. 1. vydání. Praha, Auditorium, 2012, ISBN 978-80-87284-22-3.
6. POLČÁK, R., HARAŠTA, J., STUPKA, V. Právní problémy kybernetické bezpečnosti. 1. vyd. Brno: Masarykova univerzita, 2016, ISBN 978-80-210-8426-1.
7. POLČÁK, R. Odpovědnost umělé inteligence a informační útvary bez právní subjektivity. *Bulletin advokacie*, 2018, č.11.
8. POLČÁK, R. a kol. Právo informačních technologií. Praha: Wolters Kluwer, 2018, ISBN 978-80-7598-045-8.
9. ŠTĚDRŮŇ, B. a kol. Prognostické metody a jejich aplikace Praha: C.H.Beck, 2012, ISBN 978-80-7179-174-4.
10. ŠTĚDRŮŇ, B. a kol. Právo a umělá inteligence. Plzeň: Aleš Čeněk, 2020, ISBN 978-80-7380-903-7.
11. ZELINKA, I. Umělá inteligence: hrozba nebo naděje. 1. vydání, Praha: BEN, 2003, ISBN 80-7300068-7.

Kontaktné údaje

prof. doc. JUDr. Karel Klíma, CSc., Dr. hab.
karel.klima@mup.cz
Katedra právních disciplín a veřejné správy
Metropolitní Univerzita v Praze

NEW TECHNOLOGIES AND RESPONSIBILITY FOR THEIR USE IN ARMED CONFLICT

Ľudmila Elbert¹

Abstrakt: Základom technologického pokroku sú inovácie využiteľné v ozbrojených konfliktoch. Nové technológie prinášajú veľké vojenské výhody, ako aj zlepšenie humanitárnej pomoci. Pri porušení pravidiel medzinárodného práva v čase ozbrojeného konfliktu v dôsledku použitia nových technológií však vzniká otázka zodpovednosti. O sobitne diskutovanou je otázka zodpovednosti za následky činností plne autonómnych zbraňových systémov či zbraňových systémov vybavených umelou inteligenciou schopných samostatne rozhodovať o výbere cieľa a jeho zásahu ozbrojenou silou. Súčasné pravidlá medzinárodného práva zakotvujú zodpovednosť štátu za protiprávne správanie, ako aj trestnoprávnu zodpovednosť jednotlivca, v čase ozbrojeného konfliktu kombatanťa a vojenského veliteľa, za páchanie zločinov podľa medzinárodného práva. Protiprávne správanie štátu, ako aj páchanie zločinov podľa medzinárodného práva, môže nastať tak v dôsledku použitia nových technológií, ako aj bez ich použitia. V oboch prípadoch preto ostáva zachovaná aplikácia pravidiel upravujúcich zodpovednosť štátu i trestnoprávnu zodpovednosť jednotlivca. Cieľom príspevku je vyvrátiť domnienku, že zodpovednosť za použitie nových technológií v čase ozbrojeného konfliktu sa nachádza v oblasti právneho vákua pre chýbajúcu explicitnú právnu úpravu.

Kľúčové slová: nové technológie, umelá inteligencia, autonómia, medzinárodné humanitárne právo, zodpovednosť

Abstract : Technological progress is based on innovations that can be used in armed conflicts. New technologies bring great military advantages as well as improvements in humanitarian aid. However, when international law is violated during armed conflict as a result of the deployment of new technologies, the question of responsibility arises. A particularly controversial issue is the question of responsibility for the consequences of the actions of fully autonomous weapon systems or weapon systems equipped with artificial intelligence capable of independently deciding on the selection of targets and their engagement by armed force. Current rules of international law establish

¹ Institute of International Law and European Law, Pavol Jozef Šafárik University in Košice, Faculty of Law

the responsibility of the state for wrongful acts, as well as the criminal responsibility of individuals, in times of armed conflict, combatants and military commanders, for committing crimes under international law. Wrongful acts conducted by the state, as well as the commission of crimes under international law, may occur if new technologies are deployed or not. In both cases, the application of the rules governing state responsibility and the criminal liability of individuals remains unchanged. The aim of this paper is to refute the assumption that responsibility for the deployment of new technologies in times of armed conflict is in a legal vacuum due to the lack of explicit legal regulation.

Keywords: new technologies, artificial intelligence, autonomy, international humanitarian law, responsibility

Introduction

During armed conflict, the rules of the law of armed conflict and international humanitarian law apply. Despite the fact that there is no explicit mention of new technologies among the applicable rules, this does not mean that their use remains in a legal vacuum. The existing rules are applicable to the use of any weapon, i.e., all means and methods of armed conflict and in any environment.² Efforts to enshrine a ban on new technologies with lethal effects have been unsuccessful, given the reluctance of states, the lack of consensus on the definition of these technologies, and the prevailing security and national interests in the current international community.

Based on existing rules of international humanitarian law, there are therefore a number of declarations, recommendations, and guidelines regarding the use of new technologies in times of armed conflict, with the aim of helping states and other entities to maintain compliance with international law in times of armed conflict when using new technologies. In order to promote the responsible use of new, especially digital, technologies in accordance with international humanitarian law, the International Committee of the Red Cross (hereinafter also referred to as "ICRC")

² Confirmed by F.A Barnaby, head of the Humanitarian Affairs and Policy Unit, ICRC Regional Delegation for East Asia, delivered at the Fourth Soochow International Humanitarian Forum, Suzhou, China, September 5, 2025: ICRC: Artificial Intelligence, Ethics and Armed Conflict, 8 September 2025 [online]. Available at: <https://www.icrc.org/en/article/artificial-intelligence-ethics-and-armed-conflict> (Accessed: 26 September 2025).

prepared the Policy on Artificial Intelligence in 2024.³ It approaches artificial intelligence on the basis of values founded on the fundamental principles of international humanitarian law (humanity, impartiality, neutrality, and independence). It sets out guiding principles for the use of artificial intelligence: 1. proportionality, 2. precaution, 3. "do no harm" & safety, 4. security & transparency, 5. "explainability" & responsibility, 6. accountability. These principles are in line with main focus of ICRC in relation with the AI which is responsible and human-centred approach when using AI.

The aim of this paper is therefore to highlight the existing rules of responsibility for violations of international law in times of armed conflict, the applicability of which remains valid in relation to new technologies. In the first chapter, we briefly attempt to explain the new technologies used in times of armed conflict. In the second and third chapters, by interpretation *a maiori ad minus*, we then point out the still relevant rules of responsibility for their violation as a result of the use of new technologies by interpreting the rules of international humanitarian law and international criminal law.

New technologies in armed conflict

The term "new technologies" is relatively vague. From a legal perspective, there is no definition of new technologies in general or in specific terms. New technologies are those tools that are new for a given period in human history, whether it be crossbows or the use of gunpowder and firearms. Currently, we consider new technologies used in times of armed conflict to be those that have autonomy or artificial intelligence in decisive functions. However, among new technologies we also include, for example, quantum technologies and digitization in general.

From the perspective of autonomy, autonomous weapon systems are relatively well known. However, their definition is quite broad. The ICRC⁴ considers autonomous weapon systems to be weapons that select and apply force against targets without human involvement. The person deciding on their deployment does not select or know the specific target or the exact time and/or place of the final use of force, as the weapon is activated based on the recognition of some form of military means or movement of a person. Human Rights Watch, on the other hand, categorizes

³ ICRC: Building a Responsible Humanitarian Approach: The ICRC's Policy on Artificial Intelligence, 18 November 2024 [online]. Available at: <https://www.icrc.org/en/publication/building-responsible-humanitarian-approach-icrcs-policy-artificial-intelligence> (Accessed: 26 September 2025).

⁴ ICRC: What you need to know about autonomous weapons, 2022 [online]. Available at: <https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons> (Accessed: 26 September 2025).

autonomous weapon systems into three categories⁵ according to the degree of human involvement in their activities. The first category is human-controlled weapons, i.e., systems that can select targets and strike them with force only under human guidance (*human-in-the-loop weapons*). The second category is human-controlled weapons, i.e., systems that can select targets and engage them with force under the control of a human operator who can take control of their actions (*human-on-the-loop weapons*). The third category is fully autonomous weapons, i.e., systems that are capable of selecting targets and striking them with force without human involvement (*human-out-of-the-loop weapons*).

Furthermore, the NATO Cooperative Center of Excellence for Cyber Defense also offers a categorization of weapons using autonomy or artificial intelligence in the armed forces.⁶ It distinguishes between autonomy and artificial intelligence due to inconsistent terminology and the fact that autonomy, as the ability of a machine to perform a task without human intervention, may or may not include features of artificial intelligence technology. It therefore distinguishes between systems that belong to the first and second waves of artificial intelligence. The first wave of artificial intelligence includes systems based on decision-making based on written rules (assumption – result). They do not consider the situation in which they find themselves and cannot learn from their own experiences (autonomous systems).

The second wave of artificial intelligence includes systems capable of performing specific tasks, trained on large amounts of information and using machine learning and deep learning (artificial intelligence together with control systems and decision support systems). In this sense, autonomy is somewhat confusingly presented as a level of artificial intelligence, while at other times it is considered a feature of the system that is distinct from artificial intelligence.

However, experts from the Geneva Academy and the ICRC⁷ point out a fundamental difference between autonomy and artificial intelligence. The fundamental legal challenge in the case of autonomous weapon systems is the fact that it is not a human being but the autonomous system itself that selects the specific target or the time

⁵ HRW: Losing Humanity: The Case against Killer Robots, 2012, p. 1-3 [online]. Available at: <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots> (Accessed: 26 September 2025).

⁶ NATO CCDCOE: M. Gray, A. Ertan: Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment, Tallinn 2021 [online]. Available at: https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf (Accessed: 26 September 2025).

⁷ ICRC and Geneva Academy: Expert Consultation Report on AI and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts, Geneva, ICRC, March 2024, p. 9 [online]. Available at: <https://www.geneva-academy.ch/joomlatools-files/docman-files/Artificial%20Intelligence%20And%20Related%20Technologies%20In%20Military%20Decision-Making.pdf> (Accessed: 26 September 2025).

and place of the attack. On the other hand, the fundamental challenge in the use of artificial intelligence in decision support systems remains to ensure that the system assists and supports, rather than hinders or replaces, human decision-making on the use of force in accordance with international humanitarian law. This means that decision support processes using artificial intelligence preserve human decision-making functions, as is the case with conventional weapons. Therefore, the question of responsibility especially in relation to autonomous weapon systems is debatable.

State responsibility for damage caused by new technologies in armed conflict

The use of new technologies in armed conflict can represent a significant military advantage. Besides the fact that the new technologies can represent the new tool for improving compliance with humanitarian law,⁸ from the perspective of the law of armed conflict and international humanitarian law, new technologies represent a method or means of armed conflict. Although the rules of international humanitarian law and law of armed conflicts do not explicitly mention any of the new technologies,⁹ when using new technologies, it is necessary to consider whether they fall into any of the categories of prohibited weapons.

Article 35(2) of Additional Protocol I,¹⁰ which also reflects customary law, prohibits the use of weapons and methods of warfare that, by their nature, cause excessive injury or unnecessary suffering. In light of the principle of humanity, it is necessary to examine, in particular, the effects of weapons on combatants in order to ensure a balance between military effectiveness on the one hand and the expected injury or suffering of persons on the other.

Consequently, Article 51(4) of Protocol I prohibits weapons that, by their nature, strike military objectives and civilians or civilian objects without distinction.¹¹ In

⁸ See: MARGULIERS, Peter: The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance. In: JENSEN, Eric T. – ALCALA, Ronald T.P. (eds.): The impact of emerging technologies on the law of armed conflict. Lieber Studies, volume 2. New York: Oxford University Press, 2019, p. 147 – 174. ISBN 978-01-909-1532-2.

⁹ KLUČKA, Ján: Medzinárodné právo verejné (Všeobecná a osobitná časť). 4. vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2022, p. 417 et seq. ISBN 978-80-571-0525-1.

¹⁰ Oznámenie Federálneho ministerstva zahraničných vecí č. 168/1991 Zb. o viazanosti Českej a Slovenskej Federatívnej republiky Dodatkovými protokolmi I a II k Ženevským dohovorom z 12. augusta 1949 o ochrane obetí medzinárodných ozbrojených konfliktov a konfliktov nemajúcich medzinárodný charakter, prijatých v Ženeve 8. júna 1977.

¹¹ For the current challenges for principle of distinction see: HATHAWAY, Oona A., KHAN, Azmat & REVKIN, Mara R.: The Dangerous Rise of “Dual-Use” Objects in War. In: The Yale Law Journal, vol. 134, no. 8 (2025), p. 2645 – 2750. [online]. Available at: <https://www.yalelawjournal.org/article/the-dangerous-rise-of-dual-use-objects-in-war> (Accessed: 26 September 2025).

accordance with the principle of distinction, it is therefore necessary to examine¹² whether a weapon is capable of targeting military objects and whether its effects can be limited in accordance with international humanitarian law.

The third category of prohibited methods and means of warfare, according to Article 35(3) of DP I, are those whose purpose is to cause or which may be expected to cause widespread, long-term, and serious damage to the environment. This prohibition is reinforced by Article 55(1) of DP I, which prohibits the use of methods or means of warfare intended to cause such damage to the environment or likely to cause such damage that would endanger the health or survival of the population.¹³

The general application in relation to new technologies has the Martens clause, contained in the Fourth Hague Convention of 1907. It provides protection to members of the armed forces and the civilian population in cases not expressly covered by any of the conventions of international humanitarian law or law of armed conflict.¹⁴ Under the Martens Clause, the population and the warring parties remain under the protection and influence of the principles of international law as they are evident from the customs of civilized nations, the laws of humanity, and the requirements of public conscience. The Martens Clause responds to rapid technological progress, which specific international legal regulations have not kept pace with.¹⁵

But not every new technology must inherently constitute a violation of the rules of international humanitarian law. It is always necessary to examine the effects of its use and consider possible violations of IHL. Such obligation of states to conduct legal research on new weapons, means, or methods of warfare and their compliance with the rules of international law in their study, development, acquisition, or introduction is enshrined in Article 36 of DP I. The obligation to conduct a legal review is followed by the obligation to take preventive measures, namely to verify 1. whether the target of the attack is a permitted military object, 2. whether collateral damage to civilian life or property is minimized, 3. and the attack must not be launched if it is expected that collateral damage to civilian life or property would exceed the anticipated specific and direct military advantage.

¹² ICRC: Rule 12. Definition of Indiscriminate Attacks [online]. Available at: <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule12> (Accessed: 26 September 2025).

¹³ JANKUV, Juraj - LANTAJOVÁ, Dagmar - BLAŠKOVIČ, Kristián - BUCHTA, Tomáš - ARBET, Daniel: Medzinárodné právo verejné. Druhá časť. 1. vydanie. Plzeň: Aleš Čeněk, 2016. p. 330 et seq. ISBN 978-80-738-0597-5.

¹⁴ GASSER, Hans-Peter: International Humanitarian Law. In: WOLFRUM, Rüdiger (ed.): The Max Planck Encyclopedia of Public International Law. Oxford: Oxford University Press, 2012. ISBN 978-0-19-929168-7.

¹⁵ See: KLUČKA, Ján: Medzinárodné právo, umelá inteligencia a vice versa. In: Časopis pro právní vědu a praxi, vol. 29, no. 3 (2021), p. 551- 572. ISSN: 1210-9126.

If a state violates these obligations in connection with the use of new technology in armed conflict, it is responsible for internationally wrongful acts.¹⁶ The rules governing this type of state responsibility are customary in nature. These rules were drawn up on the basis of the work of the UN International Law Commission. They are contained in the Draft Articles on the Responsibility of States for Internationally Wrongful Acts.¹⁷ In terms of the emergence of responsibility for internationally wrongful acts of a state, in addition to the wrongful act itself, i.e. the failure to fulfill an international obligation, referred to as the objective element of responsibility, it is also necessary to fulfill a second condition, namely the attribution of this conduct to the state, referred to as the subjective element of responsibility for the internationally wrongful acts of a state. From a practical point of view, however, it is relatively difficult to attribute unlawful conduct to a specific entity at a time of armed conflict.

According to the judgement of the International Court of Justice in the Nicaragua case,¹⁸ it is possible to abstract the condition for establishing state responsibility for unlawful acts, referred to as the principle of effective control. Applying the principle to the use of new technologies, the decisive factor is the degree of dependence and the degree of state control over the entity using the new technology at the time of armed conflict. The state is considered a collective entity acting through entities other than state authorities or legal¹⁹ or natural persons authorized to act on behalf of the state. In this regard, however, one cannot overlook the concept of *ultra vires*,²⁰ whereby the state is held responsible for the actions of a person who has exceeded their powers or even acted contrary to them, with the aim of protecting a third party who is unaware of the extent of the powers of the person acting on behalf of the state.

¹⁶ POŠIVÁKOVÁ, Ľudmila: Zodpovednosť štátov v medzinárodnom práve. In: STUDIA IURIDICA Cassoviensia, vol. 3, no. 1 (2015), p. 100 – 127. ISSN 1339-3995.

¹⁷ ILC: Draft articles on responsibility of States for international wrongful acts, Report of the International Law Commission, Yearbook of the International Law Commission: 2001, vol. II, (A/56/10). General Assembly resolution: 56/83. Responsibility of States for internationally wrongful acts [online]. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/No1477/97/PDF/No147797.pdf?OpenElement> (Accessed: 26 September 2025).

¹⁸ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I. C. J. Reports, 1986, p. 14, pp. 109 – 116 [online]. Available at: <https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> (Accessed: 26 September 2025).

¹⁹ See: MAREČEK, Lukáš: Criminal Liability of Legal Persons under International Law – Retrospection and Current Status. In: The Lawyer Quarterly, vol. 10, no. 4 (2020), p. 413 – 425. ISSN: 1805-840X [online]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/427> (Accessed: 26 September 2025).

²⁰ Article 7, Draft articles on responsibility of States for international wrongful acts.

Therefore, the claim by states or other entities that international law does not contain rules governing the use of new technologies in times of armed conflict is incorrect. Based on Common Article 1 of the Geneva Conventions,²¹ states have undertaken to uphold the Geneva Conventions and ensure their observance in all circumstances, including outside times of armed conflict. They can fulfill this obligation by providing adequate education on the rules of international humanitarian law or by adopting appropriate domestic legislation. The state therefore bears a kind of "meta-responsibility" for compliance with the rules of international humanitarian law.

However, the attribution of responsibility to the state for unlawful acts does not preclude the attribution of responsibility to an individual²² who has committed crimes in violation of the rules of international law.

Individual responsibility for damage caused by new technologies in armed conflict

The international community believes that human responsibility should be maintained for damage caused by the use of new technologies.²³ In times of armed conflict, this concerns the criminal responsibility of combatants and military commanders for committing war crimes as a result of the use of new technologies. Classically, therefore, in order to establish individual criminal responsibility, the subjective element of the crime (*mens rea*) (intent and knowledge) and the objective element of the crime (characteristics and form of commission of the crime) must be fulfilled. In the context of new technologies, the most problematic aspect seems to be the subjective element, i.e., proving the intent to violate the rules of international law in connection with the use of new technologies and the knowledge that the violation will occur.

²¹ Vyhláška ministra zahraničných vecí č. 65/1954 Zb. o Ženevských dohovoroch zo dňa 12. augusta 1949 na ochranu obetí vojny.

²² Article 58, Draft articles on responsibility of States for international wrongful acts.

²³ CCW: Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System (CCW/MSP/2019/9). [online]. Available at: https://ccdcoe.org/uploads/2020/02/UN-191213_CCW-MSP-Final-report-Annex-III_Guiding-Principles-affirmed-by-GGE.pdf (Accessed: 26 September 2025); AI Action Summit: Paris Declaration on Maintaining Human Control in AI enabled Weapon Systems, 11 February 2025 [online]. Available at: <https://www.elysee.fr/emmanuel-macron/2025/02/11/paris-declaration-on-maintaining-human-control-in-ai-enabled-weapon-systems> (Accessed: 26 September 2025); Report of the Secretary-General UN: Artificial intelligence in the military domain and its implications for international peace and security (A/80/78), 5 June 2025 [online]. Available at: <https://documents.un.org/doc/undoc/gen/n25/107/66/pdf/n2510766.pdf> (Accessed: 26 September 2025).

The fundamental definition of crimes under international law is contained in the Rome Statute of the International Criminal Court.²⁴ However, when determining the responsibility of individuals for crimes under international law, military commanders cannot be overlooked, in accordance with Article 28 of the Rome Statute and Articles 86 and 87 of Additional Protocol I. A military commander or other person effectively acting as a military commander is criminally responsible for crimes committed by armed forces under their effective command and control as a result of their failure to exercise proper control. The use of new technologies in armed conflict is decided by the military commander, so the fact that the unlawful conduct was committed by a subordinate does not relieve their superiors of criminal or disciplinary responsibility. Their responsibility arises if they knew or had information that would have enabled them, under the circumstances existing at the time, to conclude that the subordinate had committed or was about to commit such a violation and did not take all possible measures within their power to prevent or prosecute the violation²⁵ (Article 86(2) 2 of Additional Protocol I).

The application of these rules of international criminal law and international humanitarian law is relatively clear in cases where humans retain control over new technologies used in armed conflict,²⁶ specifically with regard to the decisive functions of weapons, such as selecting targets and deciding on their engagement by armed force. What remains as a matter of debate is the responsibility of specific individuals and the applicability of the rules of international criminal law and international humanitarian law in relation to violations of international law in connection with the use of new technologies over which humans have no control.²⁷ These are fully autonomous weapon systems or weapon systems equipped with artificial intelligence, whose actions are unpredictable and without the possibility of human intervention in the decisive functions of target selection and engagement. However, even in this case, in accordance with the rules of international humanitarian law, the responsibility of the individual who knew or should have

²⁴ Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 333/2002 Z. z. o prijatí Rímskeho štatútu Medzinárodného trestného súdu.

²⁵ See: ELBERT, Ľudmila: Medzinárodnoprávny úvod k používaniu autonómnych zbraňových systémov. Praha: Leges, 2022, p. 83. ISBN 978-80-7502-663-7.

²⁶ GREIPL, Anna Rosalie: Data-driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility? In: Journal of International Criminal Justice, vol. 21, no. 5 (2023), p. 1097–1118. ISSN 1478-1395 [online]. Available at: <https://academic.oup.com/jicj/article/21/5/1097/7259630?searchresult=1> (Accessed: 26 September 2025).

²⁷ HALAJOVÁ, Ľudmila: Individual Criminal Responsibility for War Crimes Resulting from the Use of Autonomous Weapons Systems. In: The Lawer Quarterly, vol. 10, no. 2 (2020), p. 130 – 152. ISSN: 1805-840X [online]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/402> (Accessed: 26 September 2025).

known about the unpredictability of the actions of new technologies at the time of deciding to use them should be maintained.²⁸

Conclusion

The most effective way to deal with the unpredictability of new technologies when targeting military targets is to maintain direct human control over critical system functions or shared control, where critical functions remain in the hands of a person capable of intervening in a timely manner in the event of a possible violation of international humanitarian law. The person should have sufficient time to select and approve one of the options proposed by the system, to take control of the system and return control to it, or to deactivate the system before the system begins its attack on the target.

When considering responsibility for damage caused by the use of new technologies in armed conflict, it is possible to consider parallel responsibility—state, commander, combatant. Although establishing responsibility is relatively difficult, we cannot say that it is impossible to apply the current rules governing state responsibility or the criminal responsibility of individuals. In order to hold the state responsible for wrongful acts in connection with violations of international humanitarian law and the law of armed conflict, it is necessary to fulfill the basic elements of responsibility, namely breach of obligation and its attribution to the state. Since the state acts through other entities (state authorities or persons authorized to act on behalf of the state), effective state control over the acting entity is of particular importance. In the future, it would be possible to consider the advantages of legally establishing the strict liability of the state for activities that use new technologies, in particular autonomy, which can become unpredictable, following the model of liability for damage caused by space objects.²⁹ However, given national and security interests and the need to maintain military advantage, as well as the lack of consensus on the terminology used, we consider considerations of possible agreement on the establishment of this type of liability to be utopian.

On the other hand, in order to hold individuals responsible, it is similarly necessary to comply with existing legislation. Although this leaves it up to the military commander and combatant to decide whether new technology used in armed conflict complies

²⁸ For more opinions see: GAETA, Paola: Who Acts When Autonomous Weapons Strike? The Act Requirement for Individual Criminal Responsibility and State Responsibility. In: *Journal of International Criminal Justice*, vol. 21, no. 5 (2023), p. 1033–1055. ISSN 1478-1395 [online]. Available at: <https://academic.oup.com/jicj/article/21/5/1033/7591635?searchresult=1> (Accessed: 26 September 2025).

²⁹ Vyhláška ministra zahraničných vecí č. 58/1977 Zb. o Dohovore o medzinárodnej zodpovednosti za škody spôsobené kozmickými objektmi. For more: POŠIVÁKOVÁ, Ľ. *Zodpovednosť štátov v medzinárodnom práve*, p. 119.

with the rules of international humanitarian law and law of armed conflict, it also establishes the responsibility of the commander or combatant for violating these rules as a result of using new technologies. The use of new technologies in armed conflict is therefore not a lawless area. The use of new technologies does not necessarily require new, specific legislation. At least, it is sufficient for states to comply with existing legislation based on the principle of humanity.

Bibliography

1. ELBERT, Ľudmila: Medzinárodnoprávny úvod k používaniu autonómnych zbraňových systémov. Praha: Leges, 2022. 109 p. ISBN 978-80-7502-663-7.
2. GAETA, Paola: Who Acts When Autonomous Weapons Strike? The Act Requirement for Individual Criminal Responsibility and State Responsibility. In: Journal of International Criminal Justice, vol. 21, no. 5 (2023), p. 1033–1055. ISSN 1478-1395.
3. GASSER, Hans-Peter: International Humanitarian Law. In: WOLFRUM, Rüdiger (ed.): The Max Planck Encyclopedia of Public International Law. Oxford: Oxford University Press, 2012. ISBN 978-0-19-929168-7.
4. GREIPL, Anna Rosalie: Data-driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility? In: Journal of International Criminal Justice, vol. 21, no. 5 (2023), p. 1097–1118. ISSN 1478-1395.
5. HALAJOVÁ, Ľudmila: Individual Criminal Responsibility for War Crimes Resulting from the Use of Autonomous Weapons Systems. In: The Lawer Quaterly, vol. 10, no.2 (2020), p. 130 – 152. ISSN: 1805-840X.
6. HATHAWAY, Oona A., KHAN, Azmat & REVKIN, Mara R.: The Dangerous Rise of “Dual-Use” Objects in War. In: The Yale Law Journal, vol. 134 , no. 8 (2025), p. 2645 – 2750. ISSN 0044-0094.
7. HRW: Losing Humanity: The Case against Killer Robots, 2012, p. 1-3 [online]. Available at: <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots> (Accessed: 26 September 2025).
8. ICRC: Artificial Intelligence, Ethics and Armed Conflict, 8 September 2025 [online]. Available at: <https://www.icrc.org/en/article/artificial-intelligence-ethics-and-armed-conflict> (Accessed: 26 September 2025).
9. ICRC: Building a Responsible Humanitarian Approach: The ICRC’s Policy on Artificial Intelligence, 18 November 2024 [online]. Available at: <https://www.icrc.org/en/publication/building-responsible-humanitarian-approach-icrcs-policy-artificial-intelligence> (Accessed: 26 September 2025).
10. ICRC: Rule 12. Definition of Indiscriminate Attacks [online]. Available at: <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule12> (Accessed: 26 September 2025).

11. ICRC: What you need to know about autonomous weapons, 2022 [online]. Available at: <https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons> (Accessed: 26 September 2025).
12. ICRC and Geneva Academy: Expert Consultation Report on AI and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts, Geneva, ICRC, March 2024, p. 9 [online]. Available at: <https://www.geneva-academy.ch/joomlatools-files/docman-files/Artificial%20Intelligence%20And%20Related%20Technologies%20In%20Military%20Decision-Making.pdf> (Accessed: 26 September 2025).
13. ILC: Draft articles on responsibility of States for international wrongful acts, Report of the International Law Commission, Yearbook of the International Law Commission: 2001, vol. II, (A/56/10).
14. JANKUV, Juraj - LANTAJOVÁ, Dagmar - BLAŠKOVIČ, Kristián - BUCHTA, Tomáš - ARBET, Daniel: Medzinárodné právo verejné. Druhá časť. 1. vydanie. Plzeň: Aleš Čeněk, 2016. 464 p. ISBN 978-80-738-0597-5.
15. KLUČKA, Ján: Medzinárodné právo, umelá inteligencia a vice versa. In: Časopis pro právní vědu a praxi, vol. 29, no. 3 (2021), p. 551- 572. ISSN: 1210-9126.
16. KLUČKA, Ján: Medzinárodné právo verejné (Všeobecná a osobitná časť). 4 vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2022, 536 p. ISBN 978-80-571-0525-1.
17. MAREČEK, Lukáš: Criminal Liability of Legal Persons under International Law – Retrospection and Current Status. In: The Lawyer Quarterly, vol. 10, no. 4 (2020), p. 413 –425. ISSN: 1805-840X.
18. MARGULIERS, Peter: The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance. In: JENSEN, Eric T. – ALCALA, Ronald T.P. (eds.): The impact of emerging technologies on the law of armed conflict. Lieber Studies, volume 2. New York: Oxford University Press, 2019, 389 p. ISBN 978-01-909-1532-2.
19. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, I. C. J. Reports, 1986, p. 14, pp. 109 – 116.
20. NATO CCDCOE: M. Gray, A. Ertan: Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment, Tallinn 2021 [online]. Available at: https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf (Accessed: 26 September 2025).
21. Oznámenie Federálneho ministerstva zahraničných vecí č. 168/1991 Zb. o viazanosti Českej a Slovenskej Federatívnej republiky Dodatkovými protokolmi I a II k Ženevským dohovorom z 12. augusta 1949 o ochrane obetí medzinárodných ozbrojených konfliktov a konfliktov nemajúcich medzinárodný charakter, prijatých v Ženeve 8. júna 1977.

22. Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 333/2002 Z. z. o prijatí Rímskeho štatútu Medzinárodného trestného súdu.
23. POŠIVÁKOVÁ, Ľudmila: Zodpovednosť štátov v medzinárodnom práve. In: STUDIA IURIDICA Cassoviensia, vol. 3, no. 1 (2015), p. 100 – 127. ISSN 1339-3995.
24. Vyhláška ministra zahraničných vecí č. 65/1954 Zb. o Ženevských dohovoroch zo dňa 12. augusta 1949 na ochranu obetí vojny.
25. Vyhláška ministra zahraničných vecí č. 58/1977 Zb. o Dohovore o medzinárodnej zodpovednosti za škody spôsobené kozmickými objektmi.

Contact details

JUDr. Ľudmila Elbert, PhD.

ludmila.elbert@upjs.sk

Institute of International law and European law, Pavol Jozef Šafárik University,
Faculty of Law

PRÁVNA POMOC VO SVETE HALUCINÁCIÍ

LEGAL AID IN THE WORLD OF HALLUCINATIONS

Boris Balog¹

Abstrakt: Právo na právnu pomoc znamená zabezpečenie nielen kvalifikovanej, s odbornou starostlivosťou poskytovanej právnej pomoci, ale aj dostupnej právnej pomoci. Dostupnosť pritom nie je iba kategória finančná, resp. nákladová, ale aj časová a technická. Čo ak sa tým najlacnejším a najrýchlejším a tým najdostupnejším poskytovateľom pomoci v núdzi, tým, na koho sa osoby obracajú a s kým sa radia, stáva AI, ktorá si „právo“ vymýšľa? Príspevok sa venuje zodpovednosti za škodu spôsobenú vymyslenými informáciami, ktorá poskytne umelá inteligencia. Na základe súčasnej miery právnej regulácie umelej inteligencie skúma, či existuje osobitná úprava zodpovednosti za škodu spôsobenú umelou inteligenciou, alebo, či je táto zodpovednosť iba v režime všeobecnej civilnej zodpovednosti za škodu. V tejto súvislosti sa príspevok zameriava na reguláciu umelej inteligencie na vnútornom trhu Európskej únie, a to Aktom o umelej inteligencii a pripravovanou smernicou o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii. Príspevok tiež poukazuje na to, že Akt o umelej inteligencii doteraz nebol v Slovenskej republike riadne implementovaný a vykonávací zákon k nemu chýba.

Kľúčové slová: právna pomoc, zodpovednosť, umelá inteligencia, vymyslené právo

Abstract: The right to legal aid means ensuring not only qualified legal aid provided with professional care but also accessible legal aid. Accessibility is not just a financial or cost-related category, but also a temporal and technical one. What if the cheapest, fastest, and hence most accessible provider of aid in need, the one to whom individuals turn and consult, becomes AI that 'makes up' the 'law'? This article deals with liability for damage caused by fabricated information provided by artificial intelligence. Based on the current level of legal regulation of artificial intelligence, it examines whether there is a special regulation of liability for damage caused by the Artificial Intelligence, or whether this liability is only subject to the general civil liability regime. In this

¹ Katedra ústavného práva, Právnická fakulta Univerzity Komenského v Bratislave.

context, the article focuses on the regulation of artificial intelligence within the internal market of the European Union, namely through the Artificial Intelligence Act and the prepared proposal for an EU directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). The article also points out that the Artificial Intelligence Act has not yet been properly implemented in the Slovak Republic and implementing legislation is missing.

Keywords: Legal aid, liability, artificial intelligence, AI, invented law

Úvod

Bez toho, aby som mal štatistické údaje, možno len na základe intuície, si dovoľím vysloviť, že ak sa človek ocitne v nejakej nepriaznivej životnej situácii, jej riešenie profesionálnou, či štátom autorizovanou osobou sa dostane na druhé a nižšie miesto. Na prvom mieste človek siahne po hľadaní riešenia pomocou umelej inteligencie (ďalej aj „AI“). Až potom vyhľadá lekára alebo advokáta, či inú osobu poskytujúcu profesionálne služby určené na riešenie rôznych životných situácií.

Ústava Slovenskej republiky (ďalej len „ústava“) v čl. 47 ods. 2 zaručuje každému právo na právnu pomoc v konaní pred súdmi, inými štátnymi orgánmi alebo orgánmi verejnej správy od začiatku konania, a to za podmienok ustanovených zákonom. Toto právo znamená v minimálnej formálnej rovine povinnosť orgánov uvedených v čl. 47 ods. 2 ústavy nebrániť účastníkovi, aby využíval právnu pomoc² a v materiálnej rovine tohto práva znamená aj povinnosť štátu, pozitívny záväzok štátu, vytvoriť podmienky pre dostupnosť právnej pomoci.³

Hlavným účelom čl. 47 ods. 2 ústavy je zabezpečenie toho, aby právo na súdnu a inú právnu ochranu nebolo slovami ESĽP len „*teoretické a iluzórne*“, ale aj „*praktické a účinné*“.⁴

Toto právo je ústavne naviazané na podmienku „*za podmienok ustanovených zákonom*“, čo by pri formálnom výklade znamenalo, že to nie je dotknutá osoba, ale zákonodarca, ktorý rozhoduje o tom, kedy sa osoba ocitá v situácii, že je odkázaná na právnu pomoc a za akých podmienok jej bude poskytnutá. Predstava zákonodarcu sa ale nemusí prekrývať so subjektívnym pocitom potreby právnej pomoci, ktorú môže mať osoba rozdielnu v rôznych situáciách, v ktorých sa ocitá ona sama a aj rozdielnu v porovnaní s inými osobami.

² Nález Ústavného súdu Slovenskej republiky sp. zn. II. ÚS 78/03.

³ Uznesenie Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 58/2001.

⁴ OROSZ, Ladislav - SVÁK, Ján a kol.: Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s. r. o., 2021, s. 629.

Právo na právnu pomoc sa v niektorých prípadoch mení na povinnosť právneho zastúpenia z dôvodu vecnej alebo právnej zložitosti niektorých konaní. Má sa tým prostredníctvom profesionálneho právneho zastúpenia dosiahnuť efektívna ochrana práv dotknutej osoby.

Teoretickým dôvodom povinného právneho zastúpenia pred Ústavným súdom Slovenskej republiky je skutočnosť, že Ústavný súd Slovenskej republiky skúma porušenie práva. Pri civilnom spore žalobca striktné vzaté nemusí označiť hmotné právo, ale označí skutok a súd nachádza právo. Z tohto dôvodu pred civilným súdom nie je povinné právne zastúpenie, okrem dovolania, ktoré sa týka otázok právnych. Pri správnom súdnictve je potrebné označiť právne dôvody nezákonnosti, a pretože laik právo nepozná, zákon v zásade vyžaduje povinné právne zastúpenie.⁵

Ústavný súd Slovenskej republiky chápe právo na právnu pomoc tak, že „*právo na právnu pomoc sa priznáva vždy, keď sa rozhoduje o právnom postavení oprávnenej osoby*“.⁶ Súčasne musí ísť o právnu pomoc, ktorá je dostupná, resp. z opaku, nemôže byť pre osobu z rôznych dôvodov nedostupná. Je príznačné, že z pohľadu minulého storočia, ale iste aj s významom v súčasnosti, sa dostupnosť chápala najmä z hľadiska sociálnej situácie dotknutej osoby.⁷

Dnes chápeme dostupnosť širšie, ako iba z hľadiska finančnej schopnosti získať nejakú službu. Dnes ide najmä o dostupnosť časovú. Dostupné je to, čo je možné získať časovo veľmi rýchlo, najlepšie okamžite a bez vynaloženia väčšieho úsilia, či námahy, teda „*on-line*“.

Doba vyhľadávania pomoci a rád na internete, na webových prehliadačoch, sa pomaly končí. Prečo sa spoliehať na pomoc a rady od googlu, keď je tu niečo, čo už v názve obsahuje slovo „*inteligencia*“? Inteligencia je totiž o. i. definovaná aj ako schopnosť riešiť problémy. Prečo by sa preto osoba v problémoch zdravotných, finančných, či právnych, neobrátila o pomoc a radu na inteligenciu, ktorá z podstaty musí mať schopnosť riešiť problémy. A ak nie je dostupná iná forma inteligencie, tá umelá je dnes už dostupná všade a okamžite.

Som si vedomý toho, že AI neposkytuje právnu pomoc v jej formálnom chápaní. O právnej pomoci na účely čl. 47 ods. 2 ústavy, či čl. 6 ods. 3 písm. c) Dohovoru o ochrane ľudských práv a základných slobôd možno hovoriť, len ak je poskytovaná štátom autorizovanými osobami.

Za uplatnenie práva na právnu pomoc nemožno označiť zastupovanie ktorýmkoľvek občanom spôsobilým na právne úkony alebo zastúpenie „*iným zástupcom*“ podľa §

⁵ MACEJKOVÁ, Iveta a kol.: Zákon o Ústavnom súde Slovenskej republiky. Komentár. 1. vydanie. Bratislava: C.H.Beck, 2020, s. 157.

⁶ Nález Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 248/07.

⁷ K tomu rozhodnutie EŠLP vo veci *Airey proti Írsku*.

16 ods. 1 Správneho poriadku. Právnu pomoc môže poskytnúť iba osoba s právnickým vzdelaním.⁸ O to menej to môže byť AI.

V prípade AI možno hovoriť o odpovediach na položené zadania, ktoré sa týkajú rôznych životných situácií, ktoré by si inak vyžiadali formálnu právnu pomoc.

Predmetom predloženého príspevku je v tejto súvislosti zamyslenie sa nad tým, aká je situácia človeka, ktorý vyhľadáva u AI pomoc, akej poskytovanie je inak vyhradené iba štátom autorizovanej osobe, z hľadiska zodpovednosti za škodu spôsobenú nesprávne poskytnutou radou alebo pomocou AI v dôsledku toho, že si poskytnuté informácie vymyslela.

Možnosti AI

Mnohé veci sú v dnešnom svete oveľa dostupnejšie a bezprostrednejšie ako tomu bolo v minulosti. Ide aj o oblasť tvorivej činnosti. Obrazy vznikajú za pár sekúnd,⁹ eposy sú napísané skôr, než by zaschol atrament, a symfónie sa rodia bez jediného zakašľania v koncertnej sále. Pre napísanie literárneho diela už nie je potrebná samota a ani múza a pre napísanie odborného diela už nie je potrebný výskum.

AI je odvetvie informatiky, ktoré sa zaoberá vytváraním algoritmov a systémov schopných vykonávať úlohy, ktoré by obvykle vyžadovali ľudskú inteligenciu.¹⁰ Všetko toto má potenciál nahradiť AI a jej schopnosti vytvárať výstupy akéhokoľvek druhu na základe zadanej požiadavky, teda promptu.

Jazykové modely AI (Large Language Model – LLM) ako ChatGPT, Gemini, Claude, Grok, či Copilot fungujú ako AI asistenti. Ich úlohou je na základe promptu odpovedať, a to či už formou textu, obrázku, tabuľky, hlasu, videa alebo ich kombináciami. AI asistenti sú reaktívny, čo znamená, že konajú na základe zadania. Ak zadanie dostanú, je ich úlohou zadanie spracovať a poskytnúť výsledok zodpovedajúci zadaniu. Platí pritom, že kvalita a presnosť promptu priamo ovplyvňuje kvalitu odpovedí reaktívnych jazykových modelov AI.

Schopnosťou AI je najmä učenie, rozpoznávanie vzorcov, práca s jazykom a riešenie problémov rôzneho druhu. Základom pre spracovanie jej výstupov je tzv. *machine learning*, teda strojové učenie,¹¹ pri ktorom sa stroj učí na základe prístupu k systému

⁸ DRGONEC, Ján: Ústava Slovenskej republiky. Teória a prax. Bratislava: C.H.Beck, 2015, s. 901.

⁹ Vo veci č. k. 10 C 13/ 2023–16 Mestský súd v Prahe konštatoval nemožnosť AI byť autorom diela, pretože autorské právo je priznané iba fyzickým osobám byť. Súd poukázal na fakt, že pri vytvorení obrázku AI nedochádza k vytvoreniu jedinečného výsledku tvorivej ľudskej činnosti a tým nie je možné výtvor AI považovať za autorské dielo. Súd vyjadril názor týkajúci sa zadávania promptu, ktorý by mohol byť považovaný za námet, ktorý ale tiež ako taký nie je autorským dielom.

¹⁰ ŠTĚDRŮŇ, Bohumír – JAŠEK, Roman – SVÍTEK, Miroslav a kol.: Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024, s. 13.

¹¹ K tomu bližšie – MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 2 – 9.

rozličných dát, na ktorých sa učí riešiť danú úlohu. S vyriešením každej ďalšej úlohy dochádza k ďalšiemu učeniu AI a tým k zlepšeniu jej výkonu a tým zvýšeniu kvality výstupov. Podstatným prvkom *machine learning* je ľudská spätná väzba hodnotiaca výstupy AI. Ide teda o následnú reakciu človeka na poskytnutú odpoveď AI. V tomto smere treba uviesť, že nie je bežne možné preniknúť do tajov fungovania algoritmov umelej inteligencie, nie je bežne možné vykonať jej kontrolu, respektíve zistiť, či umelá inteligencia má k dispozícii všetky potrebné dáta.¹²

Na *machine learning* nadväzuje systém neurónových sietí, ktorý je nadstavbou nad schopnosťou učiť sa, teda *deep learning*.¹³ To umožňuje samostatné získavanie príznakov z neštruktúrovaných vstupov ako sú obrázky, zvukové nahrávky či texty, pričom nepotrebuje manuálne definovanie pravidiel pre extrakciu relevantných rysov. Je tak možné, že na rovnaký prompt bude AI reagovať inak v čase, a to v dôsledku rozšírenia poznatkov, s ktorými bude pri spracovaní zadania pracovať.

Ak bude zadanie smerovať k hľadaniu odpovede na právne riešenie nejakej životnej situácie, AI na to odpovie. Odpoveď bude závisieť tak od zadaného promptu, ale aj od miery „naučenia“ AI v oblasti zadania. Súčasťou odpovede AI ale nebude žiadny disclaimer v zmysle, že AI nie je poskytovateľom právnej pomoci a jej odpoveď nie je možné pokladať za právnu radu. Úlohou AI asistenta nie je poučovať alebo vystríhať zadávateľa promptu, ale poskytnúť mu naň odpoveď, a to za každých okolností, dokonca aj vtedy, ak by si ju AI mala vymyslieť.

Fenomén halucinovania AI je všeobecne známy. Miera halucinácie AI v oblasti práva môže byť na úrovni medzi 58 % až 82 %, čo predstavuje obrovské riziko jej používania bez ľudskej kontroly a spätnej väzby.¹⁴ Podľa štúdie vedcov z Univerzity v Stanforde z januára 2024 sú právne halucinácie alarmujúco časté, vyskytujú sa v 69 % prípadov s ChatGPT 3.5 a 88 % prípadov s Llama 2, keď sa týmto modelom kladú konkrétne, overiteľné otázky o náhodných prípadoch amerického federálneho súdu.¹⁵ Každý používateľ jazykového modelu AI by mal k jeho výstupom pristupovať s primeranou mierou obozretnosti a s vedomím, že tento výsledok nemusí zodpovedať skutočnosti.

¹² DANIHLÍK, Tomáš: Některé etické aspekty používání umělé inteligence při odůvodňování soudních rozhodnutí. In: *Jurisprudence* č. 1/2025, s. 44.

¹³ K tomu bližšie – MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: *Právo a umelá inteligencia*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 10 – 13.

¹⁴ K tomu štúdia s údajmi o halucinovaní AI v práve z USA z roku 2024 „*Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive*“ dostupná na: [Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive | Stanford HAI](#).

¹⁵ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: *Právo a umelá inteligencia*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 27.

Halucinácia AI je presvedčivo znejúca odpoveď, ktorá však nie je pravdivá. Ide najmä o vymyslený text, fakt, údaj, informáciu alebo zdroj. Jazykové modely AI, ktoré si vymýšľajú tým generujú nesprávne informácie.

Odpoveď postavená na fikcii je pre AI prijateľnejšia ako priznanie, že odpoveď nepozná. Cieľom jazykových modelov AI nie je rozumieť realite, poznať fakty a na ich základe hovoriť pravdu, ale na základe predchádzajúceho kontextu predpokladať s vysokou mierou pravdepodobnosti ďalšie slovo. Ak AI nepozná odpoveď, ponúkne ako odpoveď niečo, čo pre ňu s najvyššou mierou pravdepodobnosti bude správna odpoveď, pretože to AI štatisticky bude dávať zmysel. AI kľúčovo hodnotí štatistickú pravdepodobnosť výskytu nejakého výroku a nie jeho obsahovú pravdivosť. Odpoveď AI bude znieť presvedčivo, aj ak by nebola správna, pretože skutočný obsahový rozdiel medzi faktom a presvedčivo znejúcou fikciou AI nepozná. Základom fungovania jazykového modelu AI je algoritmická podstata AI ako technológie, ktoré nefunguje na rozumovej sémantike, ale na umelom vytváraní textov.

Halucinácie produkujú výstupy generatívnej AI, ktoré môžu byť zavádzajúce a dokonca viesť k rizikám v reálnom živote s potenciálne nebezpečnými následkami pre človeka, jeho život, zdravie, či majetok.

Čiastočným riešením halucinovania AI je obmedzenie zdrojov na vytváranie odpovedí na prompty, a to z konkrétnych zadaných dokumentov alebo informačných zdrojov. Môže ísť napríklad o elektronickú zbierku zákonov, zbierky súdnych rozhodnutí, či odbornej literatúry. V takom prípade by AI mala citovať skutočné zdroje napríklad právnej úpravy a riziko halucinovania spočívajúce vo vytváraní vlastných „zákonov“ sa znižuje.

Príčinou chybného fungovania AI vedúceho k jej halucinovaniu sú nesprávne údaje, s ktorými pracuje. Kvalita údajov sa môže hodnotiť na základe viacerých kritérií:

- prístupnosť - miera, do akej sú informácie dostupné, alebo ľahko a rýchlo získateľné,
- množstvo informácií - miera, do akej je objem informácií primeraný pre danú úlohu,
- kompletnosť - rozsah, do ktorého informácie majú dostatočnú šírku a hĺbku pre danú úlohu,
- konzistencia - rozsah, do ktorého sú informácie prezentované s rovnakým obsahom naprieč viacerými systémami a platformami,
- bezchybovosť - rozsah, do ktorého sú informácie správne a spoľahlivé, a miera zhody medzi hodnotou dát (alebo súborom hodnôt) a zdrojom, o ktorom sa predpokladá, že je správny,
- relevancia - rozsah, do ktorého sú informácie relevantné pre príslušné procesy.

Človek v núdzi sa v snahe získať rýchlo, jednoducho a bezplatne právnu radu obráti na AI. Tá mu v každom prípade poskytne odpoveď. Nepredpokladám, že by sa AI obrátil niekto, kto sa práve vrátil od advokáta, s ktorým sa o riešení svojej situácie poradil. Predpokladám skôr opak. Následné konanie dotknutej osoby podľa

odpovede/rady AI môže tejto osobe spôsobiť ešte vážnejšie negatívne dôsledky, či dopady, než mala na začiatku, možno až také, ktoré ani následnou profesionálnou právnou pomocou už nebude možné vyriešiť.

S odpoveďou, že za takúto situáciu si môže dotknutá osoba sama, sa neuspokojíme a pokúsime sa nájsť odpoveď na otázku, kto a či vôbec by bol za takúto situáciu zodpovedný z hľadiska spôsobenej škody. Nepôjde tak o zodpovednosť trestnoprávnu.¹⁶

Zrekapitulujem východiskové „červené kontrolky“ pri používaní AI, ktoré by mali v prvom rade zabrániť tomu, aby takáto situácia nenastala.

1. AI asistent odpovie iba na zadanie. Čím je presnosť a kvalita zadania vyššia, tým je aj odpoveď AI presnejšia a kvalitnejšia. Formulovaniu zadania je preto potrebné venovať náležitú pozornosť.

2. Výstup AI je potrebné brať s rezervou. AI môže byť príliš sebavedomá vo svojich odpovediach, čo vedie k prezentovaniu nepravdivých informácií s vysokou istotou a presvedčivosťou.

3. Nie je možné očakávať žiadne upozornenie na to, že odpoveď môže byť nesprávna. Pri vedomí týchto východiskových bodov je potrebné odpoveď AI na riešenie nejakej životnej situácie vnímať aj v kontexte toho, že jej odpoveď môže byť postavená na vymyslených informáciách. Predmetom tohto výmyslu, halucinácie AI, môže byť celý zákon, jeho nejaké ustanovenie, súdne rozhodnutie,¹⁷ či napr. komentár k nim. Výstupom AI bude pritom texte, ktorý bude nielen obsahovo znieť hodnoverne a presvedčivo, ale bude aj formálne spĺňať požiadavky, či náležitosti, ktoré sa od príslušného výstupu vyžadujú.

Iste, text vytvorený AI nie je zákon, či právna norma. Napriek tomu, že AI by im iste poskytla náležitú formu a aj presvedčivé znenie, právo materiálne a právny predpis formálne to nebude.

¹⁶ K trestnoprávnej zodpovednosti vo vzťahu k umelej inteligencii viac – VOJTUŠ, František – KORDÍK, Marek – DRAŽOVÁ, Petra: Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia. In: Právnik, 6/2023, s. 549 – 570.

Dostupné na: [5_DISKUSE_Vojtus et al_549-570_6_2023.pdf](#).

¹⁷ Známe sú najmä prípady z USA, kedy advokáti používali rôzne vymyslené argumenty a boli za aj súdom potrestaní. Z najnovších možno spomenúť prípad Gauthier v. Goodyear Tire & Rubber Co, U.S. District Court for the Eastern District of Texas, No. 1:23-CV-00281, v ktorom tejto súd potrestal právnikov odporcu za citovanie vymyslených súdnych rozhodnutí tým, že ich vylúčil z konania a ich správanie nahlásil advokátskej komore.

Z nedávnej minulosti sú známe prípady, kedy federálny sudca v Manhattane v júni 2023 pokutoval dvoch newyorských právnikov sumou 5 000 dolárov za citovanie prípadov, ktoré vymyslela AI. Iný federálny sudca v New Yorku zvažoval uloženie sankcií v prípade týkajúcom sa Michaela Cohena, bývalého právnik a poradcu Donalda Trumpa, ktorý uviedol, že omylom dal svojmu vlastnému právnikovi falošné odkazy na prípady, ktoré právnik predložil v Cohenovom trestnom prípade týkajúcom sa daní a financovania kampane.

Každý študent práva už po prvom ročníku bakalárskeho stupňa štúdiu vie, že znakmi právnej normy je, že

- je spojená s autoritou štátu,
- je univerzálna a
- má štátom ustanovenú alebo uznanú formu.¹⁸

Právnik, ktorý používa AI si to musí uvedomovať a tak aj pristupovať k výsledkom vytvoreným AI a ich obsah overovať v oficiálnych/úradných zbierkach. Čo ak ho ale formálne a obsahovo perfektne znejúca odpoveď AI presvedčí natoľko, že si ju neoverí? A ak to neurobí právnik, ako možno očakávať, že tak bude postupovať neprávnik?

Regulácia AI

Používanie AI je dnes prirodzenou súčasťou súkromného, ale aj pracovného života mnohých ľudí, a to aj pri rizikách, ktoré používanie AI prináša. Za ideálny stav by som pokladal, ak by používanie AI bolo spojené s verejnou osvetou zameranou na bezpečné a zodpovedné používanie AI, ale aj s integráciou používania AI do vzdelávania. Tým by sa už od školských lavíc študenti učili používať AI bezpečne a zodpovedne a nebolo by to ponechané na živelný prístup k jej používaniu, ktorý môže vzťah k AI od počiatku deformovať.

Právna úprava používania AI vo vysokoškolskom prostredí smeruje k tomu, aby „vysoké školy vytvárali podmienky na tvorivý, bezpečný a zodpovedný prístup k využívaniu AI ako nástroja podpory vzdelávania, výskumnej, vývojovej alebo umeleckej a ďalšej tvorivej činnosti. Využívanie AI ale musí byť súlade so zásadami transparentnosti, etiky, akademickej integrity, ochrany práv duševného vlastníctva a ďalších práv“. ¹⁹ Absolvent vysokej školy by mal vedieť s AI narábať zodpovedne a tým sa vyhnúť situácii, že by spôsobil škodu inej osobe z dôvodu postupu podľa výstupu AI založenom na halucinácii.

Spoločnosť postavená na formálnych písaných pravidlách správania si ale s osvetou a vzdelávaním nevystačí, alebo nechce vystačiť, a potrebuje aj formálnu reguláciu spoločenských vzťahoch postavenú na právnych pravidlách správania sa.

Samotná regulácia AI nie je účelom, ale prostriedkom.²⁰ Regulácia predstavuje prostriedok aj na zabránenie vzniku škody vymyslenými informáciami AI, ale najmä na riešenie situácie poškodeného, ak prevencia zlyhala.

¹⁸ KROŠLÁK, Daniel - BALOG, Boris - SURMAJOVÁ, Žaneta: Teória štátu a práva. 1. vydanie. Bratislava: Wolters Kluwer, 2020, s. 170.

¹⁹ Vládný návrh zákona o vysokých školách a o zmene a doplnení niektorých zákonov (vysokoškolský zákon), tlač 924, § 8, dostupné na: <https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=10418>.

²⁰ ANDRAŠKO, Jozef a kol.: Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021, s. 288.

Vo vzťahu k AI platí, že izolované národné riešenia nemôžu postačovať na riešenie nadnárodných nekalých praktík vykonávaných algoritmami AI, regulačné výzvy by sa mali riešiť na najvyššej možnej normatívnej úrovni, a to na základe spoločných hodnôt európskej tradície ľudských práv.²¹

Používanie AI na vnútornom trhu Európskej únie je regulované Aktom o umelej inteligencii.²²

Účelom Aktu o umelej inteligencii je zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca, najmä pokiaľ ide o vývoj, uvádzanie na trh, uvádzanie do prevádzky a používanie systémov umelej inteligencie v Európskej únii v súlade s jej hodnotami, podporovať zavádzanie dôveryhodnej AI sústredenej na človeka a zároveň zaistiť vysokú úroveň ochrany zdravia, bezpečnosti a základných práv zakotvených v Charte základných práv Európskej únie, vrátane ochrany demokracie, právneho štátu a životného prostredia, chrániť pred škodlivými účinkami systémov AI v Európskej únii a podporovať inovácie.²³

Ak skúmame Akt o umelej inteligencii z pohľadu ochrany používateľa, ktorý by vyhľadával právnu pomoc alebo radu a riadil by sa ňou bez potrebnej miery opatrnosti, čím by si na základe vymyslených údajov v odpovedi spôsobil škodu, môžeme sa zamerať na tie ustanovenia, ktorých účelom je ochrana používateľov pred zakázanými praktikami využívajúcimi AI.

Podľa čl. 5 ods. 1 písm. a) Aktu o umelej inteligencii sa zakazuje uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, ktorý využíva podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citelne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčini, že prijmú rozhodnutie, ktoré by inak neprijali, a to spôsobom, ktorý tejto osobe, inej osobe alebo skupine osôb spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu.

Zakazujú sa najmä manipulatívne techniky, ktoré sa môžu použiť na presviedčanie osôb, aby sa správali neželaným spôsobom, alebo na ich zavádzanie nabádaním

²¹ MARTINI, Mario: Regulating Artificial Intelligence – How to De-Mystify the Alchemy of Code. In: EBERS, Martin – NAVAS, Susana: Algorithms and Law. Cambridge University Press. 2020, s. 39. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3458261.

²² Nariadenie Európskeho Parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

Predložený príspevok sa nevenuje tomuto nariadeniu ako takému, ale iba v rozsahu skúmania zodpovednosti za škodu spôsobenú AI.

²³ Akt o umelej inteligencii, recitál (1), dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=OJ:L_202401689.

na rozhodnutia spôsobom, ktorý narúša a oslabuje ich samostatnosť, rozhodovacie schopnosti a slobodnú voľbu.

Vyššie uvedené ustanovenia Aktu o umelej inteligencii treba považovať za nevyhnutnú právnu reakciu na hrozby, ktoré predstavujú niektoré systémy umelej inteligencie pre duševné súkromie a kognitívnu slobodu, ktoré zostávajú jadrom súčasných výziev pre ľudskú dôstojnosť.²⁴

Za nedodržanie zákazov praktík využívajúcich AI uvedených v čl. 5 Aktu o umelej inteligencii sa ukladajú správne pokuty až do výšky 35 000 000 eur, alebo ak je páchatelom podnik, až do výšky 7 % jeho celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia.

V záujme posilnenia ochrany používateľov modelov AI sa v čl. 50 ods. 1 Aktu o umelej inteligencii stanovuje povinnosť v oblasti transparentnosti pre poskytovateľov a nasadzujúce subjekty určitých systémov AI spočívajúca v tom, aby poskytovatelia zabezpečili, aby systémy AI určené na priamu interakciu s fyzickými osobami boli dizajnované a vyvinuté tak, aby boli dotknuté fyzické osoby informované o tom, že interagujú so systémom AI, pokiaľ to nie je zrejmé z hľadiska fyzickej osoby, ktorá je primerane informovaná, pozorná a obozretná, pričom sa prihliada na okolnosti a kontext používania.

Napokon je potrebné zmieniť aj nástroj ochrany, ktorý dáva Akt o umelej inteligencii fyzickým osobám a právnickým osobám v čl. 85, a to právo podať sťažnosť orgánu dohľadu nad trhom. Bez toho, aby boli dotknuté iné správne alebo súdne prostriedky nápravy, každá fyzická osoba alebo právnická osoba, ktorá má dôvody domnievať sa, že došlo k porušeniu ustanovení aktu o umelej inteligencii, môže podať sťažnosť príslušnému orgánu dohľadu nad trhom.

Keďže Akt o umelej inteligencii je nariadenie, vzhľadom na jeho vlastnosti nie je prípustná jeho transpozícia vnútroštátnym právnym predpisom, ale vyžaduje sa jeho vnútroštátna implementácia a vykonávanie. To predpokladá prijatie právnej úpravy iba v rozsahu zabezpečenia riadneho uplatňovania tohto nariadenia.

Na národnej úrovni je potrebné legislatívne upraviť najmä inštitucionálne zabezpečenie dohľadu nad trhom v oblasti umelej inteligencie - t.j. určiť príslušné vnútroštátne orgány pre výkon dohľadu nad trhom pri využívaní najmä vysokorizikových systémov AI a ich kompetencie, jednotné kontaktné miesto, notifikujúci orgán a tiež podmienky zriadenia regulačného experimentálneho prostredia. Rovnako je potrebné ustanoviť právomoci vnútroštátneho orgánu

²⁴ DIÁZ GONZÁLEZ, Gustavo Manuel: Prohibited Artificial Intelligence Practices. In: HUERGO LORA, Alejandro (Ed.): The EU Regulation on Artificial Intelligence: A Commentary. Milano: Wolters Kluwer Italia S.r.L., 2025, s. 41.

dohľadu nad trhom, ukladanie sankcií a zakotviť povinnosť súčinnosti medzi orgánmi dohľadu nad trhom.²⁵

Čo to znamená vo vzťahu k zodpovednosti za škodu spôsobenú chybnou radou AI na základe vymysleného obsahu? Akt o umelej inteligencii zodpovednosť za škodu nerieši. Ide iba o všeobecnú, resp. klasickú administratívno-právnu zodpovednosť poskytovateľov a nasadzujúce subjekty za porušenie povinností uložených Aktom o umelej inteligencii.

Ak by sa aj dopustili konania, ktoré je Aktom o umelej inteligencii zakázané, napr. by účelovo manipulatívnu alebo klamlivou technikou ovplyvnili správanie nejakej osoby, mohla by voči nim byť vyvodená zodpovednosť, a to aj na základe sťažnosti dotknutej osoby za porušenie Aktu o umelej inteligencii a uložená pokuta. Táto pokuta by ale predstavovala vyvodenie zodpovednosti za porušenie Aktu o umelej inteligencii orgánom dohľadu nad trhom, ale nie náhradu spôsobenej škody.

Špecifická situácia právnej pomoci, či poskytovania právnej rady AI a zodpovednosť za spôsobenú škodu predmetom úpravy Aktu o umelej inteligencii nie je.²⁶

Musíme sa tak uspokojiť so všeobecnou úpravou občianskoprávnej zodpovednosti za škodu. Dnes by to bol primárne § 420 Občianskeho zákonníka, podľa ktorého každý zodpovedá za škodu, ktorú spôsobil porušením právnej povinnosti, pričom tejto zodpovednosti sa zbaví len, ak preukáže, že škodu nezavinil.

Tradičný model zodpovednosti počíta s pôvodcom škody ako fyzickou alebo právnickou osobou, avšak pri AI môže byť príčinná súvislosť medzi konaním človeka a výsledkom algoritmu komplexná a nepriamo sprostredkovaná.²⁷ To vnáša vysokú mieru neistoty pri určovaní zodpovednej osoby za spôsobenú škodu. Je zodpovednou osobou prevádzkovateľ²⁸ alebo je to samotná AI, či jazykový model AI.

Otázky zodpovednosti umelej inteligencie sú viac ako len „komplikované“ nakoľko spochybňujú naše tradičné vnímanie jednotlivých právnych oblastí.²⁹

To, že ide o vážnu tému, ktorá je rozširovaním používania AI stále viac akútnejšia si uvedomuje aj Európska únia, ktorá po Akte o umelej inteligencii prichádza s ďalšou legislatívnou iniciatívou, a to na práve na úseku zodpovednosti za umelú inteligenciu. Ide o návrh smernice Európskeho parlamentu a Rady o prispôbení pravidiel

²⁵ V čase odovzdania príspevku takýto predpis v Slovenskej republike prijatý nebol.

²⁶ V prípade profesionálneho poskytovania právnych služieb právny poriadok vyžaduje povinné poistenie zodpovednosti za škody, čo predstavuje ochranu advokáta alebo notára a istotu osoby, ktorej poskytuje právnu službu, ak by tejto osobe bola spôsobená škoda.

²⁷ RUŽIČKOVÁ, Valéria (Ed.): Umelá inteligencia z pohľadu práva. Košice: Univerzita Pavla Šafárika, Právnická fakulta, 2021.

²⁸ Čl. 3 bod 8 Aktu o umelej inteligencii - prevádzkovateľom môže byť poskytovateľ, výrobca výrobku, nasadzujúci subjekt, splnomocnený zástupca, dovozca alebo distribútor.

²⁹ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 117.

mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu).³⁰

Návrh smernice o zodpovednosti za umelú inteligenciu vychádza z toho, že vnútroštátne pravidlá zodpovednosti nie sú vhodné na riešenie nárokov na náhradu škody spôsobenej produktmi a službami založenými na AI. Osobitné vlastnosti AI, akými sú zložitosť, autonómia a neprehľadnosť môžu poškodeným sťažovať alebo neúmerne predražovať určenie zodpovednej osoby a úspešné uplatnenie nároku na náhradu škody.

V návrhu smernice sa osobám, ktoré požadujú náhradu škody, sa umožňuje získať informácie o vysokorizikových systémoch umelej inteligencie, ktoré sa majú zaznamenávať/dokumentovať podľa Aktu o umelej inteligencii. Okrem toho sa poskytnú vyvrátiteľné domnienky osobám, ktoré požadujú náhradu škody spôsobenej systémami AI, zmiernenie dôkazného bremena a šancu uspieť s opodstatnenými nárokmi na náhradu škody.

Smernica vychádza z toho, že pre poškodených môže byť náročné preukázať príčinnú súvislosť medzi škodou a výstupom systému umelej inteligencie alebo nevytvorením výstupu systému umelej inteligencie, ktorý viedol k vzniku príslušnej škody. Preto sa navrhuje vyvrátiteľná domnienka príčinnej súvislosti týkajúca sa tejto príčinnej súvislosti. Takáto domnienka predstavuje najmenej zatažujúce opatrenie na riešenie potreby spravodlivého odškodnenia obete.

Aj v prípade smernice o zodpovednosti za umelú inteligenciu by išlo iba o úpravu všeobecnej občianskoprávnej zodpovednosti umelej inteligencii, nie špecificky v oblasti právnej pomoci alebo právnych rád, pričom aj táto právna úprava, keďže bude vyjadrená vo forme smernice, bude následne podliehať transpozícii v jednotlivých členských štátoch Európskej únie.

Záver

Na prvý pohľad by sa mohlo zdať, že umelá inteligencia potláča ľudskú kreativitu. Ak je AI schopná v krátkom okamihu vytvoriť niečo, čo by človeku inak trvalo dlhý čas a ani by to možno nebol schopný vytvoriť, tak prečo sa o to vôbec pokúšať. Jazykové modely využívajúce umelú inteligenciu odbremeňujú ľudí od potreby rozmýšľať nad riešením mnohých situácií a ponúkajú ľahko dostupné riešenia.

Zastávam laický názor, že AI nie je hrozbou pre ľudskú kreativitu. Práve naopak, AI je pre ľudskú kreativitu tým silným impulzom. AI a jej možnosti nás totiž nútia prehodnocovať mnohé známe a zaužívané spôsoby náhľadu na spoločnosť, na javy

³⁰ Návrh smernice dostupný na: eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52022PCo496&from=EN.

V čase predloženia príspevku ešte smernica nebola schválená.

v nej a na riešenie situácií, ktoré sa v nej objavujú. AI je nepriateľom stereotypu, v ktorom spoločnosť žije a ktorý je hlavnou príčinou potlačania ľudskej kreativity.

V názve príspevku hovorím o svete halucinácií. Iste, dnešný svet je stále reálny a nie je tvorený len halucináciami. Chcel som použiť provokatívne, aj keď odborné nie presné označenie stavu, keď ľudia na celom svete už niekoľko rokov využívajú AI, pričom sa s ňou mnohokrát radia aj o vážnych životných situáciách. Hľadajú v komunikácii s AI odpovede, návody, riešenia a rady. AI im ich rada poskytne, pričom pri odpovediach nemá problém si riešenie vymyslieť, či postaviť ho na vymyslených, neexistujúcich, teda vyhalucinovaných údajoch, informáciách a dátach. Platí to aj pre oblasť práva.

Pre mnohých ľudí je už teraz interakcia s AI bohatým, obohacujúcim a autentickým zážitkom. Rastú obavy zo „psychózy AI“, vzťahovej väzby a duševného zdravia.

AI je špecifický autonómny systém, ktorý na báze algoritmov, vytvára rozhodnutia, ktoré môžu mať negatívne dopady na život, resp. životnú situáciu človeka. Odpovede jazykových modelov AI si vyžadujú veľkú opatrnosť a pozorné hodnotenie.

Z hľadiska zodpovednosti za spôsobenú škodu legislatívne takéto situácie zatiaľ výslovne vyriešené nie sú ani na európskej úrovni a ani na národnej úrovni. Limitom doterajšej regulácie je najmä skutočnosť, že táto sa zameriava na vnútorný trh Európskej únie, ktorá ale nie je lídrom vo vývoji AI.

Budúcnosť regulácie AI bude nevyhnutne charakterizovaná flexibilným a rizikovo orientovaným prístupom, ktorý umožní reagovať na nové technologické trendy a zároveň zabezpečiť ochranu spoločenských hodnôt.

Tým je aj dôvera verejnosti, či spoločnosti v schopnosť verejných inštitúcií vyriešiť situácie, ak bude niekomu spôsobená škoda v dôsledku nesprávnej rady alebo pomoci AI na základe vymyslených informácií.

Zoznam použitej literatúry

1. ANDRAŠKO, Jozef a kol.: Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021. 324 s. ISBN 978-80-9738-372-5.
2. DANIHLÍK, Tomáš: Některé etické aspekty používání umělé inteligence při odůvodňování soudních rozhodnutí. In: Jurisprudence č. 1/2025, s. 43 – 49. ISSN 3029-6722.
3. DIÁZ GONZÁLEZ, Gustavo Manuel: Prohibited Artificial Intelligence Practices. In: HUERGO LORA, Alejandro (Ed.): The EU Regulation on Artificial Intelligence: A Commentary. Milano: Wolters Kluwer Italia S.r.L., 2025. 642 s. ISBN 978-88-133-8814-0.
4. DRGONEC, Ján: Ústava Slovenskej republiky. Teória a prax. Bratislava: C.H.Beck, 2015. 1622 s. ISBN 978-80-89603-39-8.

5. KROŠLÁK, Daniel - BALOG, Boris - SURMAJOVÁ, Žaneta: Teória štátu a práva. 1. vydanie. Bratislava: Wolters Kluwer, 2020. 336 s. ISBN 978-80-571-0275-5.
6. MACEJKOVÁ, Iveta a kol.: Zákon o Ústavnom súde Slovenskej republiky. Komentár. 1. vydanie. Bratislava: C.H.Beck, 2020. 1640 s. ISBN 978-80-89603-90-9.
7. MARTINI, Mario: Regulating Artificial Intelligence – How to De-Mystify the Alchemy of Code. In: EBERS, Martin – NAVAS, Susana: Algorithms and Law. Cambridge University Press, 2020. 319 s. ISBN 978-11-083-4784-6.
8. MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 255 s. ISBN: 978-80-7160-715-1.
9. OROSZ, Ladislav - SVÁK, Ján a kol.: Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s. r. o., 2021. 892 s. ISBN 978-80-571-0380-6.
10. RUŽIČKOVÁ, Valéria (Ed.): Umelá inteligencia z pohľadu práva. Košice: Univerzita Pavla Šafárika, Právnická fakulta, 2021. 81 s. ISBN 978-80-574-0037-0.
11. ŠTĚDRŮŇ, Bohumír – JAŠEK, Roman – SVÍTEK, Miroslav a kol.: Umělá intelligence a právo. Plzeň: Aleš Čeněk, 2024. 233 s. ISBN 978-80-7380-947-8.
12. VOJTUŠ, František – KORDÍK, Marek – DRAŽOVÁ, Petra: Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia. In: Právnik, 6/2023, s. 549 – 570. ISSN 0231-6625.

Kontaktné údaje

doc. JUDr. Boris Balog, PhD.

boris.balog@flaw.uniba.sk

Katedra ústavného práva

Právnická fakulta Univerzity Komenského v Bratislave

NOVÉ VÝZVY INŠTITÚTU ZODPOVEDNOSTI ZA ŠKODU SPÔSOBENÚ PORUŠENÍM PRÁVA EURÓPSKEJ ÚNIE¹

NEW ISSUES OF DAMAGES LIABILITY IN EU LAW

Miroslav Slašťan, Miloš Levrinc²

Abstrakt: Príspevok vymedzuje koncept zodpovednosti za škodu spôsobenú porušením práva EÚ, ktorého sa dopúšťa členský štát. Oprávneným subjektom na náhradu škody je jednotlivец, ktorému však podmienky vzniku nároku vyplývajú iba z rozsiahlej judikatúry Súdneho dvora, ktorá sa naviac vyvíja. Príspevok polemizuje, či je tento koncept vo svojej aktuálnej podobe udržateľný, pričom rozhodujúcu úlohu v celom procese majú vnútroštátne súdy členských štátov, ktoré paralelne (doplnkovo) aplikujú aj svoje procesné predpisy. Problematickými je najmä povaha porušovanej normy práva EÚ, ale aj podmienka dostatočne závažného porušenia normy práva EÚ a tiež rozsah subjektov, ktoré možno subsumovať pod pojem „členský štát“.

Kľúčové slová: Európska únia, zodpovednosť za škodu, členský štát, judikatúra, Súdny dvor

Abstract: The article defines the concept of liability for damage caused by a breach of EU law committed by a Member State. The party entitled to compensation for damage is an individual, for whom the conditions for the creation of a claim arise only from the extensive case-law of the EU Court of Justice, which is also in evolution process. The article argues whether this concept is sustainable in its current form, while the decisive role in the whole process is played by the national courts of the Member States, which also apply their procedural rules in parallel (additionally). The nature of the violated norm of EU law, but also the condition of a sufficiently serious breach of a norm of EU law and the scope of entities that can be subsumed under the concept of "Member State" are particularly problematic.

Key words: European Union, damage liability, Member State, case-law, Court of Justice

¹ Tento príspevok je vypracovaný v rámci projektu EÚ: ERASMUS-JMO-2025-MODULE s názvom „External Action of the European Union“ č. 101238319.

² Univerzita Komenského, Právnická fakulta, Bratislava (Miroslav Slašťan), Univerzita Mateja Bela v B. Bystrici, Právnická fakulta (Miloš Levrinc)

Úvod

Fyzickým a právnickým osobám boli na základe judikatúry Súdneho dvora EÚ priznané viaceré práva, ktorých sa môžu domáhať priamo na základe práva EÚ a ktoré im vnútroštátne právne poriadky musia bezpodmienečne zaručiť. Jedná sa o práva, ktoré zakladá právo EÚ bez ohľadu na právo vnútroštátne, pričom však vyplývajú priamo (iba) z judikatúry Súdneho dvora a nadobúdajú charakter všeobecných zásad únieho práva. Platí, že z fundamentálnej povinnosti členského štátu zabezpečiť úplný účinok práva Európskej únie (pozri čl. 4 ods. 3 ZEÚ) vyplývajú fyzickým a právnickým osobám tieto práva:

- právo na účinnú súdnu ochranu práv vyplývajúcich z únieho právneho poriadku, vrátane predbežnej súdnej ochrany týchto práv;
- právo na vrátenie plnenia poskytnutého bez právneho dôvodu, ak bolo toto plnenie poskytnuté v súvislosti s porušením únieových predpisov;
- právo na náhradu škody spôsobenej porušením únieho práva.³

Právo EÚ upravuje samostatne zodpovednosť za škodu spôsobenú jednotlivcami a samostatne zodpovednosť za škodu spôsobenú členským štátom. Obe sú veľmi aktuálne inštitúty, rozvíjajúce sa v čase, pričom sa na tomto mieste zameriame práve na zodpovednosť za škodu spôsobenú členským štátom.

Základné podmienky zodpovednosti členských štátov za škodu spôsobenú porušením práva EÚ

Právny základ (mimozmluvnej) zodpovednosti členských štátov EÚ za škodu spôsobenú porušením práva EÚ ktorýmkoľvek orgánom verejnej moci členského štátu konajúcim v jeho mene, nemá jasný a výslovný právny základ v primárnom alebo sekundárnom práve EÚ⁴ a je výlučne „produktom judikatúry Súdneho dvora“. ⁵ Uvedené samozrejme nie je ideálny stav z dôvodu právnej istoty, presného rámca a podmienok uplatnenia týchto práv, ktoré nie sú kodifikované napríklad a najmä v rámci sekundárneho práva EÚ (smerniciach či nariadeniach⁶).

³ Siman, Michael – Slašťan, Miroslav: PRÁVO EURÓPSKEJ ÚNIE (inštitucionálny systém a právny poriadok Únie s judikatúrou). Bratislava: EUROIURIS – Európske právne centrum, 2012. S. 425 – 426. ISBN 978-80-89406-12-8.

⁴ Craig, P., De Búrca, G. EU Law: Text, Cases, and Materials UK Version. 7 th edition. Oxford: Oxford University Press, 2020, s. 248.

⁵ Pozri Bobek, Michal – Bříza, Peter – Komárek, Jan: Vnitrostátní aplikace práva Evropské unie. Praha: C.H.Beck, 2011, ISBN 9788074003776, s. 285.

⁶ Ako vzor a výnimku možno uviesť smernicu Európskeho parlamentu a Rady 2014/104/EÚ z 26. novembra 2014 o určitých pravidlách upravujúcich žaloby podľa vnútroštátneho práva o náhradu škody utrpenej v dôsledku porušenia ustanovení práva hospodárskej súťaže členských štátov a Európskej únie, Ú. v. EÚ L 349, , s. 1 – 19. Pozri tiež Oznámenie Komisie o vyčíslení škody pri žalobách

Podľa judikatúry Súdneho dvora vznikajúcej postupne od roku 1991⁷ je zásada zodpovednosti členského štátu za škody, ktoré spôsobil jednotlivcom z dôvodu porušenia práva EÚ, súčasťou systému Zmluvy o fungovaní Európskej únie a tým aj únieového právneho poriadku.⁸

Podľa ustálenej judikatúry Súdneho dvora by totiž bola ohrozená úplná účinnosť práva Únie a účinná ochrana práv, ktoré z neho vyplývajú, ak by jednotliviec nemal možnosť získať náhradu škody, ktorá mu bola spôsobená v dôsledku porušenia práva Únie, ktoré možno pripísať členskému štátu.⁹ Zodpovednosť členského štátu EÚ za škodu spôsobenú porušením práva EÚ existuje bez ohľadu na to, ktorý orgán členského štátu konaním alebo opomenutím porušil povinnosť vyplývajúcu z práva EÚ.¹⁰

Platí, že podľa judikatúry Súdneho dvora sa fyzické a právnické osoby (poškodení) môžu domáhať náhrady škody, spôsobenej členským štátom porušením práva EÚ len pri súčasnom splnení všetkých podmienok, ktoré stanovila relevantná judikatúra Súdneho dvora nasledovne:

- a) porušená právna norma EÚ priznáva práva fyzickým alebo právnickým osobám;
 - b) porušenie právnej normy EÚ (protiprávnosť konania členského štátu) je dostatočne závažné;
 - c) medzi porušením právnej normy EÚ členským štátom a škodou spôsobenou fyzickým a právnickým osobám existuje priama príčinná súvislosť (kauzálny nexus) – namietaná škoda musí vyplývať z porušenia únieového práva dostatočne priamym spôsobom, aby bolo možné zaviazat štát na jej náhradu.¹¹
- Ad a)

o náhradu škody vzniknutej v dôsledku porušenia článku 101 alebo 102 Zmluvy o fungovaní Európskej únie, Ú. v. EÚ, C 167/19, 13.6.2013.

⁷ Zásada zodpovednosti členského štátu za škodu spôsobenú porušením práva EÚ bola najskôr zakotvená v rozhodnutí Súdneho dvora z 19.11.1991, Francovich a Bonifaci, C-6 a 9/90, EU:C:1991:428.

⁸ Pozri rozsudky z 19. novembra 1991, Francovich a i., C-6/90 a C-9/90, EU:C:1991:428, bod 35; z 5. marca 1996, Brasserie du pêcheur a Factortame, C-46/93 a C-48/93, EU:C:1996:79, bod 31, ako aj zo 14. marca 2013, Leth, C-420/11, EU:C:2013:166, bod 40.

⁹ Pozri v tomto zmysle rozsudok Súdneho dvora z 19. decembra 2019, C-752/18, Deutsche Umwelthilfe, ECLI:EU:C:2019:1114, bod 30.

¹⁰ Pozri v tomto zmysle rozsudky Súdneho dvora z 5. marca 1996, Brasserie du pêcheur a Factortame, C-46/93 a C-48/93, EU:C:1996:79, bod 32; z 30. septembra 2003, Köbler, C-224/01, EU:C:2003:513, bod 31; z 13. júna 2006, Traghetti del Mediterraneo, C-173/03, EU:C:2006:391, bod 30, ako aj z 25. novembra 2010, Fuß, C-429/09, EU:C:2010:717, bod 46.

¹¹ Pozri rozsudky Súdneho dvora z 5. marca 1996, Brasserie du pêcheur a Factortame, C-46/93 a C-48/93, EU:C:1996:79, bod 51 alebo z 24. marca 2009, Danske Slagterier, C-445/06, EU:C:2009:178, bod 20, alebo z 10. decembra 2020, Euromin Holdings (Cyprus), C-735/19, EU:C:2020:1014, bod 79.

Podstatným pri skúmaní, či porušená norma EÚ priznáva práva pre fyzické alebo právnické osoby sú dve otázky: aké právo právna norma stanovuje a následne kto je adresátom týchto práv.

Žaloba jednotlivca (právnickej osoby) na náhradu škody sa môže opierať tak o normu primárneho práva (napr. čl. 49 alebo 63 ZFEÚ), ako aj o ustanovenie sekundárneho práva.

V súvislosti so vznikom nárokov na náhradu škody nie je podstatné, či má dotknutá norma práva Únie priamy účinok.¹² Napriek tomu je však priamy účinok skutočnosťou, ktorá podporuje predpoklad o priznaní práv, pretože v takomto prípade možno určiť obsah priznaného práva, čo tvorí podmienku na vznik nároku na náhradu škody.¹³

Ad b)

Podmienka dostatočne závažného porušenia práva EÚ je „najzložitejšou“ kategóriou a podmienkou vzniku zodpovednosti predovšetkým z dôvodu miery subjektivity pri hodnotení, či porušenie normy EÚ je „dostatočne závažné“.¹⁴

Pri určení, či ide o dostatočne závažné porušenie práva Únie, musí vnútroštátny súd, ktorý rozhoduje o návrhu na náhradu škody, zohľadniť všetky skutočnosti príznačné pre situáciu, o ktorej má rozhodnúť.¹⁵ K týmto skutočnostiam patrí:

- stupeň jasnosti a presnosti porušenej normy,
- rozsah miery voľnej úvahy, ktorý porušená norma ponecháva vnútroštátnym orgánom,
- úmyselná alebo neúmyselná povaha nesplnenia povinnosti alebo spôsobenej škody,
- ospravedlniteľnosť alebo neospravedlniteľnosť prípadného právneho posúdenia,

¹² Rozsudky Súdneho dvora z 5. marca 1996, *Brasserie du pêcheur a Factortame*, C-46/93 a C-48/93, EU:C:1996:79, body 21 a 22, z 10. decembra 2020, *Euromin Holdings (Cyprus)*, C-735/19, EU:C:2020:1014, bod 81.

¹³ Pozri rozsudky Súdneho dvora z 24. marca 2009, *Danske Slagterier*, C-445/06, EU:C:2009:178, bod 22 až 26; z 25. novembra 2010, *Fuß*, C-429/09, EU:C:2010:717, body 49 a 50, a z 25. marca 2021, *Bälgarska Narodna Banka*, C-501/18, EU:C:2021:249, body 63 a 86, ale aj z 19. novembra 1991, *Francovich a i.*, C-6/90 a C-9/90, EU:C:1991:428, bod 40; zo 4. júla 2006, *Adeneler a i.*, C-212/04, EU:C:2006:443, bod 112, a z 24. januára 2018, *Pantuso a i.*, C-616/16 a C-617/16, EU:C:2018:32, bod 49.

¹⁴ Pozri Bobek, M. – Bříza, P. – Komárek, J.: *Vnitrostátní aplikace práva Evropské unie*. 1. vyd. Praha: C.H.Beck, 2011, s. 299.

¹⁵ Pozri návrhy generálnej advokátky J. Kokott prednesené 5. mája 2022, C-61/21, ECLI:EU:C:2022:359, bod 106.

- okolnosť, že v prípade potreby mohli postojie inštitúcie Európskej únie prispieť k prijatiu alebo zachovaniu opatrení alebo vnútroštátnej praxe, ktoré sú v rozpore s právom Únie,¹⁶

- okolnosť, či porušenie práva Únie pretrváva naďalej napriek rozsudku Súdneho dvora, ktorý toto vytýkané nesplnenie povinnosti konštatuje, alebo napriek rozhodnutiu o prejudiciálnej otázke alebo ustálenej judikatúre Súdneho dvora v danej oblasti, z ktorých vyplýva, že dotknuté správanie je porušením práva.¹⁷

V žiadnom prípade neplatí, že každé či akékoľvek porušenie práva EÚ je dostatočne závažné. Súdny dvor označil za dostatočne závažné porušenie práva EÚ (od roku 1991) v zásade len nasledovné skutočnosti:

- in concreto v rozsudku vo veci C-46/93 a C-48/93, Brasserie du pêcheur a Factortame Súdny dvor uviedol, že porušenie práva EÚ je dostatočne závažné vtedy, ak pretrváva:

i) naďalej napriek rozsudku, ktorý toto vytýkané nesplnenie povinnosti konštatuje (tzn. rozsudku Súdneho dvora napr. v konaní podľa čl. 258 až 260 ZFEÚ), alebo

ii) napriek rozhodnutiu Súdneho dvora o prejudiciálnej otázke podľa čl. 267 ZFEÚ alebo

iii) napriek ustálenej judikatúre Súdneho dvora v danej oblasti, z ktorej vyplýva, že dotknuté správanie je zjavne porušením práva¹⁸ a

- na základe prvotného rozsudku Súdneho dvora vo veci Francovich a ďalších rozhodnutí (napr. Dillenkofer)¹⁹ možno dodať, že fikcia dostatočne závažného porušenia práva EÚ platí tiež v prípade absencie (tzn. úplného opomenutia) prebratia smernice v stanovenej lehote.

Napríklad vo veci týkajúcej sa prijatia zákona zákonodarným zborom vo vzťahu k preberaniu smernice Súdny dvor uviedol, že porušenie je dostatočne závažné len vtedy, kde pri výkone svojich legislatívnych právomocí členský štát zjavne a závažne nezohľadňuje obmedzenie výkonu

¹⁶ Rozsudky z 5. marca 1996, C-46/93 a C-48/93, Brasserie du pêcheur a Factortame, EU:C:1996:79, bod 56, a z 29. júla 2019, C-620/17, Hochtief Solutions Magyarországi Fióktelepe, EU:C:2019:630, bod 42.

¹⁷ Rozsudky z 5. marca 1996, C-46/93 a C-48/93, Brasserie du pêcheur a Factortame, EU:C:1996:79, bod 57, a z 12. decembra 2006, C-446/04, Test Claimants in the FII Group Litigation, EU:C:2006:774, bod 214; z 30. mája 2017, C-45/15 P, Safa Nicu Sepahan/Rada, EU:C:2017:402, bod 31, a z 18. januára 2022, C-261/20, Thelen Technopark Berlin, EU:C:2022:33, bod 47.

¹⁸ Rozsudok Súdneho dvora z 5. marca 1996, Brasserie du pêcheur a Factortame, C-46/93 a C-48/93, EU:C:1996:79, bod 57. V rozsudku Súdneho dvora z 30.9.2003, Köbler, C-224/01, ECLI:EU:C:2003:513, bod 56 je výslovne uvedené spojenie „v zjavnom rozpore s príslušnou judikatúrou Súdneho dvora“, tzn. porušenie ustálenej judikatúry musí byť zjavné.

¹⁹ Pozri rozsudok Súdneho dvora z 19. novembra 1991, Francovich a i., C-6/90 a C-9/90, EU:C:1991:428, a rozsudok Súdneho dvora z 8.10.1996, C-178, 179 a 188 až 190/94, Dillenkofer, ECR s. 4845.

svojich právomocí. Napríklad ak má smernica nepresné znenie a neexistuje príslušná judikatúra Súdneho dvora k jej objasneniu, jej nesprávne prebratie nemôže založiť dostatočne závažné porušenie čl. 288 ZFEÚ.²⁰ Práve uvedená vec C-392/93, *British Telecommunications* má svoj ratio, avšak postupne Súdny dvor obmedzuje existenciu, či úvahu o „nepresnom znení“ smerníc, napríklad v rámci smerníc o verejnom obstarávaní.

Ďalej tiež v prípade, ak porušil právo EÚ vnútroštátny súd, je možné priznať zodpovednosť členského štátu za prípadnú škodu iba vtedy, ak právo EÚ porušil súd svojim rozhodnutím v poslednom stupni, pričom zodpovednosť môže vzniknúť iba vo výnimočnom prípade, keď vnútroštátny súd rozhodujúci v poslednom stupni porušil zjavným spôsobom uplatniteľné právo.²¹ Súdny dvor EÚ napríklad posudzoval zodpovednosť Slovenskej republiky za škodu spôsobenú jednotlivcom v dôsledku porušenia práva Únie na základe návrhu na začatie prejudiciálneho konanie Okresného súdu Prešov (Slovenská republika) a v konaní vedenom v registri Súdneho dvora EÚ pod označením C-168/15, *Milena Tomášová* proti Slovenskej republike – Ministerstvu spravodlivosti SR, Pohotovosti s.r.o., za účasti: Združenia na ochranu občana spotrebiteľa HOOS. Súdny dvor v tomto konaní rozhodol, že pokiaľ ide konkrétne o druhú z podmienok zodpovednosti za škodu spôsobenú porušením práva EÚ (porušenie normy EÚ je dostatočne závažné), táto zodpovednosť môže vzniknúť iba vo výnimočnom prípade, keď vnútroštátny súd rozhodujúci v poslednom stupni porušil zjavným spôsobom uplatniteľné právne predpisy.²²

Vo vzťahu k podmienke dostatočne závažného porušenia práva EÚ možno zhrnúť, že podľa judikatúry Súdneho dvora sú to fundamentálne vnútroštátne súdy, ktoré sú príslušné zistiť skutkový stav vo veci samej a rozhodnúť ako charakterizovať predmetné porušenie práva EÚ.²³ Platí, že pomoc im poskytne Súdny dvor v rámci nimi iniciovaného prejudiciálneho konania podľa čl. 267 ZFEÚ.

Ad c)

Pokiaľ ide o tretiu podmienku, je opäť právomocou vnútroštátnych súdov, aby preverili, či existuje priama príčinná súvislosť medzi porušením povinnosti,

²⁰ Rozsudok Súdneho dvora z 26. marca 1996, C-392/93, *British Telecommunications*, ECLI:EU:C:1996:131, body 43 až 45.

²¹ Pozri rozsudky Súdneho dvora z 30. septembra 2003, *Köbler*, C-224/01, EU:C:2003:513, bod 53, ako aj z 13. júna 2006, *Traghetti del Mediterraneo*, C-173/03, EU:C:2006:391, body 32 a 42.

²² Rozsudok Súdneho dvora z 28. júla 2016, *Milena Tomášová*, C-168/15, ECLI:EU:C:2016:602, bod 22.

²³ Rozsudok Súdneho dvora z 5. marca 1996, *Brasserie du pêcheur a Factortame*, C-46/93 a C-48/93, EU:C:1996:79, bod 58.

ktorú má členský štát, a škodou, ktorú utrpeli poškodené osoby,²⁴ teda či namietaná škoda skutočne vyplýva z porušenia práva EÚ dostatočne priamym spôsobom, aby bolo možné zaviazat štát na jej náhradu.²⁵ Určenie konkrétneho dôkazného bremena prináleží vnútroštátnym súdom. Tieto sú povinné skúmať, či namietané poškodenie dostatočne priamo vyplýva z porušenia práva Únie členským štátom, pričom sa musí prihliadnuť na zásady ekvivalencie a efektívnosti.²⁶

Súdny dvor ďalej rozhodol, že náhrada škody spôsobenej jednotlivcom porušením práva EÚ musí byť primeraná vzniknutej škode, aby sa zabezpečila účinná ochrana ich práv.²⁷ Keďže v tejto oblasti neexistujú ustanovenia na úrovni práva EÚ, je na vnútroštátnom právnom poriadku každého členského štátu, aby stanovil kritériá umožňujúce určiť rozsah náhrady škody, pričom nemôžu byť menej priaznivé ako kritériá platné pre podobné nároky vyplývajúce z vnútroštátneho práva a v žiadnom prípade nemôžu byť upravené tak, aby náhrada škody v praxi bola nemožná alebo neprimerane sťažená.²⁸ Súdny dvor tiež v tejto súvislosti určil, že v zásade prináleží poškodenému, aby po právnej stránke dostatočne preukázal rozsah škody, ktorú utrpel v dôsledku porušenia práva Únie, ktorá je predpokladom vzniku zodpovednosti štátu za takúto škodu.²⁹ Účinná ochrana práva na náhradu škody spôsobenej jednotlivcom porušením práva Únie musí umožniť žalobu o zodpovednosť založenú na bezprostredne hroziacej a predvídateľnej škode s dostatočnou istotou, aj keď škoda ešte nemôže byť presne vyčíslená.³⁰

²⁴ Rozsudok Súdneho dvora z 5. marca 1996, *Brasserie du pêcheur a Factortame*, C-46/93 a C-48/93, EU:C:1996:79, bod 56.

²⁵ Pozri rozsudky Súdneho dvora vo veciach *Test Claimants CFC*, C-201/05, Uz. 23.4.2008, Zb. s. I-2875, bod 125; *Test Claimants Thin Cap*, C-524/04, 13.3.2007, Zb. s. I-2107, bod 122 a *Test Claimants FII*, C-446/04, 12.12.2006, Zb. s. I-11753, bod 218.

²⁶ Rozsudky Súdneho dvora z 5. marca 1996, C-46/93 a C-48/93, *Brasserie du pêcheur a Factortame*, EU:C:1996:79, bod 65; z 20. októbra 2011, C-94/10, *Danfoss a Sauer-Danfoss*, EU:C:2011:674, bod 34, a z 19. júna 2014, C-501/12 až C-506/12, C-540/12 a C-541/12, *Specht a i.* EU:C:2014:2005, bod 106, alebo rozsudky z 13. júla 2006, C-295/04 až C-298/04, *Manfredi a i.*, EU:C:2006:461, bod 64, a z 5. júna 2014, C-557/12, *Kone a i.*, EU:C:2014:1317, bod 24.

²⁷ Rozsudok Súdneho dvora z 5. marca 1996, *Brasserie du pêcheur a Factortame*, C-46/93 a C-48/93, EU:C:1996:79, bod 82.

²⁸ Rozsudok Súdneho dvora z 5. marca 1996, *Brasserie du pêcheur a Factortame*, C-46/93 a C-48/93, EU:C:1996:79, bod 83.

²⁹ Rozsudok Súdneho dvora z 25. marca 2021, C-501/18, *Bälgarska Narodna Banka*, EU:C:2021:249, bod 122.

³⁰ Rozsudok Súdneho dvora z 25. marca 2021, C-501/18, *Bälgarska Narodna Banka*, EU:C:2021:249, bod 126.

Následne konštatujeme, že neexistuje taký prameň práva EÚ, z ktorého by vyplývali ďalšie hmotnoprávne a procesnoprávne aspekty uplatňovania náhrady škody v dôsledku porušenia práva EÚ členským štátom. Opäť podľa judikatúry Súdneho dvora, ak neexistuje právna úprava EÚ, potom je úlohou vnútroštátneho právneho poriadku každého členského štátu, aby označil príslušné súdne orgány a upravil konania o žalobách, ktorých cieľom je zabezpečiť úplné zachovanie práv, ktorých sa subjekty práva domáhajú na základe práva Únie.³¹

Súdny dvor tiež určil, že ak sú splnené podmienky týkajúce sa vzniku zodpovednosti štátu (jediné stanovené právom EÚ), čo prináleží posúdiť vnútroštátnym súdom³², je úlohou štátu napraviť následky spôsobenej škody v rámci vnútroštátneho práva zodpovednosti za škodu, pričom predpoklady zodpovednosti za škodu stanovené vnútroštátnym právom:

i) nemôžu byť nepriaznivejšie ako pri podobných právnych prostriedkoch týkajúcich sa výlučne len vnútroštátneho práva (zásada ekvivalencie) a

ii) nesmú byť ani formulované tak, aby získanie náhrady škody robili prakticky nemožným alebo neúmerne ťažkým (zásada efektivity).³³

Právo Únie tiež nevyklučuje, aby zodpovednosť štátu za porušenie tohto práva mohla byť podľa vnútroštátneho práva vyodená aj za menej prísnych podmienok, ale bráni tomu, aby v tejto súvislosti vnútroštátne právo ukladalo ďalšie podmienky.³⁴

Ktoré subjekty sú „členským štátom“?

Z článku 4 ods. 3 ZEÚ vyplýva, že členské štáty nesmú prijať alebo ponechať v platnosti opatrenia, ktoré by mohli ohroziť úplný účinok (tzv. effet utile) práva EÚ.³⁵ Povinnosť zabezpečiť dodržiavanie práva Únie majú v rámci svojich právomocí všetky orgány členského štátu.³⁶ Pojem „členský štát“ používajú zakladajúce zmluvy na viacerých miestach, najmä čl. 4, 34, 42 alebo 46 ZEÚ, ale aj napríklad čl. 2 ods. 3, 4 ods. 1, 34, 102, alebo 107 ods. 1 ZFEÚ. Zodpovednosť za porušenie práva EÚ členským štátom teda vyžaduje na stane porušiteľa jednoznačný subjekt, ktorý je „členským štátom“, subjekt ktorý koná v jeho mene. Judikatúra takýto subjekt

³¹ Rozsudok Súdneho dvora z 24. marca 2009, Danske Slagterier, C-445/06, EU:C:2009:178, bod 31.

³² Pozri rozsudok Súdneho dvora z 29. júla 2019, C-620/17, Hochtief, ECLI:EU:C:2019:630, bod 40.

³³ Pozri rozsudky z 19. novembra 1991, Francovich a i., C-6/90 a C-9/90, EU:C:1991:428, bod 42; z 30. septembra 2003, Köbler, C-224/01, EU:C:2003:513, bod 58; z 24. marca 2009, Danske Slagterier, C-445/06, EU:C:2009:178, bod 31; z 25. novembra 2010, Fuß, C-429/09, EU:C:2010:717, bod 62, ako aj z 9. septembra 2015, Ferreira da Silva e Brito a i., C-160/14, EU:C:2015:565, bod 50.

³⁴ Rozsudok Súdneho dvora zo 4. októbra 2018, Kantarev, C-571/16, EU:C:2018:807, body 120 a 121, ako aj citovaná judikatúra.

³⁵ Pozri rozsudok Súdneho dvora z 12.2.2009, Komisia p. Grécku, C-45/07, bod 17.

³⁶ Pozri rozsudok Súdneho dvora z 12.2.2008, Kempster, C-2/06, Zb. s. I-411, bod 35; alebo rozsudok Súdneho dvora z 13.1.2004, Kühne a Heitz, C-453/00, Zb. s. I-837, bod 20.

spresňuje ako „vnútroštátny orgán členského štátu“, ktorý má povinnosť zabezpečiť dodržiavanie práva EÚ.

Konštatujeme, že podľa článku 4 ods. 3 Zmluvy o EÚ sú všetky orgány členského štátu v rámci ich právomocí povinné zabezpečiť dodržiavanie práva Európskej únie bez ohľadu na to, či sa jedná o orgány centrálnej (federálnej) moci, orgány členských štátov federácie alebo orgány samosprávnych územných celkov.³⁷ Do rozsahu pojmu členský štát spadajú aj zákonodarné orgány³⁸, súdne orgány³⁹, správne orgány, napríklad colné orgány⁴⁰ a tiež samosprávne organizácie.⁴¹

Avšak Súdny dvor následne rozšíril pojem „členský štát“. ⁴² V rozsudku vo veci C-188/89 Foster⁴³ uviedol, že ide vždy aj o subjekt, ktorý splní nasledovné podmienky:

- i) plnení služby vo verejnom záujme,
- ii) podlieha kontrole štátu a
- iii) disponuje osobitnými právomocami presahujúcimi právomoci, ktoré vyplývajú z bežných pravidiel uplatniteľných vo vzťahoch medzi jednotlivcami.

Konštatujeme, že na preskúmanie podmienky, či je služba vo verejnom záujme poskytovaná pod kontrolou štátu, resp. subjekt je pod kontrolou štátu, sú relevantné skutočnosti a to každá samostatne:

- štát je väčšinovým alebo výlučným vlastníkom jej základného kapitálu,
- štát môže menovať členov jej riadiacich alebo kontrolných orgánov,
- štát môže dávať pokyny v súvislosti s riadením jej činnosti súvisiacej s verejnými službami.⁴⁴

Problematickým však je, že Súdny dvor netrvá na splnení troch vyššie podmienok vždy súčasne (kumulatívne).⁴⁵ Súdny dvor napríklad v rozsudku C-361/12, Carmela Carratù už nevyžaduje skúmanie podmienky väčších / osobitných právomocí (pozri odseky 29 až 31 rozsudku), pričom zo skutkovej podstaty prípadu je zrejmé, že na dotknutý vnútroštátny orgán členského štátu (Poste Italiane SpA) preniesol štát záväzok univerzálnej služby v rôznych odvetviach, tzn. subjekt vykonával služby vo verejnom záujme (tzn. sú dané dve z troch analyzovaných podmienok).⁴⁶ Nakoniec Súdny dvor v rozsudku z 10. októbra 2017, C-413/15, Farrell II výslovne uviedol, že

³⁷ Pozri rozsudok Súdneho dvora z 12.6.1990, Nemecko p. Komisia, C-8/88, Zb. s. I-2321, bod 13.

³⁸ Pozri rozsudok Súdneho dvora z 5.3.1996, Factortame, C-46 a 48/93, Zb. s. I-1029, body 36 a 34.

³⁹ Pozri rozsudok Súdneho dvora z 30.9.2003, Köbler, C-224/01, Zb. s. I-10239, bod 32.

⁴⁰ Pozri rozsudok Súdneho dvora z 13.1.2004, Kühne a Heitz, C-453/00, Zb. s. I-837.

⁴¹ Pozri rozsudok Súdneho dvora zo 4.7.2000, Haim, C-424/97, Zb. s. I-5123, body 31 a 32.

⁴² Kunertová, T.: could the broad definition of “state” for the purposes of direct effect be justifiable under the eu’s aim of promoting a fully liberalised internal market? In: The Lawyer Quarterly. No. 1 /2024, s. 82–90.

⁴³ Rozsudok Súdneho dvora z 12. júla 1990, Foster, C-188/89, Zb. s. I-3313, bod 20 a nasl.

⁴⁴ Pozri rozsudok Súdneho dvora z 12.12.2013, C-425/12, Portgás, ECLI:EU:C:2013:829, bod 29.

⁴⁵ Pozri rozsudok Súdneho dvora z 10. októbra 2017, C-413/15, Farrell II, ECLI:EU:C:2017:745, body 28 a 29.

⁴⁶ Pozri návrhy generálneho advokáta N. Wahla z 26.09.2013, C-361/12, Carmela Carratù, bod 106.

podmienky, za ktorých dotknutý subjekt musí buď podliehať štátnej moci, alebo byť kontrolovaný štátom a disponovať na tento účel väčšími právomocami v porovnaní s tými, ktoré vyplývajú z pravidiel uplatniteľných na vzťahy medzi jednotlivcami, nemajú kumulatívnu povahu,⁴⁷ pričom z judikatúry Súdneho dvora počnúc rozsudkom vo veci 152/84 Marshall, a následne vo veciach C-361/12 Carratú, C-152/02 Rieser až C-413/15, Farrell II) vyplýva, že obligatórna je podmienka plnenia služieb vo verejnom záujme. V tomto zmysle však dodávame, že ide o potenciálne o enormne širokú skupinu subjektov (ktoré o tomto postavení, ktoré im z práva EÚ/judikatúry Súdneho dvora vyplýva, pravdepodobne ani netušia).

Záver

Možno zhrnúť, že ak sú podmienky týkajúce sa vzniku zodpovednosti štátu splnené, čo prináleží určiť vnútroštátnym súdom, prináleží štátu podľa vnútroštátneho práva upravujúceho zodpovednosť za spôsobenú škodu napraviť následky škody spôsobenej jednotlivcovi predmetným porušením práva Únie, pričom podmienky náhrady škody stanovené v uplatniteľných vnútroštátnych právnych úpravách nemôžu byť menej výhodné ako podmienky uplatniteľné na podobné nároky založené na porušení vnútroštátneho práva (zásada ekvivalencie), a nemôžu byť upravené tak, aby viedli k praktickej nemožnosti alebo nadmernému sťaženiu získania náhrady (zásada efektivity).⁴⁸ Dodržiavanie týchto požiadaviek sa musí skúmať s prihliadnutím na postavenie predmetných ustanovení v celom konaní, na priebeh uvedeného konania a osobitosti týchto ustanovení na rôznych stupňoch vnútroštátnych súdov.⁴⁹

Z uvedeného vyplýva, že v každom členskom štáte musí existovať hmotnoprávny a procesnoprávny systém noriem týkajúci sa zodpovednosti za škodu, ktorý upravuje podrobne všetky ostatné podmienky tohto typu žaloby a konania (napr. pasívnu legitimáciu, procesné lehoty, vecnú a miestnu príslušnosť súdu, súdny poplatok, premlčanie nárokov a pod.), inak by nebolo možné ani overiť náležitosti zásady ekvivalencie a efektivity.

Konštatujeme, že vyššie uvedená judikatúra Súdneho dvora EÚ výslovne upravujúce iba podmienky vzniku zodpovednosti členského štátu za škodu spôsobenú porušením práva EÚ.

Následne pravidlá týkajúce sa napríklad ohodnotenia škody spôsobenej v dôsledku porušenia práva Únie určuje vnútroštátne právo každého členského štátu, pričom

⁴⁷ Rozsudok Súdneho dvora z 10. októbra 2017, C-413/15, Farrell II, ECLI:EU:C:2017:745, bod 27.

⁴⁸ Rozsudok Súdneho dvora zo 4. októbra 2018, Kantarev, C-571/16, EU:C:2018:807, body 122 a 123, ako aj citovaná judikatúra.

⁴⁹ Rozsudok Súdneho dvora z 25. marca 2021, C-501/18, Bălgarska Narodna Banka, ECLI:EU:C:2021:249, bod 116.

vnútroštátne právne úpravy, ktoré tieto pravidlá stanovujú, musia dodržiavať zásady ekvivalencie a efektivity.⁵⁰

Zásadne teda platí, že jedine vnútroštátne súdy majú právomoc:

- i) zistiť skutkový stav vo veci samej,
- ii) rozhodnúť o prípadnom porušení konkrétnej normy práv EÚ a
- iii) určiť, ako charakterizovať prípadné porušenie práva EÚ, tzn. či ide o závažné porušenie práva EÚ (splnenie všetkých podmienok zodpovednosti v zmysle judikatúry Súdneho dvora).

Neplatí, že každé alebo akékoľvek porušenie práva EÚ je dostatočne závažné, pričom Súdny dvor už posúdil niekoľko situácií, ktoré sú dostatočne závažným porušením práva Únie.

Zoznam použitej literatúry a judikatúry

1. Bobek, Michal – Bříza, Peter – Komárek, Jan: Vnitrostátní aplikace práva Evropské unie. Praha: C.H.Beck, 2011, ISBN 9788074003776
2. Craig, P., De Búrca, G. EU Law: Text, Cases, and Materials UK Version. 7 th edition. Oxford: Oxford University Press, 2020
3. Siman, Michael – Slašťan, Miroslav: Právo Európskej únie (inštitucionálny systém a právny poriadok Únie s judikatúrou). Bratislava: EUROIURIS – Európske právne centrum, 2012. ISBN 978-80-89406-12-8
4. Kunertová, T.: could the broad definition of “state” for the purposes of direct effect be justifiable under the eu’s aim of promoting a fully liberalised internal market? In: The Lawyer Quarterly. No. 1 /2024, s. 82–90.
5. Rozsudok Súdneho dvora z 13. júla 2006, C-295/04 až C-298/04, Manfredi a i., EU:C:2006:461
6. Rozsudok Súdneho dvora z 30. septembra 2003, Köbler, C-224/01, EU:C:2003:513
7. Rozsudok Súdneho dvora z 5. marca 1996, Brasserie du pêcheur a Factortame, C-46/93 a C-48/93, EU:C:1996:79
8. Rozsudok Súdneho dvora z 25. marca 2021, C-501/18, Bălgarska Narodna Banka, EU:C:2021:249
9. Rozsudok Súdneho dvora z 24. marca 2009, Danske Slagterier, C-445/06, EU:C:2009:178
10. Rozsudok Súdneho dvora z 29. júla 2019, C-620/17, Hochtief, ECLI:EU:C:2019:630
11. Rozsudok z 19. novembra 1991, Francovich a i., C-6/90 a C-9/90, EU:C:1991:428
12. Rozsudok Súdneho dvora z 25. novembra 2010, Fuß, C-429/09, EU:C:2010:717

⁵⁰ Rozsudok Súdneho dvora z 28. júla 2016, C-168/15, Tomášová, ECLI:EU:C:2016:602, bod 39.

13. Rozsudok Súdneho dvora z 9. septembra 2015, Ferreira da Silva e Brito a i., C-160/14, EU:C:2015:565
14. Rozsudok Súdneho dvora zo 4. októbra 2018, Kantarev, C-571/16, EU:C:2018:807
15. Rozsudok Súdneho dvora z 12.6.1990, Nemecko p. Komisii, C-8/88, Zb. s. I-2321
16. Rozsudok Súdneho dvora z 5.3.1996, Factortame, C-46 a 48/93, Zb. s. I-1029
17. Rozsudok Súdneho dvora z 13.1.2004, Kühne a Heitz, C-453/00, Zb. s. I-837
18. Rozsudok Súdneho dvora zo 4.7.2000, Haim, C-424/97, Zb. s. I-5123
19. Rozsudok Súdneho dvora z 12. júla 1990, Foster, C-188/89, Zb. s. I-3313
20. Rozsudok Súdneho dvora z 12.12.2013, C-425/12, Portugás, ECLI:EU:C:2013:829
21. Rozsudok Súdneho dvora z 10. októbra 2017, C-413/15, Farrell II, ECLI:EU:C:2017:745
22. Návrhy generálneho advokáta N. Wahla z 26.09.2013, C-361/12, Carmela Carratù, ECLI:EU:C:2013:620

Kontaktné údaje

Miroslav Slašťan, prof. JUDr. PhDr., PhD.
miroslav.slastan@flaw.uniba.sk
Univerzita Komenského, Právnická fakulta

Miloš Levrinc, JUDr., PhD.
milos.levrinc@umb.sk
Právnická fakulta Univerzity Mateja Bela v Banskej Bystrici

ŠTÁT, SPOLOČNOSŤ, KYBERPRIESTOR: NÁVRAT DO MINULOSTI?¹

STATE, SOCIETY, CYBERSPACE: BACK TO THE PAST?

Branislav Fábry²

Abstrakt: Článok sa zaoberá aktuálnym vývojom štátu a spoločnosti, ktorý súvisí aj s rozmachom nových technológií, zvlášť v oblasti kyberpriestoru. Autor skúma výhody a nevýhody, ktoré prinášajú tieto nové technológie, najmä obmedzovanie slobody a dopady na práva pracujúcich, ale tiež javy, spojené s monopolizáciou zo strany technologických gigantov. V súvislosti s tým autor analyzuje vývoj, počas ktorého sa kyberpriestor zmenil z priestoru slobody na priestor neslobody. S tým súvisí aj snaha autora poukázať na riziká daného trendu monopolizácie. Článok však súčasne poukazuje aj na rastúcu nespravodlivosť, ktorá je hrozbou pre demokratický a právny štát. Autor tiež skúma, nakoľko sa štát a spoločnosť začínajú podobať politickým systémom z minulosti. Jedným z najvýznamnejších prejavov tohto trendu je aj rastúca nerovnosť a rozloženie daňovej záťaže vzáujme najbohatších skupín obyvateľstva. Na záver sa článok venuje aj potenciálnym možnostiam sociálnych a ekonomických zmien. Zaoberá sa pritom najmä otázkou, aká reakcia by mala prichádzať zo strany Európskej únie a aké sú jej limity.

Kľúčové slová: štát, kyberpriestor, sloboda, stredná trieda, daňová spravodlivosť

Abstract: The article deals with the current development of the state and society, which is also related to the boom of new technologies, especially in the field of cyberspace. The author points out to the chances and the risks of new technologies, especially restrictions of freedom and the impact of digitalization on workers' rights, but also with the phenomena of monopolization made by the technological giants. In this regard, the author analyzes the development of cyberspace that has changed from a space of freedom to unfree space and points out the risks of that trend. The article also deals with the threats to a democratic state based on rule of law. The author also analyses how far are the

¹ VEGA 2/0118/24 „Sociálna povaha normativity ako východisko vysvetlenia vzťahu individuálnej a kolektívnej autonómie“.

² Univerzita Komenského v Bratislave, Právnická fakulta.

state and society beginning to resemble political system known from the past. One of the most significant manifestations of this trend is growing inequality and the distribution of the tax burden in the interests of the richest groups of the population. Finally, the article discusses the potential possibilities of social and economic changes that would reverse this trend. It addresses mainly the question what reaction should come from the European Union and what are its limits.

Key words: state, cyber space, freedom, middle class, tax equality

Smutný úvod: Zánik priestoru slobody

Svoj príspevok si dovoľím začať jedným vtipom, ktorý o súčasnom stave v kyberpriestore veľa vypovedá:

- Aký je rozdiel medzi Google a Jurským parkom?
- Jedno je monštrum, ktoré zožerie všetko, na čo narazí a to druhé

je sci-fi film Stevena Spielberga z deväťdesiatych rokov.

Keď v 20. storočí vznikal kyberpriestor ako nová sféra ľudskej aktivity, prinášal so sebou nevídané možnosti. Predovšetkým ponúkal priestor pre realizáciu ľudskej slobody a oblasť, ktorá nebola podrobne regulovaná predpismi rôznych subjektov. V priebehu 21. storočia sa však situácia postupne menila, sloboda sa obmedzovala a v kyberpriestore sa čoraz viac začali objavovať limity, a tiež javy ako sledovanie užívateľov, ich manipulácia či obchod s dátami a profilmi.

Monopolizácia a spolupráca so štátom

Zjednodušene možno konštatovať, že veľké technologické spoločnosti si v kyberpriestore „vykolíkovali“ vlastné územie a stali sa hrozbou pre slobodu a súkromie jednotlivca. Typickým javom sa stal neustály rast moci týchto spoločností. Zmenila sa aj kontrola nad týmito podnikmi. Napr. v spoločnosti Alphabet Inc. dnes kontrolujú pôvodní zakladatelia Larry Page a Sergej Brin len 3 % akcií, zatiaľ čo najväčšími akcionármi sa stali obrovské investičné spoločnosti sveta - Vanguard Group a BlackRock.³

Alphabet Inc. pritom dnes nekontroluje iba dominantný globálny vyhľadávač Google, ale aj služby Youtube, Google Maps, atď. Zvlášť ostražito pritom treba vnímať snahu tejto spoločnosti o dominanciu v oblastiach, ktoré môžu viesť k oslabovaniu spotrebiteľských práv, napr. kontrolu systémov na porovnávanie cien. Podobné

³ INVESTING.COM: Who owns Alphabet? GOOGL Shareholders. Investing.com, 30 June 2025. Dostupné na: <https://www.investing.com/equities/google-inc-ownership> (cit.25.09.2025); a Alphabet Inc. (GOOG). Finance.yahoo.com, 30 June 2025. Dostupné na: <https://finance.yahoo.com/quote/GOOG/holders/> (cit.25.09.2025).

snahy o dominanciu v rôznych oblastiach sú typické aj pre ďalšie technologické spoločnosti ako Meta, ktorá ovláda nielen sociálnu sieť Facebook, ale aj Instagram, WhatsApp, atď. Pre celkovo štyri najväčšie technologické spoločnosti z USA sa vžila skratka GAFA – tá zahŕňa Google (Alphabet), Apple, Facebook (Meta) a Amazon.⁴ Spolu s Microsoft a Netflix sa označujú aj ako tzv. Silicon Six.

Vážnym problémom týchto dominantných subjektov v oblasti kyberpriestoru je spolupráca s tajnými službami USA, ktorým poskytujú chránené informácie o ich klientoch, donedávna v rámci programu PRISM.⁵ **Dokumenty uverejnené whistleblowermi** poukazovali na ovplyvňovanie politických procesov v zahraničí s pomocou nových technológií, ale aj na širšie spektrum protiprávných konaní tajných služieb, najmä pri zahraničných intervenciách.⁶ Whistlebloweri sa preto stali objektom najrôznejších foriem prenasledovania zo strany štátnych orgánov USA, vrátane pokusov o cenzúru zo strany veľkých technologických spoločností a objavili sa aj snahy o blokádu ich bankových operácií.⁷

Sledovaniu a šikane zo strany tajných služieb USA, spolupracujúcich s technologickými firmami, sa podľa zistení whistleblowerov nevyhli ani najvyšší predstavitelia štátov ako nemecká kancelárka Angela Merkelová či brazílska prezidentka Dilma Rousseffová.⁸ Existujú dokonca podozrenia, že informácie od tajných služieb USA mohli hrať dôležitú úlohu pri impeachmente D. Rousseffovej v Brazílii v roku 2016.⁹ Podobné využívanie informácií predstavuje aj do budúca silný nástroj pre ovplyvňovanie politickej situácie či kybernetické zasahovanie do politických a spoločenských pomerov v krajinách, ktoré nebránia svoju kybernetickú suverenitu.

Téma suverenity v oblasti kyberpriestoru sa stala významnou otázkou vzťahu medzi Čínou a USA a spor sa vyhracuje prakticky už od začiatku 21. storočia. Čína sa v rámci

⁴ SEMINARA, Jole: Market Dominance of GAFA companies and challenges posed to competition policy? Tesi di Laurea Magistrale. Politecnico di Torino, 2019. s. 43 a nasl.

⁵ RAMONET, Ignacio: Impero de la vigilancia. Buenos Aires: Capital Intelectual, 2016, 160, s. 54 a nasl.

⁶ AUST, Stefan – AMMANN, Thomas: Digitale Diktatur. Berlin: Ulstein, 2016, s. 138 a nasl.

⁷ KARHULA, Päivikki: What is the effect of WikiLeaks for Freedom of Information? International Federation of Library Associations and Institutions, 19 January 2011. Dostupné na: <https://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information/> (cit. 25.09.2025).

⁸ BROWN, Deborah: Brasil, Germany introduce resolution on The Right to Privacy in the Digital Age in UN General Assembly. AccesNow, 1 November 2013. Dostupné na: <https://www.accessnow.org/brazil-germany-introduce-resolution-on-the-right-to-privacy-in-the-digital/> (cit. 25.09.2025).

⁹ MELITO, Leandro: US espionage: recalling when WikiLeaks revealed NSA spied on former President Dilma Rousseff and members of her government. Brasil de Fato, 26 June 2024. Dostupné na: <https://www.brasildefato.com.br/2024/06/26/us-espionage-recalling-when-wikileaks-revealed-nsa-spied-on-former-president-dilma-rousseff-and-members-of-her-government/> (cit. 25.09.2025).

tohto sporu rozhodla na svojom území blokovať hlavné americké internetové spoločnosti a obmedziť ich pôsobenie v Číne. Zákazy sa síce stále dajú obísť, avšak aj tak veľmi oslabujú vplyv amerických spoločností v krajine. Čína vychádza z predstavy budovania vlastnej kybernetickej suverenity, ako základnej súčasti svojej štátnej suverenity. Podľa čínskeho názoru by bolo veľmi nebezpečné, ak by otázky, koho možno ako teroristu alebo extrémistu obmedzovať pri pôsobení v čínskom kyberpriestore určovali americké koncerny a nie čínske zákony.¹⁰ Samozrejme, nemožno pochybovať, že zákazy čínskych orgánov sú motivované aj inými dôvodmi. Existujú vážne podozrenia, že aj samotná Čína sa rozhodla spolupracovať s čínskymi technologickými spoločnosťami a presadzovať sa ich prostredníctvom vo svete. Nuž a tak ako sa hovorí o americkej GAFA, niekedy sa spomína aj čínsky BAT (Baidu, Alibaba, Tencent).¹¹ Niektoré internetové spoločnosti sa stali vďaka významným, iné však narazili na určité prirodzené prekážky. Napr. vyhľadávač Baidu je po Google druhým najväčším vyhľadávačom sveta, ale na Západe sa aj kvôli kultúrnym špecifikám pri vyhľadávaní príliš nepresadil a v globálnom merítku Google konkurovať nedokáže.¹² Čosi podobné platí aj pre známu čínsku sociálnu sieť RenRen.¹³ Na druhej strane, veľký úspech zaznamenala sociálna sieť TikTok, podobne ako technologická spoločnosť Huawei, ktoré sa kvôli tomu stali predmetom vyšetrovania štátnych orgánov v rôznych západných štátoch.¹⁴ Je zrejmé, že podozrenia zo spolupráce s čínskymi štátnymi orgánmi majú svoje racionálne jadro, len sa treba spýtať, či pri obmedzovaní podnikania čínskych technologických spoločností pôjde skutočne o ochranu kybernetickej suverenity, záujmov používateľov alebo ochranu dominantného postavenia tých monopolov, ktoré lepšie spolupracujú s tajnými službami západných štátov.

Nezávislosť v oblasti kyberpriestoru?

Samozrejme, že obraz boja medzi USA a Čínou o dominanciu v kyberpriestore je komplikovanejší a tajné služby týchto dvoch štátov majú dosah aj na technologické

¹⁰ TECH CRUNCH: China Blocks Access to Twitter, Facebook after Riots. Tech Crunch, 7 July 2009. Dostupné na: <https://techcrunch.com/2009/07/07/china-blocks-access-to-twitter-facebook-after-riots/?guccounter=2> (cit.25.09.2025).

¹¹ HONG Shen: China's Tech Giants: Baidu, Alibaba, Tencent. Konrad Adenauer Stiftung, July 2020, s. 33 a nasl.

¹² MUNAWAR, Atif: Baidu vs Google: 8 differences marketers need to know. EC Innovations, 17 September 2025. Dostupné na: <https://www.ecinnovations.com/blog/baidu-vs-google/> (cit.25.09.2025).

¹³ LIANG, Chengyu: Renren, Once China's Answer to Facebook, Is a Digital Ghost Town. Sixth Tone, 3 September 2018. Dostupné na: <https://www.sixthtone.com/news/1002846> (cit.25.09.2025).

¹⁴ FURCHT-GOTT-ROTH, Harold: Chinese Government helps Huawei with 5G. Forbes, 8 May 2017. Dostupné na: <https://www.forbes.com/sites/haroldfurchtgottroth/2017/05/08/chinese-government-helps-huawei-with-5g/> (cit.25.09.2025).

spoločnosti z iných krajín, napr. z Južnej Kórey. Existujú však štáty, ktoré sa voči týmto snahám o dominancie vymedzujú. Napr. v Rusku si štátna moc udržuje vplyv nad známym vyhľadávačom Yandex, ako aj nad spoločnosťou mail.ru, resp. nad sociálnou sieťou v kontakte.¹⁵ Samozrejme, spôsob, akým si štát vytvoril kontrolu nad touto sociálnou sieťou bol veľmi sporný a viedol aj k odchodu známeho inovátora Pavla Durova z Ruska.¹⁶ Ten zostal presvedčeným zástancom slobodného Internetu, odmietol spoluprácu so štátnou mocou pri udalostiach na Ukrajine v roku 2014 a rozhodol sa, že vytvorí novú **sociálnu sieť mimo Ruska**. Značné zdroje, ktorými disponoval, mu umožnili vytvorenie sociálnej siete Telegram s centrom v Berlíne, ktorá sa však v roku 2017 presunula do Dubaja. Vzhľadom na svoju kvalitu i postoj k slobode si získal Telegram postupne veľkú popularitu verejnosti a aj nezanedbateľný vplyv. Niektorých európskych politikov však lákala možnosť, že by sa im podarilo rozvinúť úzku spoluprácu s touto sociálnou sieťou. Daná spolupráca by bola výhodná aj preto, že práve na Telegram sa presunulo mnoho subjektov, znechutených z rastúcej cenzúry a obmedzovania slobody prejavu na iných platformách.

Pavel Durov sa v roku 2021 stal o. i. aj občanom Francúzska, avšak 24. augusta 2024 pri návšteve tejto krajiny bol zadržaný. Dôvodom sa stalo 12 obvinení z trestných činov.¹⁷ Väčšinu tvorili obvinenia zo spoluúčasti pri rôznych trestných činoch, od pedofílie až po podvody, ďalej z kryptologických služieb pre organizovaný zločin, vytvárania zločineckej skupiny, atď. Táto „spoluúčasť“ mala spočívať v nespolupráci so štátnymi orgánmi pri postupe voči kriminalite tretích strán na platforme Telegram.

Sám Pavel Durov v prvej verejnej reakcii po incidente uviedol: *„Francúzske orgány mali mnoho spôsobov, ako ma kontaktovať a požiadať o pomoc. Ako francúzsky občan som často navštevoval francúzsky konzulát v Dubaji... Ak je krajina nespokojná s internetovou službou, podľa zavedenej praxe začne súdny spor proti samotnej službe. Použitie zákonov éry pred smartfónmi na obvinenie riaditeľa zo zločinov spáchaných tretími stranami na platforme, ktorú spravuje, je nesprávny prístup. Vytváranie technológií nie je jednoduché. Žiadny inovátor nevytvorí nové nástroje, ak vie, že môže byť osobne zodpovedný za potenciálne zneužitie týchto nástrojov.“*¹⁸ Durov ďalej

¹⁵ [РБК](#): Друзья за \$1,47 млрд: как соцсеть «ВКонтакте» перешла в руки Усманова. [РБК](#), 16 September 2014. Dostupné na: <https://www.rbc.ru/business/16/09/2014/54240224cbb20f324f30ee7d> (cit.25.09.2025).

¹⁶ Tamže.

¹⁷ TRIBUNAL JUDICIAIRE DE PARIS: Communiqué de Presse. Paris, le 26 août 2024. Dostupné na: <https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf> (cit.25.09.2025).

¹⁸ DUROV, Pavel: Thanks everyone for your support and love! Telegram, status, 5 September 2024. Dostupné na: <https://t.me/durov/342> (cit.25.09.2025).

uviedol, že Telegram intenzívne moderuje obsah a komunikuje aj s vládami pri hľadaní rovnováhy medzi dôvernosťou a bezpečnosťou. Ak však s konkrétnym štátom nenájdu zhodu, sú pripravení daný trh opustiť. Pavel Durov to v statuse vyjadril takto: „*Sme vedení snahou konať dobro a chrániť základné práva ľudí, najmä tam, kde sú tieto práva porušované.*“¹⁹ Nemožno však vylúčiť, že francúzske orgány sa pokúšali primäť Pavla Durova k vyššej miere spolupráce práve obmedzením osobnej slobody.

Umelá inteligencia a zánik strednej triedy?

Zásadnou výzvou pre uvedené kybernetické impériá sa stáva téma umelej inteligencie, ktorá ponúka možnosti pre nástup nových globálnych spoločností. Ide o podobnú výzvu, aká nastala pred 250 rokmi počas prvej priemyselnej revolúcie, ktorá vytvorila novú spoločnosť a nové formy ekonomických vzťahov. V konečnom dôsledku viedla k tomu, že v súčasnej Európe žijeme v bohatstve a prosperite, oslobodila ľudí od rôznych fyzicky náročných činností, ponúkla nové príležitosti pre rozvoj, a pod. Teraz ale nastáva ďalší zásadný zlom, keď tento vek postupne končí a objavuje sa nová éra technologického pokroku. Pri priemyselnej revolúcii 19. storočia bola ľudská ruka nahradená mechanickou silou, v 21. storočí sa však nahradzuje ľudský mozog - nie vo všetkých, ale v mnohých, často i základných oblastiach. Ani to samotné by nemuselo byť dôvodom na obavy, pretože z dlhodobého hľadiska by mohla byť výsledkom ešte blahobytnější spoločnosť než v súčasnosti. Cesta k nej však bude zrejme zložitá a ak nestihneme zareagovať na určité výzvy včas, potom sa dostaneme do podobne veľkých problémov, aké sa vyskytovali počas priemyselnej revolúcie v 19. storočí. Vtedy vznikli problémy s neprimerane dlhým pracovným časom zamestnancov, ich nízkym vekom dožitia, ale problémom bola aj rozšírená detská práca v baniach či v textilnom priemysle.²⁰ V mnohých novovznikajúcich priemyselných odvetviach panovali neľudské pracovné podmienky. To viedlo k nespokojnosti širokých vrstiev obyvateľstva, k intenzívnemu triednemu boju, vzniku revolučných hnutí, k násiliu a vojnám. Pri súčasnej technologickej revolúcii sa tiež objavuje nespokojnosť a nerovnosť, ale treba sa pokúsiť predísť ďalšiemu rozmachu týchto negatívnych javov.

V súčasnosti je najväčšou obavou nahradzovanie pracovnej sily novými technológiami, ovládaných umelou inteligenciou. World Economic Forum čakáva, že

¹⁹ Tamže.

²⁰ BRIE, Michael: [Gründungsdokument des wissenschaftlichen Sozialismus: Engels' Die Lage der arbeitenden Klasse in England als praktisch eingreifende verbindende Erzählung](#). In: PROKLA. Zeitschrift für kritische Sozialwissenschaft. Roč. 50, 3/2020, s. 556 a nasl.

asi 92 miliónov pracovných miest vďaka automatizácii úplne zanikne.²¹ OECD Employment Outlook zasa predpokladá, že štvrtina pracovných miest sa ocitne v ohrození.²² Kai-Fu Lee, jeden z najznámejších technologických expertov, dokonca predpovedá, že umelá inteligencia odstráni 40 percent pracovných miest na svete do 15 rokov.²³ Tiež poukazuje na to, že vedúci pracovníci sú pod obrovským tlakom akcionárov a predstavenstiev, aby maximalizovali krátkodobé zisky, takže sa od nich žiada, aby automatizovali veľmi rýchlo.

Umelá inteligencia sa naozaj stáva likvidátorom pracovných miest – mnohé z nich určite zaniknú, avšak spolu s ich zánikom pôjdu ruka v ruke ďalšie problémy – znížia sa aj daňové príjmy. Nepôjde pritom iba o pokles výnosov z priamych daní, ale bez príjmu ľudia nebudú ani toľko konzumovať a umelá inteligencia už vôbec nie – preto poklesnú aj výnosy zo spotrebných daní či dane z pridanej hodnoty. Súčasne je očividné, že pri strate zamestnanosti bude musieť štát podporovať rastúce množstvo nezamestnaných ľudí. Potreba ďalších daňových príjmov vznikne aj preto, že nové technológie zväčšia priepasť medzi bohatými a chudobnými. To všetko môže mať vážne následky pre verejné rozpočty. Keďže umelá inteligencia nebude platiť ani odvody, sociálne systémy sa bez príspevkov od pracujúcich dostanú do problémov. Už dnes sa pritom veľa hovorí o kríze dôchodkového zabezpečenia kvôli demografickému vývoju, avšak naše systémy sociálneho zabezpečenia či zdravotného poistenia sa môžu zrútiť ešte skôr práve z dôvodu, že existujúce pracovné miesta sa postupne nahradia systémami umelej inteligencie.²⁴ Kvôli uvedeným argumentom je treba už teraz riešiť otázku, ako sa s týmto problémom vysporiadame, a naopak, ktoré príležitosti vyplývajúce z nástupu umelej inteligencie využijeme.

Do budúca možno predpokladať, že z rastúcich ziskov zo zavedenia umelej inteligencie budú profitovať najmä tí, ktorí dokážu do nových technológií investovať dostatočné množstvo kapitálu. Naopak tí, ktorí sú závislí od príjmu z vlastnej práce, sa kvôli umelej inteligencii ocitnú v ohrození, zvlášť kvôli hroziacej strate zamestnania. Zásadnou otázkou preto je, ako sa s týmto problémom vysporiadame a aký druh základného zabezpečenia by bolo možné do budúcnosti vytvoriť. Zvlášť veľké obavy treba mať o o ľudí v profesiách, ktorí vykonávajú rutinnú intelektuálnu

²¹ WORLD ECONOMIC FORUM: Future of Jobs Report 2025. World Economic Forum, 8 January 2025. Dostupné na: <https://www.weforum.org/stories/2025/01/future-of-jobs-report-2025-jobs-of-the-future-and-the-skills-you-need-to-get-them/> (cit. 25.09.2025).

²² BASSANTINI, Andrea – BROECKE, Stijn. (eds): OECD Economic Outlook 2023. OECD. Artificial Intelligence and Labour Market, OECD Publications, 2025. 307, s. 116.

²³ KAI-FU, Lee: AI Superpowers. China, Silicon Valley, and the new world order. Houghton Mifflin Harcourt, 2021. 272, s. 240 a nasl.

²⁴ PRECHT, Richard: Hirten, Jäger, Kritiker. Eine Utopie für digitale Gesellschaft. München. Goldmann, 2020, s. 142 a nasl.

prácu a v budúcnosti prídu o zamestnanie bez vlastnej viny vo veku 40 alebo 50 rokov, pretože pracovali v banke, na úrade alebo dokonca ako advokáti. Práve u týchto skupín osôb možno očakávať pokles ich kúpnej sily a klesajúce spoločenské uznanie. Nie je úplne jasné, aká časť takýchto pracovných vzťahov zanikne, určite sa to však dotkne významnej časti populácie. Pôjde pritom najmä o strednú triedu, ktorá vykonáva uvedenú rutinnú intelektuálnu prácu v bankách, na úradoch alebo v právnických profesiách.²⁵ To povedie k politickej nestabilite, lebo títo príslušníci strednej triedy boli tradične vnímaní ako stabilizujúci faktor v spoločnosti. Samozrejme, že sa vytvoria aj úplne nové pracovné miesta a určite bude treba dátových analytikov, dizajnérov virtuálnej reality či nových ľudí v oblasti geriatrickej starostlivosti. Možno však pochybovať, že zamestnanec banky vo veku 50 rokov, ktorý prišiel o prácu, sa ani po preškolení nestane dátovým analytikom. Rovnako len ťažko možno očakávať, že sa dokáže uplatniť v oblasti geriatrickej alebo zdravotnej starostlivosti. Samozrejme, objavajú sa aj výnimky, avšak väčšina ľudí, ktorí stratili prácu, nezačne pracovať na pracovných miestach, ktoré sa v budúcnosti vytvoria. Skôr je pravdepodobné, že bude existovať súčasne problém s prebytkom i nedostatkom pracovných síl na trhu. Rozhodujúca však nebude preto ani tak otázka, či v budúcnosti vznikne viac alebo menej pracovných miest, ale to, ako bude vyzeráť budúcnosť príslušníkov upadajúcej strednej triedy.

Návrat do minulosti?

Jedným z hlavných problémov súčasných spoločností je veľká daňová a odvodová nespravodlivosť a práve tento jav sa prehlbuje pôsobením dominantných kybernetických spoločností. Podľa Fair Tax Foundation za posledných desať rokov tzv. Silicon Six vygenerovala za desať rokov príjmy vo výške 11 biliónov dolárov, avšak rozdiel medzi sadzbami dane a skutočne zaplatenými daňami z príjmu právnických osôb bol 277,8 miliárd USD.²⁶ Big Tech teda všeobecne pravdepodobne platí oveľa nižšie sadzby dane z príjmu právnických osôb (a dane zo ziskov všeobecnejšie) ako subjekty v iných vysoko ziskových odvetviach, napr. v energetike.

To predstavuje problém pre malých podnikateľov, dôležitých z hľadiska príjmov do štátnych rozpočtov. Skúsme si napr. predstaviť majiteľa kníhkupectva na Slovensku, ktorý musí riadne platiť daň z príjmu a porovnať ho s koncernom Amazon, ktorý platí na daniach len zlomok zo svojich európskych príjmov.²⁷ Samozrejme, tento problém

²⁵ Tamže, s. 116 a nasl.

²⁶ FAIR Tax Foundation: The Silicon Six and their enduring global tax gap. Fair Tax Foundation, April 2025, s. 7. Dostupné na: <https://fairtaxmark.net/wp-content/uploads/Silicon-Six-Report-2025.pdf> (cit.25.09.2025).

²⁷ SWENEY, Mark: Amazon paid just £15m in tax on European revenues of £19.5bn. Guardian, 10 August 2017. Dostupné na: <https://www.theguardian.com/technology/2017/aug/10/amazon-uk-halves-its-corporation-tax-to-74m-as-sales-soar-to-7bn> (cit.25.09.2025).

nespôsobujú len kybernetické spoločnosti, ale čosi podobné platí pre Starbucks, ktorý súťaží s malými vlastníkmi kaviarní, či McDonalds, ktorý súťaží s malými lokálnymi reštauráciami. Avšak hoci sa daňová „optimalizácia“ a systém daňových rajov nedá obmedziť len na tzv. Big Tech, práve jeho pôsobenie predstavuje ďalšiu eskaláciu negatívnych trendov v daňovej oblasti. Tento trend ekonomickej nespravodlivosti často vedie k nespravodlivým javom. Vzhľadom na verejné financie sa často tematizuje „zneužívanie“ sociálnych dávok nemajetnými osobami, na zneužívanie daňových inštitútov veľkými ekonomickými subjektami sa však hľadí ako na „gavaliersky delikt“.

V súčasnosti sme sa tak dostali do situácie, ktorá z veľkej časti pripomína neblahé javy z minulosti. Prostredníctvom daňových „optimalizácií“ sa totiž vytvára návrat feudálnych praktík, keď existovali privilegované skupiny obyvateľov (šľachta a vysoký klérus), ktoré boli z väčšej časti zbavené daňových povinností. Takto to fungovalo i vo Francúzsku **pred Veľkou francúzskou revolúciou**, keď tzv. tretí stav tvorený živnostníkmi a sedliakmi znášal celé finančné bremeno štátnych výdavkov.²⁸ Generálne stavy, ktoré kráľ zvolal na rok 1789, mali legalizovať ďalšie zvýšenie daňového bremena tretieho stavu, avšak tento to odmietol a vyvolal revolúciu. V súčasnosti sa situácia z daného obdobia opakuje. Daňové bremeno sa čoraz viac prenáša na menej majetné skupiny obyvateľstva, zatiaľ čo **najbohatší platia iba nepatrné dane**. To musí nutne vyvolávať nespokojnosť. Podobne veľkú nespokojnosť vyvolávajú opakujúce sa škandály spojené s „optimalizáciou daní“ či s daňovými rajmi ako Panama Papers, Paradise Papers, Pandora Papers, atď. Mediálne materiály dokazujúce obrovské daňové úniky sa stali významným poukazom na nespravodlivosti súčasného ekonomického systému, ich potenciál je však obmedzený. Aj pri týchto škandáloch sa totiž niektoré informácie obchádzajú a skupina dôležitých subjektov býva zo škandálu vyňatá...

Napr. nemecký denník *Süddeutsche Zeitung*, ktorý sa podieľal na zverejnení informácií v Panama Papers, odmietol poskytnúť informácie nielen verejnosti, ale aj orgánom činným v trestnom konaní. Napísal: „*SZ neposkytne údaje k dispozícii ani verejnosti ani orgánom činným v trestnom konaní. Pretože SZ nie je predĺženou rukou prokuratúry, ani daňových vyšetrovateľov. Štátne vyšetrovacie orgány v Nemecku či v zahraničí majú už teraz, pri odôvodnenom podozrení, možnosť zhabať príslušné dokumenty.*“²⁹

²⁸ NORBERG, Kathryn: The French Fiscal Crisis of 1788 and the Financial Origins of the Revolution of 1789. In: HOFFMAN, Phillip – NORBERG, Kathryn (eds.): *Fiscal Crises, Liberty and Representative Government, 1450–1789*. Stanford, CA: Stanford University Press, 1994, s. 256.

²⁹ KRACH, Wolfgang: Häufige Fragen zu Panama Papers – und Antworten. *Süddeutsche Zeitung*, 5. April 2016. Dostupné: <https://www.sueddeutsche.de/politik/panama-papers-haeufige-fragen-zu-panama-papers-und-antworten-1.2935507> (cit. 25.09.2025).

Zverejňujú sa hlavne informácie o osobách, ktoré sú mediálne zaujímavé, napr. politici, avšak mnohé ekonomicky vplyvné subjekty sa v mediálnych zoznamoch neobjavujú. *Süddeutsche Zeitung* to vysvetlil takto: „Ak prominentný nemecký bankový manažér skryl svoj dom na Mallorke do schránkovej firmy, ale riadne zaplatil dane, nie je pre nás v princípe dôvod, aby sme o tom informovali.“³⁰

Situáciu z minulých storočí veľmi pripomína aj dominancia veľkých ekonomických subjektov nad politikou. Napr. pre Východoindickú spoločnosť vo Veľkej Británii v 18. a začiatkom 19. storočia nebolo rozhodujúce, kto stojí na čele štátu. V samotnej Indii táto spoločnosť formálne uznávala suverenitu Veľkého mogula a pomerne dlho vyberala dane či vykonávala svoje práva v jeho mene.³¹ Nebola však na jeho moci závislá. Podmienkou jej moci bol monopol na obchod s Indiou, čo sa podarilo dosiahnuť po spojení tzv. londýnskej a tzv. anglickej Východoindickej spoločnosti (1708)³². Vývoj v krajine tak určovalo dominantné postavenie jednej obchodnej spoločnosti. Tento monopol trval hlboko do 19. storočia a až do roku 1858 mal podnik dominantné postavenie na indickom subkontinente, čo robilo akúkoľvek trhovú súťaž iluzórnou. Avšak keď sa veľká obchodná spoločnosť dostala do úpadku po povstaní 1857-58, jej záväzky prebral na seba britský štát.³³ Trochu podobne to platí aj v súčasných štátnych celkoch, kde nie je rozhodujúce, kto stojí na čele jednotlivých vlád. Samozrejme, veľmi dôležitým aspektom súčasného pôsobenia kybernetických spoločností je to, že pôsobia cezhranične a to v podstatne väčšom rozsahu než mohli veľké ekonomické subjekty v minulých storočiach.

Nové myslenie ako záver?

Aby sme sa dokázali obmedziť vyššie uvedené javy, je potrebné zmeniť niekoľko predstáv o spoločnosti, ktoré v súčasnosti dominujú.

Predovšetkým v oblasti sociálnej a ekonomickej spravodlivosti treba opustiť predstavu z 19. storočia o závislosti dôchodkových systémov od odvodov, viazaných na prácu. Keďže umelá inteligencia nahradí príliš veľké množstvo pracujúcich a súčasne prichádza k starnutiu populácie, nemožno očakávať, že súčasný model dôchodkového systému so zaťažením práce je perspektívny. Riešením nie je ani neustále zvyšovanie veku odchodu do dôchodku, ani ústavné zakotvenie určitých foriem dôchodkového systému. Právny stav, ktorý bude existovať o niekoľko desiatok rokov, nemožno predvídať a medzitým môže tzv. druhý pilier

³⁰ Tamže.

³¹ SPEAR, Percival: *Oxford History of Modern India*. Dehli – New York: Oxford University Press, 1978. 472. s. 47 a nasl.

³² STRNAD, Jaroslav – FILIPOVSKÝ, Jan – HOLMAN, Jaroslav – VAVROUŠKOVÁ, Stanislava: *Dějiny Indie*. Praha: Lidové Noviny, s. 621-622.

³³ Tamže, s. 737 a nasl.

dôchodkového sporenia zaniknúť, ako v niektorých štátoch Latinskej Ameriky, napr. v Argentíne.³⁴ Umelá inteligencia síce odvody neplatí, ale vytvára obrovské množstvo bohatstva, ktorého malá časť môže znamenať riešenie problému s dôchodkovými systémami. Samostatnou témou v tejto súvislosti môže byť aj otázka tzv. nepodmieneného príjmu, ktorý by predstavoval riešenie i pre narastajúci počet osôb vyradených z pracovného procesu práve umelou inteligenciou. I keď táto téma by si zaslúžila samostatné spracovanie.

Druhou zásadnou výzvou pre nové myslenie je prehodnotenie nášho prístupu k základným právam. V období priemyselnej revolúcie z 19. storočia dominoval ekonomický model, ktorý predpokladal, že v konkurencii sa presadia len podniky, ktoré budú málo hľadiť na sociálne práva pracujúcich (mzda, pracovný čas) a budú udržiavať nízke náklady, dnes existuje podobne bezohľadný ekonomický model, ktorý porušuje právo na súkromie a dáta užívateľov. Často sú to práve „bezplatné“ služby, ktoré sa koncernom vyplatia prostredníctvom dát o užívateľoch. Porušovanie práv týchto osôb veľmi prispelo k poklesu dôveru v štátne inštitúcie a platné právo štátov. V danej súvislosti je treba viac zdôrazňovať práva vyplývajúce z Charty základných práv EÚ, najmä tie, ktoré sa týkajú práva na súkromie a ochrany dát.³⁵ Súčasne je výzvou téma vytvorenia európskych kybernetických koncernov, ktoré by boli konkurentom kybernetickým monopolom z USA a Číny, aspoň v európskom kyberpriestore.³⁶

Tretou veľkou výzvou pre nové myslenie je potreba obratu vzťahu medzi Big Tech a štátnymi inštitúciami. V súčasnom svete totiž prichádzajú nové idey zo Silicon Valley alebo z iných technologických centier a politika na ne iba reaguje. Tiež prichádza k digitálnej manipulácii politického rozhodovania, čo umožňuje technologickým spoločnostiam zasahovať do politiky a znemožňovať iniciatívy, ktoré by boli pre ne neželané. Pôsobenie veľkých kybernetických spoločností pritom ohrozuje aj základné demokratické princípy. Vzhľadom na to, že EÚ nemá vlastnú sústavu veľkých kybernetických koncernov, mala by sa usilovať o vymanenie sa z daného vplyvu a vytvárať nové idey práve vo vzťahu k týmto veľkým spoločnostiam. Avšak dokonca aj v oblastiach, kde EÚ predkladá vlastné predstavy regulácie, napr. AI Act, ponecháva viacero oblastí neregulovaných, napr. sektor obrany.³⁷ Tým umožňuje kybernetickým spoločnostiam vyhnúť sa svojim povinnostiam.

Keď sa EÚ v minulosti vytvárala, jedným z jej hlavných argumentov bolo, že v globalizovanom svete poskytuje lepšie možnosti ochrany práv jednotlivcov proti

³⁴ FERRO, Gustavo – CASTAGNOLO, Fernando: On the closure of the Argentine fully funded system. *Pensions International Journal* 15/2010, 25–37, s. 29 a nasl.

³⁵ Charta základných práv Európskej únie (2016/C 202/02), najmä čl. 7 a 8.

³⁶ MITRACHE, Marius-Mircea: France's Grand Design for Europe and the Elusive Quest for European Sovereignty. *Political Studies Forum*, 1/2021, s. 23–42.

³⁷ Nariadenie EP a Rady 2024/1689, čl. 2 ods. 3.

veľkým ekonomickým subjektom než národné štáty. Práve oblasť kyberpriestoru je tou sférou, kde by mohla danú tézu potvrdiť a práve tým posilniť svoju vlastnú legitimitu.

Zoznam použitej literatúry

1. Alphabet Inc. (GOOG). Finance.yahoo.com, 30 June 2025. Dostupné na: <https://finance.yahoo.com/quote/GOOG/holders/> (cit.25.09.2025)
2. AUST, Stefan – AMMANN, Thomas: Digitale Diktatur. Berlin: Ulstein, 2016, 352 s.
3. BASSANTINI, Andrea – BROECKE, Stijn. (eds): OECD Economic Outlook 2023. OECD. Artificial Intelligence and Labour Market., OECD Publications, 2025. 307 s.
4. BRIE, Michael: [Gründungsdokument des wissenschaftlichen Sozialismus: Engels' Die Lage der arbeitenden Klasse in England als praktisch eingreifende verbindende Erzählung](#). In: PROKLA. Zeitschrift für kritische Sozialwissenschaft. Roč. 50, 3/2020, s. 553-560
5. BROWN, Deborah: Brasil, Germany introduce resolution on The Right to Privacy in the Digital Age in UN General Assembly. AccesNow, 1 November 2013. Dostupné na: <https://www.accessnow.org/brazil-germany-introduce-resolution-on-the-right-to-privacy-in-the-digital/> (cit.25.09.2025)
6. DOUROV, Pavel: Thanks everyone for your support and love! Telegram, status, 5 September 2024. Dostupné na: <https://t.me/durov/342> (cit.25.09.2025)
7. Fair Tax Foundation: The Silicon Six and their enduring global tax gap. Fair Tax Foundation, April 2025. Dostupné na: <https://fairtaxmark.net/wp-content/uploads/Silicon-Six-Report-2025.pdf> (cit.25.09.2025)
8. FERRO, Gustavo – CASTAGNOLO, Fernando: On the closure of the Argentine fully funded system. Pensions International Journal, 15/2010, s. 25–37
9. FURCHTOTT-ROTH, Harold: Chinese Government helps Huawei with 5G. Forbes, 8 May 2017. Dostupné na: <https://www.forbes.com/sites/haroldfurchtgottroth/2017/05/08/chinese-government-helps-huawei-with-5g/> (cit.25.09.2025)
10. HONG Shen: China's Tech Giants: Baidu, Alibaba, Tencent. Konrad Adenauer Stiftung, July 2020, s. 33-41
11. Charta základných práv Európskej Únie (2016/C 202/02)
12. INVESTING.COM: Who owns Alphabet? GOOGLE Shareholders. Investing.com, 30 June 2025. Dostupné na: <https://www.investing.com/equities/google-inc-ownership> (cit.25.09.2025)
13. KAI-FU Lee. AI Superpowers. China, Silicon Valley, and the new world order. Hofton Milffinn Harcourt, 2021. 272 s.

14. KARHULA, Päivikki: What is the effect of WikiLeaks for Freedom of Information? International Federation of Library Associations and Institutions, 19 January 2011. Dostupné: <https://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information/> (cit.25.09.2025)
15. KRACH, Wolfgang: Häufige Fragen zu Panama Papers – und Antworten. Süddeutsche Zeitung, 5. April 2016. Dostupné: <https://www.sueddeutsche.de/politik/panama-papers-haeufige-fragen-zu-panama-papers-und-antworten-1.2935507> (cit.25.09.2025)
16. LIANG Chengyu: Renren, Once China's Answer to Facebook, Is a Digital Ghost Town. Sixth Tone, 3 September 2018. Dostupné: <https://www.sixthtone.com/news/1002846> (cit.25.09.2025)
17. MELITO, Leandro: US espionage: recalling when WikiLeaks revealed NSA spied on former President Dilma Rousseff and members of her government. Brasil de Fato, 26 Jun 2024. Dostupné: <https://www.brasildefato.com.br/2024/06/26/us-espionage-recalling-when-wikileaks-revealed-nsa-spied-on-former-president-dilma-rousseff-and-members-of-her-government/> (cit.25.09.2025)
18. MITRACHE, Marius-Mircea: France's Grand Design for Europe and the Elusive Quest for European Sovereignty. Political Studies Forum, 1/2021, s. 23-42.
19. MUNAWAR, Atif: Baidu vs Google: 8 differences marketers need to know. EC Innovations, 17 September 2025. Dostupné na: <https://www.ecinnovations.com/blog/baidu-vs-google/> (cit.25.09.2025)
20. Nariadenie EP a Rady 2024/1689 z 13. júla 2024, ktorým sa harmonizujú pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)
21. NORBERG, Kathryn: The French Fiscal Crisis of 1788 and the Financial Origins of the Revolution of 1789. In: HOFFMAN, Phillip – NORBERG, Kathryn (eds.): Fiscal Crises, Liberty and Representative Government, 1450–1789. Stanford, CA: Stanford University Press, 1994, s. 253-298.
22. PRECHT, Richard: Hirten, Jäger, Kritiker. Eine Utopie für digitale Gesellschaft. München. Goldmann, 2020, s. 142 a nasl.
23. RAMONET, Ignacio: Impero de la vigilancia. Buenos Aires: Capital Intelectual, 2016, 160 s.
24. SEMINARA, Jole: Market Dominance of GAFA companies and challenges posed to competition policy? Tesi di Laurea Magistrale. Politecnico di Torino, 2019. 126 s.
25. SPEAR, Percival: Oxford History of Modern India. Dehli – New York: Oxford University Press, 1978. 472 s.

26. STRNAD, Jaroslav – FILIPOVSKÝ, Jan – HOLMAN, Jaroslav – VAVROUŠKOVÁ, Stanislava: Dějiny Indie. Praha: Lidové Noviny, 2003, 1190 s.
27. SWENEY, Mark: Amazon paid just £15m in tax on European revenues of £19.5bn. Guardian, 10 August 2017. Dostupné na: <https://www.theguardian.com/technology/2017/aug/10/amazon-uk-halves-its-corporation-tax-to-74m-as-sales-soar-to-7bn> (cit.25.09.2025)
28. TECH CRUNCH: China Blocks Accrs to Twitter, Facebook after Riots. Tech Crunch, 7 July 2009. Dostupné na: <https://techcrunch.com/2009/07/07/china-blocks-access-to-twitter-facebook-after-riots/?guccounter=2> (cit.25.09.2025)
29. TRIBUNAL JUDICIAIRE DE PARIS: Communiqué de Presse. Paris, le 26 août 2024. Dostupné na: <https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf> (cit.25.09.2025)
30. WORLD ECONOMIC FORUM: Future of Jobs Report 2025. World Economic Forum, 8 January 2025. Dostupné na: <https://www.weforum.org/stories/2025/01/future-of-jobs-report-2025-jobs-of-the-future-and-the-skills-you-need-to-get-them/> (cit.25.09.2025)
31. РБК: Друзья за \$1,47 млрд: как соцсеть «ВКонтакте» перешла в руки Усманова. РБК, 16 September 2014. Dostupné na: <https://www.rbc.ru/business/16/09/2014/54240224cbb20f324f30ee7d> (cit.25.09.2025)

Kontaktné údaje

doc. JUDr. Branislav Fábry, PhD.

branislav.fabry@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

NÁHRADA ŠKODY ZA PORUŠENIE GDPR – PRÁVNA ÚPRAVA MEDZINÁRODNEJ PRÁVOMOCI¹

COMPENSATION FOR DAMAGE CAUSED BY GDPR INFRINGEMENT – INTERNATIONAL JURISDICTION

Katarína Burdová²

Abstrakt: Článok skúma rozsah a limity ustanovenia článku 79 ods. 2 GDPR v kontexte civilných konaní o náhradu škody, ktorú si dotknutá fyzická osoba uplatňuje voči prevádzkovateľovi alebo sprostredkovateľovi. Analýza sa zameriava na vzťah tohto ustanovenia k systému medzinárodnej právomoci podľa nariadenia Brusel Ia a nového Lugánskeho dohovoru, pričom poukazuje na interpretačné nejasnosti, ktoré pretrvávajú a môžu negatívne ovplyvniť realizáciu práva dotknutej osoby na účinný súdny prostriedok nápravy voči prevádzkovateľovi a sprostredkovateľovi, ktoré je zakotvené v článku 79 ods. 1 GDPR. Štúdia identifikuje kľúčové otvorené otázky týkajúce sa najmä pojmov prevádzkareň a obvyklý pobyt dotknutej osoby – a ich dopadov na predvídateľnosť fóra z pohľadu žalovaného. Osobitná pozornosť sa venuje situáciám s väzbou na štáty mimo EÚ a možnostiam spojenia konaní voči viacerým žalovaným. Záver zdôrazňuje, že judikatúra Súdneho dvora Európskej únie k týmto otvoreným otázkam môže priniesť stabilizáciu aplikačnej praxe a prispieť k dosiahnutiu rovnováhy medzi ochranou práv dotknutých osôb a požiadavkami právnej istoty v cezhraničných sporoch.

Kľúčové slová: medzinárodná právomoc, GDPR, nariadenie Brusel Ia, náhrada škody

Abstract: The article examines the scope and limitations of Article 79(2) of the GDPR in the context of civil proceedings for damages claimed by a data subject against a controller or processor. The analysis focuses on the relationship

¹Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17Ro5-04-V01-00002 (Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality) Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No.17Ro5-04-V01-00002 (Competence Center for the Regulation of Cybersecurity, Privacy Protection and Cybercrime).

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra medzinárodného práva a medzinárodných vzťahov.

between this provision and the system of international jurisdiction under the Brussels Ia Regulation and the new Lugano Convention. It highlights the ongoing interpretative uncertainties that could negatively impact the data subject's right to an effective judicial remedy against the controller or processor, as guaranteed by Article 79(1) of the GDPR. Key open issues, particularly concerning the concepts of "establishment" and "habitual residence" of the data subject and their impact on the foreseeability of the forum from the defendant's perspective, are examined. Particular attention is devoted to situations involving connections to non-EU states, as well as to the possibility of joining proceedings against multiple defendants. The conclusion emphasizes that the case law of the Court of Justice of the European Union on these unresolved issues could stabilize judicial practice and lead to achieving a balance between protecting the rights of data subjects and ensuring legal certainty in cross-border disputes.

Key words: international jurisdiction, GDPR, Brussels Ia Regulation, compensation for damage

Úvod

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)³ (ďalej len „GDPR“) zakotvuje nielen verejnoprávne prostriedky vymáhania práva ochrany osobných údajov⁴ ale aj prostriedky súkromnoprávne.⁵ Jadrom právnej úpravy prostriedkov súkromnoprávneho vymáhania sú o. i. ustanovenia článkov 82, 79

3 Ú. v. EÚ L 119, 4.5.2016, s. 1–88 Toto nariadenie zrušilo smernicu Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (ďalej len „smernica 95/46/EHS“) Ú. v. ES L 281, 23.11.1995, s. 31 – 50.

⁴ Najmä v ustanoveniach čl. 77 a čl. 78 ods. 1 GDPR.

⁵ Pri vymedzení tohto pojmu budeme vychádzať z vymedzenia, ktoré na účely antimonopolného práva podáva Kalesná, ktorá uvádza: „Súkromnoprávnym vymáhaním antimonopolného práva sa potom rozumie dovolávanie sa porušenia verejného súťažného práva v súkromnoprávných sporoch medzi dvoma a viacerými subjektmi súkromného práva. Riešenie týchto sporov prislúcha civilným súdom a ich ťažisko spočíva v rozhodovaní o nároku na náhradu škody z porušenia súťažného práva.“ KALESNÁ, Katarína: Bude fungovať súkromnoprávne vymáhanie súťažného práva? In: Právny obzor, roč. 101, č. 1, (2018), s. 54. Pričom pojem antimonopolné právo a súťažné právo nahradzame pojmom právo ochrany osobných údajov a pojem subjekty súkromného práva pojmom fyzická osoba a prevádzkovateľ a spracovateľ.

a článok 80⁶ GDPR.⁷ Súdny dvor Európskej únie⁸ potvrdil súbežné a nezávislé uplatnenie verejnoprávnych a súkromnoprávnych prostriedkov podľa tohto nariadenia.⁹

V súvislosti so súkromnoprávnym vymáhaním práva na ochranu osobných údajov je potrebné zdôrazniť význam článku 79 ods. 1 GDPR, ktorý priznáva dotknutej osobe právo na účinný súdny prostriedok nápravy uplatniteľný priamo voči prevádzkovateľovi a sprostredkovateľovi (ako je to explicitne uvedené v názve tohto článku)¹⁰, pričom stanovuje, že *„bez toho, aby bol dotknutý akýkoľvek dostupný správny alebo mimosúdny prostriedok nápravy vrátane práva na podanie sťažnosti dozornému orgánu podľa článku 77, každá dotknutá osoba má právo na účinný súdny prostriedok nápravy, ak sa domnieva, že v dôsledku spracúvania jej osobných údajov v rozpore s týmto nariadením došlo k porušeniu jej práv ustanovených v tomto nariadení.“*¹¹ S výnimkou autonómneho práva na náhradu škody v zmysle čl. 82

⁶ Článok 80 ods. 1 GDPR stanovuje, že *„dotknutá osoba má právo poveriť neziskový subjekt, organizáciu alebo združenie, ktoré boli riadne zriadené v súlade s právom členského štátu, ktorých ciele podľa stanov sú vo verejnom záujme a ktoré pôsobia v oblasti ochrany práv a slobôd dotknutých.“* Takéto ustanovenie smernica 95/46/ES neobsahovala.

⁷ K výhodám a nevýhodám súkromnoprávného vymáhania pozri bližšie napr. LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 217-220. V tejto súvislosti môže byť z hľadiska cezhraničných sporov osobitne zaujímavé, ako uvádza autorka, že rozsudky vydané na základe civilných žalôb v týchto veciach je jednoduché uznať a vykonať nielen v členských štátoch EÚ na základe nariadenia Brusel Ia, ale ich uznanie a výkon môže byť podstatne jednoduchšie aj v nečlenských štátoch EÚ a to v porovnaní s rozhodnutiami orgánov dohľadu.

⁸ Rozsudok Súdneho dvora (prvá komora) z 12. januára 2023 vo veci C-132/21 BE proti Nemzeti Adatvédelmi és Információszabadság Hatóság za účasti: Budapesti Elektromos Művek Zrt. ECLI:EU:C:2023:2

⁹ K otázke vzťahu súkromnoprávnych a verejnoprávnych prostriedkov pozri bližšie napr. RODRIGUEZ PINEAU, Elena: Parallel Litigation in Proceedings relating to Data Protection. In: PFEIFFER, Magdalena a kol. (eds.): Liber Amicorum Monika Pauknerová. Praha: Wolters Kluwer ČR, 2021, s. 395-404. Touto otázkou sa v súčasnosti zaoberá aj Súdny dvor Európskej únie a to na základe prejudiciálnej otázky podanej rakúskym Najvyšším správnym súdom, ktorá sa týka *„možnosti dozorného orgánu zamietnuť sťažnosť, ak bol predtým podaný súdny prostriedok nápravy s rovnakým predmetom, aj keď toto konanie ešte prebieha alebo keď rozhodnutie vydané v tomto konaní ešte nie je právoplatné.“* Návrhy generálneho advokáta Jean Richard De La Tour prednesené 4. septembra 2025 vo veci C-414/24 Datenschutzbehörde, Dr. G. S. za účasti: Bundesministerium für Justiz, D GmbH, ECLI:EU:C:2025:656.

¹⁰ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 220.

¹¹ Predchodcom tohto ustanovenia bol článok 22 smernice 95/46/ES.

vrátane ods. 6 tohto článku, GDPR¹² nezakotvuje ďalšie civilné súdne prostriedky nápravy a ich úpravu ponecháva členským štátom Európskej únie.

V tejto súvislosti sa preto zameriame na ustanovenie čl. 82 GDPR, ktoré zakladá právo fyzickej osoby¹³ na náhradu škody, ktorá vznikla v dôsledku porušenia GDPR zo strany prevádzkovateľa¹⁴ alebo spracovateľa,¹⁵ pričom v článku 82 ods. 6 GDPR je stanovené, že *„návrhy na začatie súdnych konaní na účely uplatnenia práva na náhradu škody sa podávajú na súdy príslušné podľa práva členského štátu uvedeného v článku 79 ods. 2.“*

Ustanovenie článku 79 ods. 2 GDPR je normou medzinárodného práva procesného, ktorá upravuje medzinárodnú právomoc civilných súdov členských štátov Európskej únie. A je to práve existencia medzinárodnej právomoci, ktorá zásadným spôsobom ovplyvňuje odpoveď na otázku, či dotknutá fyzická osoba bude mať možnosť dovolávať sa práva na náhradu škody, ktorú jej priznáva článok 82 GDPR v prípadoch s väzbou k viacerým právnym poriadkom súčasne a to nielen voči prevádzkovateľom a sprostredkovateľom z iných členských štátov EÚ ale aj z nečlenských štátov EÚ.

GDPR sa totiž z hľadiska teritoriálnej¹⁶ pôsobnosti vzťahuje tak na spracovanie osobných údajov zo strany prevádzkovateľov a sprostredkovateľov v rámci činnosti

¹² Predchodcom tohto ustanovenia bol článok 23 smernice 95/46/ES, ale smernica priznávala toto právo dotknutej osobe len voči prevádzkovateľovi. K tomu pozri bližšie REQUEJO ISIDRO Marta: La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679. In: LA LEY mercantil, č. 42, 2017, s. 5, ktorá dodáva, že podľa súčasnej právnej úpravy je každý prevádzkovateľ alebo sprostredkovateľ považovaný za zodpovedného za všetky škody, aby sa zabezpečilo účinné odškodnenie dotknutej osoby; inými slovami, podľa článku 82 ods. 4 GDPR si dotknutá osoba môže zvoliť, či bude žiadať náhradu škody od prevádzkovateľa, sprostredkovateľa alebo od oboch.

¹³ Ako uvádzajú autori českého komentára k GDPR právnickej osobe nemôže vzniknúť v dôsledku porušenia povinností pri spracovaní osobných údajov škoda, pretože právnická osoba žiadne osobné údaje nemá. SEDLÁČEK, Dušan. Článek 82 [Právo na náhradu újmy a odpovědnost]. In: UŘIČAŘ, Miroslav - RÁMIŠ, Vladan a kol.: Obecné nařízení o ochraně osobních údajů. 1. vydání. Praha: C. H. Beck, 2021, ISBN 978 80 7400 815 3, s. 1192.

¹⁴ Článok 4 ods. 7 GDPR.

¹⁵ Článok 4 ods. 8 GDPR.

¹⁶ Bližšie k teritoriálnej pôsobnosti GDPR pozri MESARČÍK, Matúš: Apply or not to apply? A comparative view on territorial application of CCPA and GDPR. In: Bratislava Law Review, roč. 4, č. 2, (2020), s.81-94. Ako uvádza tento autor, GDPR je na základe článku 3 ods. 2 aplikovateľné aj v prípadoch, kedy prevádzkovateľ alebo sprostredkovateľ nie je usadený v EÚ ale sú splnené podmienky podľa čl. 3 ods.2 písm. a) alebo b) GDPR a zároveň v tejto súvislosti uvádza ako príklad situáciu, kedy je americká spoločnosť bez prevádzky v EÚ poskytovateľom mobilnej aplikácie sociálnej siete dostupnej a určenej spotrebiteľom z EÚ. Spracovanie osobných údajov dotknutých osôb používajúcich túto aplikáciu v Ríme alebo Paríži by spadalo, podľa tohto autora, do územnej pôsobnosti GDPR. Situácia by bola iná, ak by aplikácia bola určená iba pre americký trh a nebola by dostupná na stiahnutie v Európskej únii. MESARČÍK, Matúš: Apply or not to apply? A comparative view on territorial application of CCPA and GDPR. In: Bratislava Law Review, roč. 4, č. 2, (2020), s. 86.

prevádzky v Únii, ale aj na spracovanie realizované prevádzkovateľom alebo sprostredkovateľom, ktorí nie sú usadení v EÚ. A ako upozorňuje Benvenuti¹⁷, pravidlá medzinárodnej právomoci majú najmä v prípadoch, kedy má jedna zo strán sporu sídlo v nečlenskom štáte mimoriadny význam, pretože rozhodné právo uplatniteľné na takéto spory sa určuje podľa práva štátu konajúceho súdu. Ak sa teda majú uplatňovať únieové pravidlá ochrany osobných údajov, je potrebné navrhnúť pravidlá medzinárodnej právomoci tak, aby zaistili právomoc súdov členských štátov pre takýto druh sporov aj v prípade, že ide o spracovanie osobných údajov realizované mimo územia EÚ.

Článok 79 ods. 2 GDPR tak umožňuje realizáciu práva na účinný súdny prostriedok nápravy pre dotknutú fyzickú osobu. Avšak ako norma upravujúca medzinárodnú právomoc civilných súdov má garantovať nielen realizáciu práva na prístup k súdu pre žalobcu ale aj práva na zákonného sudcu žalovaného. Toto právo je napr. v prípade nariadenia Európskeho parlamentu a Rady (EÚ) č. 1215/2012 z 12. decembra 2012 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (prepracované znenie)¹⁸ (ďalej len „nariadenie Brusel Ia“) zhmotnené o. i. v požiadavke vyjadrenej v odôvodnení 16, aby kritériá právomoci boli založené na úzkej väzbe medzi súdom a žalobou. *„Existencia takejto úzkej väzby by mala zaručiť právnu istotu a vylúčiť, že osoba by bola žalovaná na súde členského štátu, s čím nemohla rozumne predvídať. Je to dôležité predovšetkým v prípade sporov týkajúcich sa mimozmluvných záväzkov vyplývajúcich z porušenia práva na súkromie a práva na ochranu osobnosti vrátane poškodzovania dobrého mena.“*¹⁹

V ďalšom texte sa zameriame na analýzu ustanovenia článku 79 ods. 2 GDPR vo väzbe na civilné konania o náhradu škody, ktorú si uplatňuje fyzická osoba od prevádzkovateľa alebo spracovateľa s cieľom preskúmať, či súčasná právna úprava zabezpečuje každej dotknutej fyzickej osobe právo na účinný súdny prostriedok nápravy a zároveň je dostatočne predvídateľná pre prevádzkovateľa a sprostredkovateľa. V tomto článku nebude venovaná pozornosť tým situáciám, kedy je žalovaným orgán verejnej moci pri výkone verejnej moci.

Kritériá medzinárodnej právomoci podľa článku 79 ods. 2 GDPR

Zo znenia článku 79 ods. 2 GDPR vyplýva, že návrh na náhradu škody sa podáva buď na súde členského štátu, v ktorom má obvyklý pobyt dotknutá osoba alebo na súde členského štátu, v ktorom je prevádzkareň žalovaného. Táto možnosť výberu daná

¹⁷ BENVENUTI, Edoardo: Private international law as a mean to project EU digital values abroad. In: EU and Comparative Law issues and Challenges Series, roč. 7, special issue, (2023), s. 229.

¹⁸ Ú. v. EÚ L 351, 20.12.2012, pp. 1–32.

¹⁹ Odôvodnenie 16 nariadenia Brusel Ia.

žalobcovi zodpovedá, ako uvádza Buonaiuti,²⁰ cieľu, ktorý je možné vyvodiť z článku 79 ods. 1 GDPR, a ktorým je zaručiť právo dotknutej osobe na účinný súdny prostriedok nápravy.

Uvedená právna úprava umožňuje dotknutým fyzickým osobám forum shopping.²¹ Rozsah umožnenia forum shopping podľa článku 79 ods. 2 GDPR je široký a súvisí so širokým výkladom pojmu prevádzkareň.

Pojem prevádzkareň nemá legálnu definíciu a ako upozorňuje Mesarčík,²² pri interpretácii tohto pojmu zohráva dôležitú úlohu judikatúra Súdneho dvora Európskej únie a aj odôvodnenie 22 GDPR, ktoré uvádza, že „prevádzkareň znamená efektívny a skutočný výkon činnosti prostredníctvom stálych dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.“ Je teda zrejmé, že tento pojem je podstatne širším ako pojem bydlisko²³, ktorý používa nariadenie Brusel Ia, vďaka čomu GDPR umožňuje, aby na súdoch členských štátov EÚ bolo možné žalovať širší okruh žalovaných s bydliskom v nečlenských štátoch (v porovnaní s nariadením Brusel Ia).

Dôležité, z hľadiska právnej úpravy medzinárodnej právomoci, je to, že jeden prevádzkovateľ alebo sprostredkovateľ môže mať prevádzkarne na území rôznych členských štátov Európskej únie.²⁴ V tejto súvislosti vyvstáva otázka, či na účely článku 79 ods. 2 GDPR je relevantná hlavná prevádzkareň žalovaného alebo len tá prevádzkareň, v kontexte činnosti ktorej vznikla škoda príp. či je možné (alebo dokonca potrebné) založiť medzinárodnú právomoc na konanie na základe kritéria prevádzkarne len vo vzťahu k tej škode, ktorá vznikla v kontexte činnosti tej ktorej prevádzkarne žalovaného.

²⁰ MARONGIU BUONAIUTI, Fabrizio: La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento „Bruxelles I-bis“. In: Cuadernos de Derecho Transnacional, roč. 9, č. 2, (2017), s. 457.

²¹ Podľa Lysinú „forum shopping predstavuje vo všeobecnosti taktiku, či postup navrhovateľa, pri ktorom si tento vyberá súd, na ktorý predloží návrh na začatie konania (resp. uprednostní jeden súd pred ostatnými, ktoré sú rovnako príslušné na prejednanie veci... aby bolo možné uplatniť tento daný postup bude nevyhnutné súčasné naplnenie niekoľkých požiadaviek... musí existovať súčasne viacero súdov vybavených právomocou na prejednanie veci... tieto právomoci by mali byť vzájomne rovnocenné.“ LYSINA, Peter: Forum shopping v medzinárodnom práve súkromnom EÚ. In: LENHART, Michal – ANDRAŠKO, Jozef – HAMULÁK, Juraj (eds.): Milníky práva v stredoeurópskom priestore 2017: zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2017. ISBN 978-80-7160-445-7, s. 176.

²² MESARČÍK, Matúš: Apply or not to apply? A comparative view on territorial application of CCPA and GDPR. In: Bratislava Law Review, roč. 4, č. 2, (2020), s. 85.

²³ K pojmu bydlisko na účely nariadenia Brusel Ia pozri články 62 a 63 nariadenia Brusel Ia.

²⁴ Uvedené vyplýva aj z článku 4 ods. 16 GDPR.

Doktrína neponúka jednoznačné odpovede na všetky uvedené otázky.

Autori sa zhodujú v tom, že z odôvodnenia 146 GDPR, v ktorom sa uvádza že „dotknuté osoby by za utrpenú škodu mali dostať úplnú a účinnú náhradu“ je potrebné vyvodiť záver, že súd s právomocou podľa článku 79 ods. 2 GDPR má právomoc na konanie o náhrade celej škody, ktorá bola spôsobená spracovaním v rozpore s GDPR a to bez ohľadu na to, či k vzniku škody došlo na území viacerých členských štátov alebo tretích štátov.²⁵ Odlišne však pristupujú k riešeniu otázky, či na základe článku 79 ods. 2 GDPR na založenie právomoci súdu stačí, že sa na území daného členského štátu nachádza akákoľvek prevádzkareň žalovaného alebo sa vyžaduje, aby išlo o hlavnú prevádzkareň žalovaného.

Autori, ktorí sa prikláňajú k prvému riešeniu poukazujú na to, že článok 79 ods. 2 GDPR nestanovuje okrem polohy prevádzkarne žiadne ďalšie požiadavky,²⁶ a argumentujú právom na účinný súdny prostriedok nápravy pre dotknutú osobu, ktoré nie je možné obmedziť reštriktívnym výkladom tohto ustanovenia, ktorý navyše nemá oporu v jeho texte. Naopak odporcovia tohto prístupu zdôrazňujú, že takéto kritérium právomoci otvára príliš široké možnosti pre žalobcu a je otázna predvídateľnosť právomoci pre žalovaného v prípade, ak prevádzkareň, ktorej poloha založila medzinárodnú právomoc, sa nijako nepodieľala na spracovaniach, ktorých sa návrh na náhradu škody týka.²⁷ Preto napr. Lundstedt²⁸ navrhuje interpretovať toto ustanovenie tak, že v prípade, ak má žalovaný viacero prevádzkarní, rozhodujúca je tá prevádzkareň, ktorá sa považuje za hlavnú prevádzkareň na základe kritérií podľa článku 4 ods. 16 GDPR a argumentuje, že takýmto výkladom sa zabezpečí vyššia miera právnej istoty pre všetky subjekty a prispeje sa tak k naplneniu jedného z cieľov GDPR.

²⁵ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 248.

²⁶ DE MIGUEL ASENSIO, Pedro Alberto: Derecho a indemnización en materia de datos personales: aspectos internacionales. In: Cuadernos de Derecho Transnacional, č. 2, roč. 16, (2024), s. 490. K tejto otázke pozri tiež VAN CALSTER, Geert: On soggy grounds. The GDPR and jurisdiction for infringement of privacy. Dostupné online: <https://gavclaw.com/2018/07/26/on-soggy-grounds-the-gdpr-and-jurisdiction-for-infringement-of-privacy>

²⁷ DE MIGUEL ASENSIO, Pedro Alberto: Derecho a indemnización en materia de datos personales: aspectos internacionales. In: Cuadernos de Derecho Transnacional, č. 2, roč. 16, (2024), s. 492; rovnako tiež M REQUEJO ISIDRO Marta: La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679. In: La Ley mercantil, č. 42, 2017, s. 11.

²⁸ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 246 a 247.

Kritérium obvyklého pobytu dotknutej osoby²⁹ je rovnako autonómnym pojmom a rovnako nemá legálnu definíciu, a hoci sa využíva ako kritérium právomoci v prameňoch medzinárodného práva súkromného EÚ, ide skôr o pramene upravujúce rodinné veci či dedenie.³⁰ Aj v súvislosti s týmto kritériom medzinárodnej právomoci panuje v odborných kruhoch zhoda na tom, že je možné pred súdom členského štátu obvyklého pobytu dotknutej osoby žalovať o náhradu celej škody.³¹ Ako uvádza Lundstedt³² obvyklý pobyt dotknutej osoby sa posudzuje ku dňu začatia konania, čo žalobcovi uľahčuje uplatnenie nároku na náhradu škody, ale opäť vzbudzuje otázky, nakoľko je právomoc súdu daného štátu pre žalovaného predvídateľná v prípade, že tento štát nie je štátom, v ktorom je prevádzkareň žalovaného a žalovaný žiadnym spôsobom nesmeroval činnosť do tohto štátu a v danom štáte nebol obvyklý pobyt (teda centrum záujmov) dotknutej osoby v čase vzniku škody.³³

Vo vedeckej literatúre sa kritérium obvyklého pobytu dotknutej osoby diskutuje aj v kontexte kolektívnych žalôb, pričom autori sa prikláňajú skôr k možnosti jeho využitia v takýchto prípadoch za predpokladu, že dotknuté subjekty majú obvyklý pobyt v rovnakom členskom štáte. Objavujú sa aj právnej názory, ktoré poukazujú na nepoužiteľnosť tohto kritéria pri kolektívnych žalobách.³⁴

²⁹ Nariadenie Brusel Ia, ktoré upravuje medzinárodnú právomoc súdov členských štátov, používa kritérium bydliska a jeho interpretáciu v prípade fyzickej osoby ponecháva na národné právo členských štátov (pozri čl. 62 nariadenia Brusel Ia).

³⁰ Napríklad v Nariadení Rady (EÚ) 2019/1111 z 25. júna 2019 o právomoci a uznávaní a výkone rozhodnutí v manželských veciach a vo veciach rodičovských práv a povinností a o medzinárodných únosoch detí (prepracované znenie) (ďalej len „nariadenie Brusel IIb“). Súdny dvor v rámci výkladu pojmu obvyklý pobyt na účely nariadenia Brusel IIb rozhodol, že „*pojmem „obvyklý pobyt“ sa v zásade vyznačuje dvoma prvkami, a to jednak vôľou dotknutej osoby zriadiť zvyčajné centrum svojich záujmov na určenom mieste a jednak prítomnosťou, ktorá predstavuje dostatočný stupeň stability na území dotknutého štátu...osoba môže mať v určitom okamihu iba jeden obvyklý pobyt.*“ Rozsudok Súdneho dvora (tretia komora) z 25. novembra 2021 vo veci C-289/20 IB proti FA, ECLI:EU:C:2021:955, body 51 a 58. Zároveň existuje pomerne rozsiahla judikatúra Súdneho dvora Európskej únie vo vzťahu k výkladu pojmu obvyklý pobyt dieťaťa, ktorý vykazuje odlišnosti v porovnaní s pojmom obvyklý pobyt dospelaj osoby. Je otázne, nakoľko sú závery týchto rozsudkov využiteľné pri interpretácii článku 79 ods. 2 GDPR. Domnievam sa, že s ohľadom na skutočnosť, že ide o kritérium právomoci a zároveň kritérium týkajúce sa fyzickej osoby, nie je dôvod predpokladať, že by sa interpretácia tohto pojmu zásadne odlišovala na účely článku 79 ods. 2 GDPR

³¹ DE MIGUEL ASENSIO, Pedro Alberto: Derecho a indemnización en materia de datos personales: aspectos internacionales. In: Cuadernos de Derecho Transnacional, č. 2, roč. 16, (2024), s. 493.

³² LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 247.

³³ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 247.

³⁴ K tejto diskusii pozri bližšie napr. SILVA DE FREITAS, Eduardo: The Interplay of Digital and Legal Frontiers: analyzing jurisdictional rules in GDPR collective actions and the Brussels I-bis Regulation. In: Dutch Journal on Private International Law, 2023, č. 2, s. 227-242.

V súvislosti s takto stanovenými kritériami právomoci podľa článku 79 ods. 2 GDPR vyvstáva otázka, ako postupovať v prípadoch, keď dotknutá fyzická osoba nemá obvyklý pobyt v žiadnom členskom štáte EÚ ale v treťom – nečlenskom štáte³⁵ a utrpela škodu v dôsledku spracúvania, ktoré je v rozpore s GDPR, prevádzkovateľom alebo sprostredkovateľom, ktorý nemá prevádzkareň v žiadnom členskom štáte Európskej únie (čl. 3 ods. 2 GDPR). Kritéria podľa článku 79 ods. 2 GDPR by v takomto prípade neumožňovali založenie právomoci žiadneho súdu členského štátu.³⁶ Takáto interpretácia by však nepochybne odporovala právu na účinný súdny prostriedok nápravy podľa článku 79 ods. 1 GDPR. Rovnako tak kritériá medzinárodnej právomoci podľa článku 79 ods. 2 GDPR neumožňujú spojenia konania voči viacerým prevádzkovateľom alebo sprostredkovateľom, ktorí sa zúčastnili na tom istom spracúvaní, ak majú prevádzkarne v rôznych členských štátoch a žalobca nemá obvyklý pobyt na území žiadneho členského štátu EÚ. Otázne je tiež, či sú uvedené kritériá aplikovateľné aj v prípade vzájomnej žaloby dotknutej fyzickej osoby podľa čl. 82 ods. 6 GDPR, ak konanie inicioval sprostredkovateľ alebo prevádzkovateľ voči tejto osobe na súde iného štátu ako tých, ktoré majú právomoc podľa článku 79 ods. 2 GDPR.

Všetky uvedené situácie vyvolávajú spoločnú otázku a to, či pravidlá v článku 79 ods. 2 GDPR vylučujú možnosť aplikácie kritérií medzinárodnej právomoci podľa nariadenia Brusel Ia alebo nie.

Aplikačný vzťah čl. 79 ods. 2 GDPR a nariadenia Brusel Ia

GDPR neobsahuje v normatívnej časti žiadne ustanovenie, ktoré by upravovalo vzťah kritérií medzinárodnej právomoci podľa čl. 79 ods. 2 GDPR ku kritériám medzinárodnej právomoci podľa nariadenia Brusel Ia. Určitú pomôcku v tomto smere poskytujú odôvodnenia 145 a 147 GDPR, ktoré uvádzajú, že *„pri konaniach voči prevádzkovateľovi alebo sprostredkovateľovi by žalobca mal mať možnosť podať žalobu na súdoch členského štátu, v ktorom má prevádzkovateľ alebo sprostredkovateľ prevádzkareň, alebo kde má dotknutá osoba bydlisko, s výnimkou prípadov, keď prevádzkovateľom je orgán verejnej moci členského štátu pri výkone verejnej moci.“* A *„ak toto nariadenie obsahuje osobitné pravidlá o určení právomoci, najmä pokiaľ ide o konania na uplatnenie súdnych prostriedkov nápravy vrátane náhrady škody voči prevádzkovateľovi alebo sprostredkovateľovi, uplatňovanie týchto osobitných pravidiel*

³⁵ Odôvodnenie 14 GDPR uvádza *„Ochrana, ktorá sa poskytuje týmto nariadením, by sa mala vzťahovať na fyzické osoby bez ohľadu na ich štátnu príslušnosť alebo miesto bydliska vo vzťahu ku spracúvaniu ich osobných údajov. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“*

³⁶ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 252-253.

by nemalo byť dotknuté všeobecnými normami o určení právomoci, ako sú napríklad normy stanovené v nariadení."

Nariadenie Brusel Ia v článku 67 stanovuje, že „*toto nariadenie nemá vplyv na uplatňovanie ustanovení upravujúcich právomoc a uznávanie a výkon rozsudkov v špecifických veciach, ktoré sú obsiahnuté v právnych nástrojoch Únie alebo vnútroštátnych právnych predpisoch harmonizovaných v súlade s týmito právnymi nástrojmi.*“ Vo vedeckom komentári k článku 67 sa uvádza, že toto ustanovenie zakotvuje zásadu *lex specialis derogat legi generali*, z ktorej vyplýva prednostná aplikácia *lex specialis* na tie otázky, ktoré *lex specialis* upravuje, ak si *lex specialis* nárokuje prednosť pred nariadením Brusel Ia. Ak sa však *lex specialis* odvoláva na nariadenie Brusel Ia a to či už priamo alebo zavedením mechanizmu priaznivejšieho zaobchádzania, nariadenie Brusel Ia sa s dovoľením *lex specialis* uplatní.³⁷

Doktrína sa nezhoduje v odpovedi na otázku, či z tejto právnej úpravy vyplýva záver, že článok 79 ods. 2 GDPR nahrádza kritériá právomoci podľa nariadenia Brusel Ia alebo len dopĺňa tento systém kritérií o dodatočné kritériá, ktoré by mali byť vždy dostupné pre dotknuté fyzické osoby.

Časť autorov sa prikláňa k záveru, že pravidlá zakotvené v článku 79 ods. 2 GDPR vylučujú možnosť aplikácie kritérií právomoci podľa nariadenia Brusel Ia a argumentujú znením článku 79 ods. 2 GDPR ako aj článku 67 nariadenia Brusel Ia a tiež tým, že ochrana dotknutej osoby nepredstavuje absolútnu hodnotu a musí sa posudzovať z hľadiska konkurujúcich základných práv, ako je právo na účinný súdny prostriedok nápravy, ktoré by mohlo byť dotknuté, ak by sa umožnilo nadmerné rozširovanie fór s právomocou.³⁸ K tejto interpretácii sa prikláňa napr. Mariottini,³⁹

³⁷ LAZIĆ, Vesna – MANKOWSKI, Peter. (eds.): The Brussels I-bis Regulation. Interpretation and Implementation. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2023, s. 523-524.

³⁸ MARIOTTINI, Cristina M.: Article 67. In: REQUEJO ISIDO, Marta (Ed.): Brussels I Bis. A Commentary on Regulation (EU) No 1215/2012. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2022, s. 882.

³⁹ Táto autorka uvádza, že bez rozhodnutia Súdneho dvora EÚ v tejto veci sa argumenty v prospech reštriktívneho výkladu zdajú byť silnejšie, a to aj vzhľadom na skutočnosť, že takýto výklad nie je nezlučiteľný s odôvodneniami 145 a 147 GDPR. MARIOTTINI, Cristina M.: Article 67. In: REQUEJO ISIDO, Marta (Ed.): Brussels I Bis. A Commentary on Regulation (EU) No 1215/2012. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2022, s. 883.

Kyselovská⁴⁰ či Requejo Isidro,⁴¹ ktorá dodáva ďalší zaujímavý argument, keď pripomína, že ďalším zo základných cieľov GDPR je voľný pohyb osobných údajov ako nevyhnutnosť pre riadne fungovanie vnútorného trhu, čo sa podľa tejto autorky v oblasti právnej úpravy medzinárodnej právomoci prejavuje v požiadavke, aby kritériá medzinárodnej právomoci, z ktorých si môže žalobca vybrať, neboli formulované natoľko široko, že by odrádzali prevádzkovateľov alebo sprostredkovateľov od vstupu na vnútorný trh alebo od zotrvania na ňom.

Opačný názor zastáva napr. Asensio,⁴² ktorý zdôrazňuje, že cieľom GDPR je posilniť ochranu dotknutých osôb tým, že sa im umožní podať žalobu na súdoch podľa článku 79 ods. 2 GDPR, pričom uvádza, že s ohľadom na tento účel právnej úpravy a odôvodnenie 145 GDPR, článok 79 ods. 2 GDPR dopĺňa a nevylučuje tie pravidlá právomoci podľa nariadenia Brusel Ia, ktoré neoslabujú pravidlá v článku 79 ods. 2 GDPR. K podobnému záveru dospievajú aj Van Calster,⁴³ Lundstedt,⁴⁴ Marongiu Buonaiuti.⁴⁵ Aj v prípade zástancov uvedeného názoru však nie je jednoznačná zhoda na odpovedi na otázku, ktoré ustanovenia nariadenia Brusel Ia odporujú a ktoré neodporujú článku 79 ods. 2 GDPR. Napr. nie je zhoda na tom, či popri článku 79 ods. 2 GDPR je možné založiť aj právomoc súdu miesta plnenia, ktoré je predmetom zmluvy podľa čl. 7 ods. 1 nariadenia Brusel Ia, ak je nárok založený na spracovaní

⁴⁰ Táto autorka zdôrazňuje povahu *lex specialis* čl. 79 ods. 2 GDPR k článku 7 ods. 2 nariadenia Brusel Ia a uvádza, že sa nestotožňuje s názorom, že nariadenie Brusel Ia dopĺňa pravidlá medzinárodnej právomoci obsiahnuté v článku 79 ods. 2 GDPR. KYSELOVSKÁ, Tereza: *Mezinárodní právo soukromé a právo k duševnímu vlastnictví – procesní otázky*. 1. vyd. Brno: Masarykova univerzita, 2023, ISBN 978-80-280-0467-5, s. 82.

⁴¹ REQUEJO ISIDRO, Marta: *La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679*. In: *La Ley mercantil*, č. 42, 2017. Táto autorka zároveň zdôrazňuje, že z nariadenia Brusel Ia možno v každom prípade prevziať časť týkajúcu sa overovania vlastnej právomoci a prípustnosti (články 27 a 28). S väčšími pochybnosťami aj časť týkajúcu sa prekážky *res iudicata* a súvisiacich vecí (články 29 až 34), pravdepodobne obmedzenú na prípady prekážky *res iudicata* medzi členskými štátmi – s vylúčením článku 33. Pričom uplatnenie týchto pravidiel bude závisieť od toho, ako sa bude interpretovať článok 81 GDPR.

⁴² MIGUEL ASENSIO, Pedro Alberto: *Derecho a indemnización en materia de datos personales: aspectos internacionales*. In: *Cuadernos de Derecho Transnacional*, č. 2, roč. 16, (2024), s. 493.

⁴³ VAN CALSTER, Geert: *On soggy grounds. The GDPR and jurisdiction for infringement of privacy*. Dostupné online: <https://gavclaw.com/2018/07/26/on-soggy-grounds-the-gdpr-and-jurisdiction-for-infringement-of-privacy>

⁴⁴ LUNDSTEDT, Lydia: *International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR*, In: *Scandinavian Studies in Law*, roč. 65, (2018), s. 253.

⁴⁵ MARONGIU BUONAIUTI, Fabrizio: *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento „Bruxelles I-bis“*. In: *Cuadernos de Derecho Transnacional*, roč. 9, č. 2, (2017), s. 450.

nevyhnutnom pre plnenie zmluvy, ktorej je fyzická osoba zmluvnou stranou,⁴⁶ prípadne na možnosti založenie právomoci na ustanovení čl. 26 nariadenia Brusel Ia. Niektorí autori preto navrhujú posudzovanie kritérií právomoci jednotlivo, iní zasa zdôrazňujú účel konkrétnej právnej úpravy právomoci, ktorú to ktoré kritérium podľa nariadenia Brusel Ia sleduje.

Lustráciou dostupných databáz slovenských a českých súdnych rozhodnutí sa nepodarilo identifikovať žiadne relevantné súdne rozhodnutie, ktoré by sa zaoberalo otázkou aplikačného vzťahu článku 79 ods. 2 GDPR a nariadenia Brusel Ia. V literatúre je pomerne často citovaná holandská aplikačná prax, ktorú sumarizuje Henckel,⁴⁷ ktorá poukazuje na viaceré holandské rozhodnutia, ktoré sa týkali porušovania súkromia zo strany takých spoločností, akými sú Google, Microsoft, TikTok a Facebook, v ktorých holandské súdy konštatovali, že ustanovenie o medzinárodnej právomoci podľa čl. 79 ods. 2 GDPR dopĺňajú kritériá právomoci podľa nariadenia Brusel Ia.⁴⁸

Výhodou tohto prístupu nepochybne je, že poskytuje riešenie pre otázky možnosti/nemožnosti spojenia konania voči viacerým žalovaným (čl. 8 ods. 1 nariadenia Brusel Ia), vzájomné žaloby (čl. 8 ods. 3 nariadenia Brusel Ia) a tiež pre situácie, kedy dotknutá osoba nemá obvyklý pobyt v EÚ a ani žalovaný nemá prevádzkareň v EÚ (napr. čl. 6 nariadenia Brusel Ia umožňujúci aplikáciu národných pravidiel).

Aplikačný vzťah článku 79 ods. 2 GDPR k pravidlám medzinárodnej právomoci podľa nového Lugánskeho dohovoru⁴⁹

Kým aplikačný vzťah GDPR a nariadenia Brusel Ia je pomerne diskutovanou otázkou, už menej sa skúma aplikačný vzťah článku 79 ods. 2 GDPR ku kritériám medzinárodnej právomoci podľa nového Lugánskeho dohovoru. Táto otázka je relevantná v prípade, ak je na súde členského štátu podaný návrh podľa čl. 82 ods. 6 GDPR a žalovaný by mal bydlisko vo Švajčiarsku, Nórsku alebo na Islande. Aplikujú sa na takéto situácie prednostne pred čl. 79 ods. 2 GDPR pravidlá medzinárodnej právomoci podľa nového Lugánskeho dohovoru alebo je potrebné aplikovať kritériá podľa čl. 79 ods. 2 GDPR?

⁴⁶ K tomu pozri názory za a proti v článku SILVA DE FREITAS, Eduardo: The Interplay of Digital and Legal Frontiers: analyzing jurisdictional rules in GDPR collective actions and the Brussels I-bis Regulation. In: Dutch Journal on Private International Law, 2023, č. 2, s. 227-242.

⁴⁷ HENCKEL, Kirsten: The Brussels Ibis reform, third state defendants and the Dutch experience. In: Dutch Journal on Private International Law, č. 1, roč. 43, (2025), s. 21.

⁴⁸ HENCKEL, Kirsten: The Brussels Ibis reform, third state defendants and the Dutch experience. In: Dutch Journal on Private International Law, č. 1, roč. 43, (2025), s. 22.

⁴⁹ Dohovor o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach Ú. v. EÚ L 147, 10.6.2009, s. 5 – 43

Lundstedt vidí riešenie tejto otázky v aplikácii článku 67 ods. 1⁵⁰ nového Lugánskeho dohovoru a konštatuje, že súdy členských štátov neaplikujú žiadne ustanovenie nového Lugánskeho dohovoru, ktoré odporujú čl. 79 ods. 2 GDPR.⁵¹

Tento záver však považujem za problematický. Ustanovenie článku 67 ods. 1 nového Lugánskeho dohovoru totiž upravuje aplikačný vzťah tohto dohovoru k iným medzinárodným zmluvám nie k prameňom práva EÚ, ktorým GDPR nepochybne je. Navyše nový Lugánsky dohovor obsahuje osobitné ustanovenie, ktoré upravuje vzťah k úniovým pravidlám medzinárodnej právomoci v občianskych a obchodných veciach a tým je článok 64 ods. 1 písm. b) nového Lugánskeho dohovoru. Je zrejmé, že toto ustanovenie Lugánskeho dohovoru nepočíta s existenciou úniových pravidiel právomoci na konanie v občianskych a obchodných veciach v inom predpise ako je nariadenie Brusel Ia, čo zodpovedá dobe, v ktorej bol tento dohovor uzavretý. Nič to však nemení na potrebe teleologického výkladu ustanovenia čl. 64 ods. 1 písm. b) nového Lugánskeho dohovoru a rešpektovaní, že *„tento dohovor sa vždy uplatní vo veciach právomoci, ak má žalovaný bydlisko na území štátu, kde sa uplatňuje tento dohovor, ale neuplatňuje sa žiadny z právnych nástrojov uvedených v odseku 1 tohto článku, alebo ak súdy tohto členského štátu majú právomoci podľa článku 22 alebo článku 23 tohto nariadenia.“* (článok 64 ods. 2 a) nového Lugánskeho dohovoru) a jeho prednostnej aplikácie zo strany súdov členských štátov EÚ pred článkom 79 ods. 2 GDPR. V opačnom prípade hrozí riziko odmietnutia uznania rozhodnutia vydaného súdom členského štátu vo Švajčiarsku, Nórsku resp. na Islande (článok 64 ods. 3 nového Lugánskeho dohovoru).

Záver

Je potrebné oceniť, že pri úprave súkromnoprávných nástrojov vymáhania práva na ochranu osobných údajov v GDPR neboli opomenuté ani otázky medzinárodnej právomoci, ktoré predstavujú kľúčové ustanovenia v kontexte realizácie práva na účinný súdny prostriedok nápravy.

Právna úprava medzinárodnej právomoci v článku 79 ods. 2 GDPR nepochybne predstavuje významný krok smerom k ochrane dotknutej fyzickej osoby, avšak analýza ukázala, že hoci cieľom normotvorcu bolo zabezpečiť čo najširšiu dostupnosť účinného súdneho prostriedku nápravy, stále existujú situácie, pre ktoré kritériá právomoci podľa článku 79 ods. 2 GDPR neposkytujú riešenie a v iných prípadoch

⁵⁰ Článok 67 ods. 1 nového Lugánskeho dohovoru stanovuje, že *„tento dohovor nemá vplyv na medzinárodné zmluvy, ktorými sú zmluvné strany a/alebo štáty viazané týmto dohovorom viazané a ktoré upravujú právomoc alebo uznávanie a výkon rozsudkov v špecifických veciach. Bez toho, aby boli dotknuté záväzky vyplývajúce z iných medzinárodných zmlúv, ktorými sú viazané niektoré zmluvné strany, nebráni tento dohovor zmluvným stranám v uzatváraní takýchto medzinárodných zmlúv.“*

⁵¹ LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s. 250 a s. 253.

umožňujú založenie právomoci takého fóra, ktoré je pre žalovaných nepredvídateľným. Nejasné prepojenie s režimom nariadenia Brusel Ia a s novým Lugánskym dohovorom navyše vytvára priestor pre neistotu v aplikačnej praxi.

Pre ďalší vývoj bude kľúčové, aby sa k otázke vyváženia práv žalobcu a žalovaného v tomto špecifickom kontexte vyjadril Súdny dvor Európskej únie. Len jeho judikatúra môže poskytnúť potrebné usmernenie a tým aj stabilitu, ktorá prispeje k zosúladeniu jedného z cieľov GDPR – ochrany práv jednotlivcov – s požiadavkou právnej istoty a predvídateľnosti v medzinárodnom civilnom konaní. Do budúcnosti možno preto očakávať, že aplikačná prax členských štátov spolu s judikatúrou Súdneho dvora postupne vytvoria ucelenejší rámec, ktorý prinesie odpovede na otvorené otázky a umožní efektívnejšie uplatňovanie práva na náhradu škody v prípadoch s cezhraničným prvkom.

Zoznam použitej literatúry

1. BENVENUTI, Edoardo: Private international law as a mean to project EU digital values abroad. In: EU and Comparative Law issues and Challenges Series, roč. 7, special issue, (2023), s. 227-266.
2. HENCKEL, Kirsten: The Brussels Ibis reform, third state defendants and the Dutch experience. In: Dutch Journal on Private International Law, č. 1, roč. 43, (2025), s. 3-28.
3. MIGUEL ASENSIO, Pedro Alberto: Derecho a indemnización en materia de datos personales: aspectos internacionales. In: Cuadernos de Derecho Transnacional, č. 2, roč. 16, (2024), s. 487 – 500.
4. KALESNÁ, Kalesná: Bude fungovať súkromnoprávne vymáhanie súťažného práva? In: Právny obzor, 101, č. 1, (2018), s. 54 – 61.
5. KYSELOVSKÁ, Tereza: Mezinárodní právo soukromé a právo k duševnímu vlastnictví – procesní otázky. 1. vyd. Brno: Masarykova univerzita, 2023, 283 s., ISBN 978-80-280-0466-8 (print), 978-80-280-0467-5 (online)
6. LAZIĆ, Vesna – MANKOWSKI, Peter. (eds.): The Brussels I-bis Regulation. Interpretation and Implementation. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2023, 556 s., ISBN 978 1 80037 015 9.
7. LUNDSTEDT, Lydia: International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR, In: Scandinavian Studies in Law, roč. 65, (2018), s.214-255.
8. LYSINA, Peter: Forum shopping v medzinárodnom práve súkromnom EÚ. In: LENHART, Michal – ANDRAŠKO, Jozef – HAMULÁK, Juraj (eds.): Míľniky práva v stredoeurópskom priestore 2017: zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou. Bratislava:

Univerzita Komenského v Bratislave, Právnická fakulta, 2017. ISBN 978-80-7160-445-7, s. 174-181.

9. MARONGIU BUONAIUTI, Fabrizio: La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento „Bruxelles I-bis“. In: Cuadernos de Derecho Transnacional, roč. 9, č. 2, (2017), s. 448-464.
10. MESARČÍK, Matúš: Apply or not to apply? A comparative view on territorial application of CCPA and GDPR. In: Bratislava Law Review, roč. 4, č. 2, (2020), s.81-94.
11. PFEIFFER, Magdalena a kol. (eds.): Liber Amicorum Monika Pauknerová. Praha: Wolters Kluwer ČR, 2021, 552 s., ISBN 978 80 7676 187 2.
12. REQUEJO ISIDRO, Marta: La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679. In: La Ley mercantil, č. 42, 2017, s. 1-25.
13. REQUEJO ISIDO, Marta (Ed.): Brussels I Bis. A Commentary on Regulation (EU) No 1215/2012. Cheltenham, UK, Northampton, MA, USA: Edward Elgar Publishing, 2022, 1011 s., ISBN 978 1 7899 817 6.
14. REVOLIDIS, Ioannis: Judicial jurisdiction over internet privacy violations and the GDPR: A case of „privacy tourism“? In: Masaryk University Journal of law and Technology. Roč. 11, č. 1, (2017), s. 7 – 38.
15. UŘIČAŘ, Miroslav - RÁMIŠ, Vladan a kol.: Obecné nařízení o ochraně osobních údajů. 1. vydání. Praha: C. H. Beck, 2021, 1386 s., ISBN 978 80 7400 815 3.

Kontaktné údaje

doc. JUDr. Katarína Burdová, PhD.

katarina.burdova@flaw.uniba.sk

Právnická fakulta Univerzity Komenského v Bratislave

OCHRANA PRÁV DETÍ V DIGITÁLNOH SVETE¹

THE PROTECTION OF CHILDREN'S RIGHTS IN THE DIGITAL AGE

Lilla Garayova²

Abstrakt: Príspevok sa zameriava na analýzu uplatňovania práv detí v digitálnom prostredí so zvláštnym dôrazom na výklad Dohovoru o právach dieťaťa v kontexte súčasného technologického vývoja. Cieľom je identifikovať, ako sa základné práva detí premietajú do online priestoru a aké požiadavky z toho vyplývajú pre štáty, regulačné orgány a ďalších aktérov. Štúdia využíva normatívnu analýzu medzinárodných dokumentov, osobitne všeobecného komentára č. 25, a komparatívne posudzuje záverečné odporúčania Výboru pre práva dieťaťa pred a po roku 2021, aby zachytila posun v prístupe k digitálnym právam detí. Výsledky ukazujú, že po prijatí všeobecného komentára dochádza k výraznému rozšíreniu monitorovania digitálnych otázok a k systematickému začleňovaniu online prostredia do jednotlivých oblastí práv detí. Analýza poukazuje na potrebu vyváženého prístupu, ochrany a autonómie detí pri používaní digitálnych technológií. Vedeckým prínosom práce je komplexné uchopenie digitálneho prostredia ako prirodzeného rozšírenia existujúcich práv detí. Praktický prínos spočíva v identifikácii prvkov, ktoré by mali tvoriť základ národných politík a regulačných opatrení v oblasti online bezpečnosti a digitálnej inklúzie detí.

Kľúčové slová: medzinárodné právo, práva detí, detské práva, Dohovor o právach dieťaťa, digitálne prostredie

Abstract: The contribution examines how children's rights are applied in the digital environment, with particular attention to the interpretation of the Convention on the Rights of the Child in the context of contemporary technological developments. Its aim is to identify how core children's rights translate into the online sphere and what obligations this creates for states, regulatory authorities and other actors. The study employs a normative analysis of international instruments, with a focus on General Comment No. 25,

¹ Táto práca bola podporovaná Radou Grantovej agentúry Academia aurea na základe Zmluvy č. GAAA/2024/39.

² Doc. JUDr. PhDr. Lilla Garayová, PhD. LL.M – prodekan, docentka medzinárodného práva, Ústav medzinárodného a európskeho práva, Paneurópska vysoká škola, Tomášikova 20, 821 02 Bratislava, Slovensko, ORCID: 0000-0002-7999-4823; lilla.garayova@paneurouni.com.

and offers a comparative assessment of the Committee on the Rights of the Child's concluding observations issued before and after 2021 in order to capture the evolving approach to children's digital rights. The findings show that following the adoption of the General Comment there has been a significant expansion in the monitoring of digital issues and a more systematic integration of the online environment across different areas of children's rights. The analysis highlights the need to balance access, protection and autonomy when children engage with digital technologies. The scientific contribution of the paper lies in framing the digital environment as an inherent extension of existing children's rights. Its practical contribution consists in identifying elements that should form the basis of national policies and regulatory measures in the field of online safety and digital inclusion for children.

Keywords: international law, childrens rights, online child sexual exploitation, digital environment, UN Convention on the Rights of the Child, children's rights

Úvod

Dnešné deti žijú vo svete, v ktorom je digitálny a fyzický svet neoddeliteľne prepojený. Jeden z troch používateľov internetu na svete má menej ako 18 rokov,³ napriek tomu však zákony príliš dlho nedokázali plne uznať deti ako samostatnú skupinu nositeľov práv v digitálnom svete. Predpoklad, že kyberpriestor je sférou len pre dospelých, bol spochybnený skutočnosťou, že deti používajú online platformy na vzdelávanie, hranie, socializáciu a vyjadrovanie sa. S touto príležitosťou prichádza aj riziko: eskalácia sexuálneho vykorisťovania a zneužívania detí online, kyberšikana a porušovanie súkromia na základe údajov predstavujú naliehavé výzvy. V tejto súvislosti sa medzinárodný rámec práv detí – založený na Dohovore OSN o právach dieťaťa (UNCRC)⁴ – testuje a prehodnocuje. Končí sa pôsobnosť UNCRC na okraji obrazovky? Alebo sa jeho ochrana musí rozšíriť aj na virtuálne priestory rovnako plnohodnotne ako na priestory fyzické? Tento článok presadzuje tézu, že práva detí musia byť realizované v digitálnom prostredí ako integrálna súčasť života detí, nie ako samostatná oblasť s nižšími štandardmi. Medzinárodné právo v oblasti detských práv, riadené UNCRC, má zabezpečiť, aby sa v digitálnom svete naplňali práva detí na ochranu, zabezpečenie a participáciu na rovnakom základe ako v offline kontexte.

³ DADI, Afework Fekadu – DACHEW, Berihun Assefa – TESSEMA, Gizachew Assefa: Problematic internet use: A growing concern for adolescent health and well-being in a digital era. In: Journal of Global Health, Roč. 14 (2024), s. 03034. doi: 10.7189/jogh.14.03034.

⁴ UN General Assembly: Convention on the Rights of the Child. In: United Nations, Treaty Series, vol. 1577, p. 3, 20 November 1989.

Na podporu tejto argumentácie prvá časť tejto štúdie poskytuje teoretický rámec práv detí v digitálnom veku, pričom čerpá z UNCRC a prelomového Všeobecného komentára č. 25 (2021) o právach detí vo vzťahu k digitálnemu prostrediu.⁵ Časť II skúma, ako sa kľúčové práva a zásady UNCRC – od práva na prístup k informáciám po právo na ochranu pred násilím – uplatňujú v online prostredí, a analyzuje napätie medzi umožnením digitálneho prístupu detí, zabezpečením ich ochrany pred ujmom a rešpektovaním ich autonómie a rozvíjajúcich sa schopností. Časť III ponúka empirický pohľad prostredníctvom porovnania záverečných odporúčaní Výboru OSN pre práva dieťaťa pred a po Všeobecnom komentári č. 25, pričom odhaľuje výrazný nárast pozornosti, ktorú výbor venuje digitálnym a online otázkam vo svojich odporúčaniach po roku 2021. Záver poukazuje na príklady nedávnych regulačných inovácií, ktoré uvádzajú tieto zásady do praxe, so zameraním na európsky vývoj, ako je Všeobecné nariadenie o ochrane údajov (GDPR)⁶ a Akt o digitálnych službách (DSA) EÚ,⁷ ako aj britský kódex vekovo primeraného dizajnu,⁸ a skúma globálne trendy. V poslednej časti sa nakoniec zamýšľa nad tým, čo v praktickom a normatívnom zmysle znamená brať deti vážne ako nositeľov práv v rozvíjajúcom sa digitálnom ekosystéme. Cieľom príspevku je analyzovať, ako sa základné práva dieťaťa podľa Dohovoru o právach dieťaťa uplatňujú v digitálnom prostredí, a identifikovať rozsah povinností, ktoré z toho vyplývajú pre štáty a ďalších aktérov. Štúdia zároveň sleduje vývoj prístupu Výboru pre práva dieťaťa pred a po prijatí Všeobecného komentára č. 25, s cieľom zachytiť posun v medzinárodnom monitorovaní digitálnych práv detí. Príspevok sa usiluje poukázať na kľúčové právne výzvy digitalizácie detstva a na prvky, ktoré môžu slúžiť ako základ budúcich regulačných a politických opatrení.

Dohovor OSN o právach dieťaťa a digitálne prostredie

Dohovor OSN o právach dieťaťa,⁹ prijatý v roku 1989, predchádza digitálnej revolúcii, ale jeho široké záruky – právo na život, rozvoj, ochranu pred ujmom, vzdelanie, súkromie, slobodu prejavu, hru a ďalšie – sú formulované technologicky neutrálnym

⁵ United Nations, Committee on the Rights of the Child: General Comment No. 25 (2021) on children's rights in relation to the digital environment, adopted on 2 March 2021.

⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu digitálnych služieb a o zmene smernice 2000/31/ES (Akt o digitálnych službách – Digital Services Act).

⁸ Information Commissioner's Office: Age appropriate design: a code of practice for online services (UK Age Appropriate Design Code). London: ICO, 2020.

⁹ UN General Assembly: Convention on the Rights of the Child. In: United Nations, Treaty Series, vol. 1577, p. 3, 20 November 1989.

spôsobom. UNCRC výslovne nespomína internet ani digitálne technológie, ale jej ustanovenia sú „*plne uplatniteľné na digitálne prostredie*“, ako potvrdil Výbor OSN pre práva dieťaťa.¹⁰

Za posledné dve desaťročia sa čoraz viac prejavuje potreba interpretovať dohovor z hľadiska digitálnej reality. V roku 2014 venoval Výbor deň všeobecnej diskusie téme „digitálne médiá a práva detí“¹¹ a vzrástli požiadavky na autoritatívne usmernenia. Výsledkom bolo vydanie všeobecného komentára č. 25 (2021), míľnikového dokumentu, ktorý formuluje, ako musia štáty implementovať UNCRC s ohľadom na skúsenosti detí online.

Všeobecný komentár č. 25 (GC25) jasne stanovuje, že práva každého dieťaťa musia byť rešpektované, chránené a naplňované v digitálnom prostredí. Namiesto toho, aby GC25 považoval digitálny svet za samostatný, integruje ho ako rozmer existujúcich práv detí. Definuje digitálne prostredie vo všeobecnom zmysle tak, aby zahŕňalo sieťové technológie, obsah, služby a aplikácie, umelú inteligenciu, pripojené zariadenia a ďalšie prvky.

Zásadné je, že GC25 uznáva, že digitálne vylúčenie môže zhoršiť existujúce nerovnosti, zatiaľ čo digitálne začlenenie môže podporiť realizáciu celého spektra práv detí, ak je sprevádzané primeranými ochrannými opatreniami. Inými slovami, prístup k digitálnym nástrojom môže posilniť práva na vzdelanie, informácie a účasť, ale nekontrolovaný digitálny rast so sebou prináša aj riziko nových foriem porušovania práv – od online zneužívania až po invazívne praktiky v oblasti údajov. GC25 výslovne odkazuje na všeobecné zásady Dohovoru: nediskriminácia, najlepší záujem dieťaťa, právo na život, prežitie a rozvoj a právo byť vypočutý (články 2, 3, 6, 12 UNCRC) by mali usmerňovať konanie štátu v digitálnom kontexte. Napríklad zásada najlepšieho záujmu dieťaťa (článok 3) znamená, že pri navrhovaní digitálnych politík, platforiem a produktov sa musí zohľadňovať a uprednostňovať blaho detí pred komerčnými alebo inými záujmami.¹²

Právo byť vypočutý (článok 12) znamená, že deti by mali byť aktívne konzultované a zapájané do tvorby zákonov a služieb, ktoré sa ich týkajú. Je pozoruhodné, že samotný proces vypracovania GC25 bol vzorom pre tento prístup: viac ako 700 detí z celého sveta, vrátane mnohých z globálneho Juhu, bolo oslovených, aby sa podelili o

¹⁰ United Nations, Committee on the Rights of the Child: General Comment No. 25 (2021) on children's rights in relation to the digital environment, adopted on 2 March 2021.

¹¹ Committee on the Rights of the Child: Report of the 2014 Day of General Discussion "Digital Media and Children's Rights". United Nations, 2014.

¹² GARAYOVÁ, Lilla: Protecting children's rights in the age of digitalisation: Legal implications for the best interests of the child. In: Pakistan Journal of Life and Social Sciences, Roč. 22, č. 2 (2024), s. 7351–7366. doi: 10.57239/PJLSS-2024-22.2.00555.

svoje skúsenosti a pohľady na digitálny svet.¹³ Obohatilo to nielen obsah Všeobecného komentára, ale symbolizovalo aj posun smerom k zaobchádzaniu s deťmi ako so zainteresovanými stranami v tvorbe digitálnych politík, v súlade s ich postavením ako nositeľov práv.

Všeobecný komentár poskytuje podrobné usmernenia týkajúce sa rôznych práv. Zaoberá sa občianskymi právami a slobodami (napr. prístupom k informáciám, slobodou prejavu a združovania sa online), právami na súkromie a ochranu údajov, ochranou pred všetkými formami násilia a vykorisťovania (vrátane digitálnych rizík, ako je kyberšikana, sexuálne vykorisťovanie online, obchodovanie s ľuďmi a vystavenie škodlivému obsahu) a právami na vzdelanie, hru a kultúru v digitálnom kontexte. Naliehavo vyzýva štáty, aby prijali komplexný prístup: aktualizáciu právnych predpisov a regulácií, odbornú prípravu učiteľov a odborníkov, usmerňovanie rodičov, podporu digitálnej gramotnosti a spoluprácu so súkromným sektorom s cieľom vytvoriť bezpečné online priestory.

Kľúčovým posolstvom je, že by sa mal podporovať zmysluplný prístup k digitálnym technológiám pre všetky deti (prekonávanie digitálnej priepasti), ale tento prístup musí byť sprevádzaný úsilím o posilnenie a ochranu práv detí.

GC25 tiež zdôrazňuje, že zodpovednosť za dodržiavanie práv detí v digitálnom prostredí sa netýka len vlád, ale aj súkromných spoločností (technologických firiem, online platforiem, poskytovateľov internetových služieb) ako nositeľov povinností podľa Dohovoru.¹⁴ Štáty sú vyzvané, aby zabezpečili, že podnikateľské subjekty plnia svoje povinnosti v oblasti práv detí, napríklad prostredníctvom regulácie alebo usmernení.

Objasnením, že existujúce práva sa uplatňujú online rovnako ako offline, GC25 odstraňuje akúkoľvek vnímanú normatívnu medzeru. Odmieta prístupy, ktoré deti jednoducho zakazujú alebo vylučujú z digitálnych priestorov; namiesto toho presadzuje právo detí na príležitosti a účasť online, pričom zároveň požaduje prísnejšie opatrenia na ich ochranu a zabezpečenie ich údajov.¹⁵ Vízia Výboru, ako je stanovená v GC25, je ambiciózna: internet, ktorý *„rešpektuje, chráni a naplňuje celý*

¹³ Committee on the Rights of the Child: General comment No. 25 (2021) on children's rights in relation to the digital environment, 2 March 2021, para. 5.

¹⁴ AYLAWEW, Yohannes Eneyew – VERDOODT, Valerie – LIEVENS, Eva: General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa. In: Human Rights Law Review, Roč. 24, č. 3 (september 2024). doi: 10.1093/hrlr/ngae018.

¹⁵ THIRD, Amanda – MOODY, Lucy: Our rights in the digital world: A report on the children's consultations to inform UN CRC General Comment 25. London – Sydney: 5Rights Foundation and Western Sydney University, 2021.

rozsah práv detí".¹⁶ Takto sa digitálne prostredie nevníma ako hrozba sama osebe, ale ako priestor príslubov aj nebezpečenstiev. Realizácia týchto príslubov si vyžaduje zámerné začlenenie práv detí do zákonov, politik a návrhov.

Uplatňovanie práv detí online

Jednou z hlavných výziev pri realizácii práv detí v digitálnom prostredí je vyváženie troch niekedy protichodných požiadaviek: prístup, ochrana a autonómia. Tieto požiadavky voľne zodpovedajú tomu, čo sa v oblasti práv detí často označuje ako „3P“ (po anglicky *provision, protection, participation* – alebo poskytovanie, ochrana, účasť). V digitálnom kontexte sa prejavujú ako napätie, s ktorým sa musia tvorcovia politik a zainteresované strany vysporiadať.

Prístup - Článok 17 UNCRC uznáva právo dieťaťa na prístup k primeraným informáciám a článok 13 chráni slobodu prejavu, vrátane slobody vyhľadávať a prijímať informácie prostredníctvom akýchkoľvek médií. V dnešnom svete tieto práva znamenajú, že deti by mali mať rovnaký prístup k digitálnym technológiám a internetu ako prostriedku vzdelávania, informácií, sociálnych kontaktov a vyjadrovania. Digitálny prístup môže byť hnacou silou ďalších práv – napríklad online vzdelávacie platformy môžu podporovať právo na vzdelanie (článok 28) a digitálne nástroje môžu pomáhať deťom so zdravotným postihnutím, aby mohli rovnako ako ostatné deti využívať svoje práva (článok 23). GC25 potvrdzuje, že zmysluplný prístup k digitálnym technológiám môže podporovať rozvoj detí a realizáciu ich práv, najmä ak je spojený s digitálnou gramotnosťou. Napríklad počas pandémie COVID-19 sa stal nepopierateľným význam pripojenia k internetu pre školskú dochádzku a sociálny život detí.¹⁷ Štáty majú preto povinnosť preklenúť digitálnu priepasť a zabezpečiť, aby znevýhodnené alebo marginalizované deti (kvôli chudobe, vidieckej lokalite, pohlaviu, zdravotnému postihnutiu atď.) nezaostávali v digitálnom veku – v súlade so zásadami nediskriminácie a rovnosti príležitostí uvedenými v Dohovore.

Výbor vo svojich nedávnych pripomienkach ocenil úsilie o digitálnu inklúziu ako pozitívny krok.¹⁸ Napríklad v roku 2023 Výbor s uznaním ocenil opatrenia, ktoré Spojené kráľovstvo podniklo na podporu digitálnej inklúzie počas pandémie, pričom uznal, že prístup je pre deti nevyhnutný na uplatňovanie ich práv. Prístup však musí byť spojený s prostredím, ktoré je bezpečné a vhodné pre vek a schopnosti detí;

¹⁶ LIVINGSTONE, Sonia – THIRD, Amanda – LANSDOWN, Gerison: Children vs adults: negotiating UNCRC General Comment No. 25 on children's rights in the digital environment. In: MURRAY, Andrew – GILL, Lex (eds.): Research Handbook on Law and Technology. Cheltenham: Edward Elgar, 2024, doi: 10.4337/9781800887206.00042.

¹⁷ Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc. CRC/C/GC/25 (2 March 2021), paras. 11, 99.

¹⁸ UN Committee on the Rights of the Child: Concluding Observations: United Kingdom, 2 June 2023. Children's Legal Centre Wales

jednoduché pripojenie detí na internet bez ochrany nie je primeraný prístup založený na právach.

Ochrana pred ujmom - Práva detí na ochranu pred násilím, vykorisťovaním a škodlivým obsahom sú priamo ovplyvnené digitálnymi technológiami. Článok 19 Dohovoru zaväzuje štáty chrániť deti pred všetkými formami násillia, článok 34 pred sexuálnym vykorisťovaním a zneužívaním a článok 36 pred všetkými ostatnými formami vykorisťovania. V digitálnej sfére to znamená riešiť hrozby, ako je šikanovanie, obťažovanie, sexuálne zneužívanie, obchodovanie s ľuďmi, vystavenie pornografii alebo extrémnemu násilliu a šírenie materiálov so sexuálnym zneužívaním detí (*child sexual abuse material* - CSAM). Rozsah týchto hrozieb narastá – počet hlásení o online materiáloch so sexuálnym zneužívaním detí prudko vzrástol (americká horúca linka NCMEC zaznamenala v rokoch 2019 až 2023 nárast hlásení o CSAM o 87%),¹⁹ a až jedno z piatich detí v niektorých krajinách zažilo v uplynulom roku sexuálne zneužívanie online.

GC25 naliehavo žiada prijatie dôrazných opatrení, vrátane aktualizácie trestných zákonov, zlepšenia techník presadzovania práva (pri zachovaní procesných práv detí) a medzinárodnej spolupráce v boji proti zneužívaniu detí online. Zdôrazňuje tiež preventívne opatrenia: vzdelávanie detí a rodičov, podporu pozitívnych online zážitkov a integráciu bezpečnosti už pri návrhu do digitálnych produktov. Ešte pred GC25 výbor identifikoval problémy ako kyberšikana ako vážne obavy. V roku 2016 napríklad Výbor s obavami konštatoval, že šikanovanie – vrátane kyberšikanovania – je vážnym a rozšíreným problémom, a odporučil vzdelávať deti, učiteľov a rodiny v oblasti bezpečného používania internetu a zapojiť platformy sociálnych médií do boja proti kyberšikanovaniu.²⁰ Zdôrazňuje sa tým, že cieľom ochrany nie je úplne odstrániť deti z online prostredia, ale zmierniť riziká a budovať odolnosť.

Zahrňa to aj ochranu údajov a súkromia. Uznanie, že nadmerné zbieranie údajov alebo profilovanie detí digitálnymi službami môže predstavovať riziko (napr. zneužitie osobných údajov, rušivé monitorovanie, manipulácia prostredníctvom cielených reklám). Podľa článku 16 UNCRC (ochrana súkromia) a moderných zákonov o ochrane údajov si deti zaslúžia osobitné záruky v súvislosti so spôsobom zbierania a používania ich údajov. Stručne povedané, právo na ochranu vyžaduje, aby bolo digitálne prostredie bezpečné pre deti.

Autonómia a účasť - Ako deti rastú, vyvíja sa ich schopnosť autonómneho rozhodovania a majú právo zúčastňovať sa na záležitostiach, ktoré sa ich týkajú

¹⁹ WeProtect Global Alliance: Analysis of the sexual threats children face online. In: 2023 Global Threat Assessment. WeProtect, 2023, s. —. Zisťovanie uvádza, že objem hlásení detského sexuálneho zneužívanie materiálov zaznamenaných National Center for Missing and Exploited Children vzrástol o 87 % od roku 2019.

²⁰ UN Committee on the Rights of the Child: Concluding Observations, CRC/C/GBR/CO/5, 3 June 2016: United Kingdom of Great Britain and Northern Ireland.

(článok 12), právo na slobodu myslenia (článok 14), svedomia a náboženstva a právo na slobodu združovania (článok 15). Online platformy sa stali kľúčovými miestami pre aktivizmus mládeže, budovanie komunity a sebaujadrenie. Brať deti vážne ako nositeľov práv znamená rešpektovať tieto slobody - aj v digitálnom priestore. Jedným z aspektov autonómie je súkromie: deti, najmä dospelávajúci, potrebujú určitú súkromnú sféru, aby mohli objavovať svoju identitu a komunikovať – napriek tomu sú však často pod intenzívnym dohľadom online, či už zo strany rodičov, škôl alebo spoločností. Nájsť rovnováhu medzi právom dieťaťa na súkromie a povinnosťou dohliadať na/chrániť ho je citlivá záležitosť. UNCRC zavádza pojem „*vyvíjajúce sa schopnosti*“ (článok 5) – rodičia a iné osoby by mali poskytovať usmernenia a vedenie v súlade s vývojom zrelosti dieťaťa. V praxi to znamená, že online súkromie a konanie 16-ročného dieťaťa si zaslúži väčší rešpekt ako v prípade 6-ročného dieťaťa a právne rámce môžu kalibrovať požiadavky (napríklad mnohé jurisdikcie stanovujú vekové hranice, od ktorých môže dieťa súhlasiť so spracovaním osobných údajov alebo používaním určitých online služieb).

GC25 zdôrazňuje, že opatrenia na ochranu detí online musia rešpektovať aj ich ostatné práva a varuje pred neprimeranými obmedzeniami. Ako Výbor poznamenáva, príliš prísny prístup – napríklad plošný zákaz sociálnych médií alebo všadeprítomné filtrovanie informácií – môže porušovať práva detí na prístup k informáciám, účasť a právo byť vypočuté. Kľúčové je nájsť správnu rovnováhu. Výbor vyzýva k vyváženému prístupu, ktorý chráni deti pred ujmom a zároveň im umožňuje zodpovedne sa zapájať do digitálneho prostredia. Tento názor odrážajú aj usmernenia Rady Európy, ktoré zdôrazňujú potrebu ochranných opatrení a stratégií gramotnosti/posilňovania postavenia.²¹

Tieto tri rozmery – prístup, ochrana, autonómia – sa niekedy považujú za protichodné, ale autorka tejto štúdie ich vníma ako komplementárne. Najlepší záujem dieťaťa (článok 3) poskytuje interpretačný princíp na riešenie napätia v konkrétnych prípadoch: napríklad pri rozhodovaní o moderovaní obsahu alebo overovaní veku by sa malo starostlivo zvážiť ako ochranné dôvody, tak aj vplyv na prístup k informáciám a účasť, s cieľom nájsť riešenia, ktoré slúžia celkovému najlepšiemu záujmu detí.

Digitálne prostredie, ktoré rešpektuje práva detí, je také, ktoré maximalizuje inklúziu a posilňovanie postavenia a zároveň minimalizuje riziko. Tento dvojité cieľ je jadrom mnohých nových nariadení a výslovne ho podporuje GC25. V ďalšej časti skúmame, ako sa tieto zásady začali presadzovať v praxi Výboru OSN pre práva dieťaťa, najmä prostredníctvom jeho záverečných odporúčaní adresovaných zmluvným štátom.

²¹ Council of Europe, Committee of Ministers: Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Recommendation CM/Rec(2018)7, adopted 4 July 2018). Strasbourg: Council of Europe.

Od marginality k mainstreamu - Digitálna technológia v záverečných odporúčaniach Výboru

Vplyv Všeobecného komentára č. 25 je zrejmý v rozvíjajúcej sa práci Výboru OSN pre práva dieťaťa. Výbor vydáva záverečné odporúčania pre štáty po preskúmaní ich pravidelných správ o implementácii UNCRC. Tieto pozorovania poukazujú na pokrok, obavy a odporúčania. Empirický pohľad na záverečné odporúčania pred a po roku 2021 odhaľuje jasný nárast odkazov na digitálne skúsenosti a práva detí.

V desaťročí pred GC25 sa Výbor zaoberal digitálnymi otázkami, ale len sporadicky a často z hľadiska konkrétnych škôd. Napríklad v záverečných odporúčaniach pre Spojené kráľovstvo v roku 2016 sa uvádzali obavy týkajúce sa kyberšikany a odporúčalo sa, aby štát „zintenzívnil úsilie“ v boji proti šikane, vrátane online šikany, prostredníctvom vzdelávania detí a zapojenia platforiem sociálnych médií do riešení.²² Výbor v tomto odporúčaní odkazoval aj na svoj Deň všeobecnej diskusie v roku 2014, čím preukázal povedomie o vplyve digitálnych médií.

Podobne sa občas objavovali otázky ako sexuálne zneužívanie detí online alebo potreba vzdelávania v oblasti bezpečnosti na internete, ktoré boli zvyčajne zaradené do sekcií týkajúcich sa násilia alebo zneužívania. Výbor však vo svojich vyjadreniach zriedka považoval digitálne prostredie za holistický kontext pre práva detí; internet bol skôr spomínaný ako faktor určitých porušení (napr. šírenie detskej pornografie online) alebo ako nástroj, ktorý je možné využiť (napr. na vzdelávanie). Neexistovala žiadna konzistentná výzva na komplexnú digitálnu politiku pre deti a pojmy ako digitálne prostredie alebo online ekosystém sa takmer nevyskytovali. Koncepcia digitálnych práv detí bola ešte v plienkach. Samotné správy štátov sa často zameriavali na tradičné otázky, pričom digitálne otázky boli druhoradé. Hoci Výbor uznal vznikajúce online riziká – napríklad vydal odporúčania týkajúce sa regulácie médií alebo školení o bezpečnom používaní IKT –, tieto odkazy boli relatívne málo početné a úzko vymedzené.

Po prijatí GC25 v roku 2021 došlo k výraznému posunu. Záverečné poznámky Výboru začali systematicky integrovať digitálny rozmer do viacerých oblastí práv. GC25 výslovne pripomenul štátom, že Dohovor sa vzťahuje aj na online prostredie, čím Výboru poskytol silnejší základ na preskúmanie národných snáh v oblasti digitálnej inklúzie, ochrany a regulácie. Napríklad v záverečných odporúčaniach Spojeného kráľovstva z roku 2023 (v nadväznosti na kombinovanú 6./7. správu Spojeného kráľovstva) Výbor nielen privítal kroky podniknuté na zlepšenie digitálneho prístupu detí, ale vydal aj konkrétne odporúčania týkajúce sa digitálneho prostredia.²³

²² UN Committee on the Rights of the Child: Concluding Observations, CRC/C/GBR/CO/5, 3 June 2016: United Kingdom of Great Britain and Northern Ireland.

²³ Office of the Commissioner for Children and Young People (NICCY): Advice on Ofcom's consultation on a safer online life for women and girls – practical guidance for tech companies.

S uznaním vzal na vedomie úsilie vynaložené v oblasti digitálnej inklúzie počas pandémie COVID-19 a ocenil pokrok v poskytovaní deťom prístupu k online vzdelávaniu a službám.²⁴ Zároveň naliehavo vyzval Spojené kráľovstvo, aby prijalo pripravovaný zákon o online bezpečnosti, aby sa zabezpečilo, že všetky zákony a politiky v digitálnom prostredí chránia deti pred škodlivým obsahom a inými online rizikami. Toto odporúčanie (odseky 28 – 29 Záverečného odporúčania pre Spojené kráľovstvo z roku 2023) výslovne zasadzuje diskusiu do kontextu digitálneho prostredia, čo naznačuje širší prístup ako v predchádzajúcich rokoch, keď Výbor spravidla izoloval jednu otázku (napríklad kyberšikanu) v jednom odseku.

Podobne aj nedávne záverečné odporúčania pre iné krajiny (napr. Slovensko 2025,²⁵ Fínsko 2023,²⁶ Južná Afrika 2022,²⁷ atď.) čoraz častejšie odkazujú na potrebu národných stratégií v oblasti digitálnych práv detí a upozorňujú na GC25 ako usmernenie. Výbor odporučil, aby štáty vypracovali komplexné plány na implementáciu odporúčaní GC25, ako je začlenenie digitálnej gramotnosti do školských osnov, posilnenie legislatívy v oblasti ochrany detí online a spolupráca s technologickými spoločnosťami na presadzovaní bezpečnostných noriem. Výrazy *digitálne prostredie* a *online* sa po roku 2021 objavujú oveľa častejšie vo výstupoch Výboru, často vo viacerých častiach záverečných odporúčaní (napr. vzdelávanie, násilie, vykorisťovanie, súkromie).

Podstata týchto odporúčaní tiež odráža jemnejšie chápanie. Kým sa napríklad skoršie hodnotenia zameriavali len na hrozby (ako napr. materiály so sexuálnym zneužívaním detí), novšie pozorovania pokrývajú celé spektrum: od zabezpečenia spravodlivého prístupu k internetu pre znevýhodnené deti, cez ochranu súkromia a osobných údajov, až po riešenie nenávistných prejavov alebo dezinformácií online, ktoré môžu ovplyvniť deti. Výbor presadzuje rovnováhu založenú na právach: pripomína štátom, aby chránili deti a zároveň rešpektovali ich práva na informácie a účasť online. Je to v súlade s dôrazom GC25, že opatrenia by nemali neprimerane obmedzovať prospešné využívanie digitálnych zdrojov pre mladých ľudí.

Dôležitým dôsledkom tejto zmeny je, že štáty sú teraz zodpovedné za implementáciu práv detí v digitálnom kontexte ako súčasť ich celkového dodržiavania UNCRC. Prítomnosť GC25 vo výstupoch Výboru signalizuje vládam, že digitálna politika je kľúčovou súčasťou práv detí, nie voliteľnou alebo sekundárnou záležitosťou. Mnohé štáty odvtedy vo svojich správach odkazujú na GC25 a uznávajú,

²⁴ UN Committee on the Rights of the Child: Concluding Observations: United Kingdom, 2 June 2023.

²⁵ UN Committee on the Rights of the Child: Concluding Observations, CRC/C/SVK/CO/6, 26 February 2025: Slovak Republic. United Nations.

²⁶ UN Committee on the Rights of the Child: Concluding Observations, CRC/C/FIN/CO/5-6, 26 May 2023: Finland. In: United Nations.

²⁷ UN Committee on the Rights of the Child: Concluding Observations, CRC/C/ZAF/CO/3-6, 11 March 2024: South Africa. United Nations.

že musia aktualizovať svoje zákony a postupy. Odporúčania Výboru často povzbudzujú štáty, aby vyhľadávali technickú pomoc alebo zdieľali osvedčené postupy na ochranu detí online, čím preukazujú pochopenie, že ide o rýchlo sa vyvíjajúcu oblasť, ktorá si vyžaduje medzinárodnú spoluprácu.

Frekvencia výskytu pojmov ako digitálny alebo online v záverečných odporúčaní sa po roku 2021 výrazne zvýšila a kontext sa posunul od izolovaných obáv ku komplexnému prístupu k právam detí v digitálnom priestore. Toto empirické pozorovanie podčiarkuje normatívny bod: práva detí v digitálnom prostredí sa posunuli z okraja do hlavného prúdu medzinárodného monitorovania. Hlas Výboru v tejto otázke zosilňuje posolstvo, že práva detí nekončia tam, kde začína digitálny svet. Namiesto toho rámec UNCRC – dynamicky interpretovaný prostredníctvom GC25 – sprevádza dieťa do virtuálnych priestorov a trvá na ochrane a slobodách v týchto priestoroch rovnako ako v školách, domovoch alebo na ihriskách.

Záver

Digitálne prostredie je dnes základnou súčasťou detstva. V tomto článku sme argumentovali, že medzinárodné právo na čele s UNCRC a objasnené všeobecným komentárom č. 25 – musí digitálnu sféru prijať ako neoddeliteľnú súčasť realizácie práv detí. Práva detí sa nekončia na prahu kyberpriestoru; skôr sa celé spektrum práv prenáša spolu s dieťaťom a vyžaduje si rešpekt, ochranu a naplnenie online rovnako ako offline. Dosiahnutie tohto cieľa je jednou z veľkých výziev v oblasti práv detí v 21. storočí, ktorá si vyžaduje jasnosť doktríny, inovatívne zákony a záväzok počúvať samotné deti.

Z doktrínálneho hľadiska sme videli, že UNCRC poskytuje silný rámec, ktorý pri správnom výklade pokrýva aj digitálne otázky – od súkromia po ochranu pred ujmom – a že GC25 bol prelomovým momentom pri formulovaní povinností štátov v tejto oblasti. Empiricky sa prax Výboru OSN pre práva dieťaťa vyvinula tak, že do svojho monitorovania začlenila digitálne práva, čím všetkým štátom signalizovala, že digitálny život detí je kľúčovou súčasťou ich bilancie v oblasti ľudských práv. Porovnanie záverečných odporúčaní pred a po roku 2021 zdôraznilo dôležitý bod: len čo Výbor výslovne uznal digitálne práva, podnietilo to konzistentnejšiu a podstatnejšiu pozornosť venovanú týmto otázkam na medzinárodnej úrovni.

Súbežne s tým právne a regulačné trendy – najmä v Európe – naznačujú sľubné prijatie zásad detských práv. Legislatíva ako GDPR²⁸ a DSA²⁹ a nástroje ako Kódex

²⁸ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

²⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu digitálnych služieb a o zmene smernice 2000/31/ES (Akt o digitálnych službách – Digital Services Act).

vekovo primeraného dizajnu³⁰ poskytujú konkrétne mechanizmy na presadzovanie práv detí na súkromie, ochranu pred škodlivým obsahom a účasť v bezpečnejšom online priestore. Tieto snahy, hoci sa stále vyvíjajú, ukazujú, ako sa abstraktné zásady Dohovoru dajú premeniť na prevádzkové normy (napr. žiadne profilovanie detí pre reklamy, vysoké nastavenia ochrany súkromia ako predvolené, povinné posudzovanie rizík pre platformy). Ilustrujú tiež synergiu medzi globálnymi usmerneniami a miestnymi opatreniami - vplyv GC25 je viditeľný v mnohých z týchto reforiem a naopak, národné inovácie ponúkajú modely, ktoré sa dajú replikovať aj inde.

Ešte však máme pred sebou veľa práce. Digitálne prostredie sa neustále mení, rovnako ako riziká a príležitosti pre deti. Nástup nových technológií, ako je generovanie obsahu na základe umelej inteligencie, biometrické sledovanie alebo imerzná realita, otestuje našu schopnosť dodržiavať práva detí. Musíme zostať ostražití, aby sa ochranné opatrenia nezmenili na neoprávnené obmedzenia. Musíme tiež zabezpečiť, aby žiadne dieťa nezostalo opomenuté: digitálne vylúčenie sa stalo novou podobou sociálneho vylúčenia a preklenutie tejto priepasti (pre dievčatá, deti z rurálnych oblastí, deti so zdravotným postihnutím a iné) je neoddeliteľnou súčasťou prístupu založeného na právach.

Brať deti vážne ako nositeľov práv v digitálnom prostredí znamená naďalej ich zapájať do hľadania riešení. Skúsenosti a postrehy detí budú neoceniteľné pri tvorbe politík, ktoré skutočne fungujú v praxi (alebo na obrazovke). Či už ide o návrh rozhrania aplikácie, ktoré je intuitívne a nevyužíva deti, alebo o vypracovanie národnej stratégie online bezpečnosti, zahrnutie pohľadu detí pomáha zosúladiť výsledky s ich najlepšimi záujmami. Duch článku 12, umocnený ochotou digitálnej generácie vyjadriť svoj názor, dáva nádej, že ďalšiu vlnu digitálnych inovácií budú riadiť tí, ktorých sa to najviac týka: samotní mladí ľudia.

Realizácia medzinárodnej ochrany detí v digitálnom prostredí nie je jednorazovým projektom, ale neustálou úlohou. Vyžaduje si inovácie založené na právach a medzinárodnú spoluprácu, ktorá uznáva bezhraničnú povahu internetu.

Hlavné posolstvo je jednoduché, ale hlboké: práva detí za obrazovkou sú stále právami detí. Našou úlohou je posunúť toto chápanie ďalej a zabezpečiť, aby sa právo, politika a prax vyvíjali súbežne s realitou detí, aby sa sľub UNCRC naplnil aj v tejto digitálnej ére.

Zoznam použitej literatúry

1. AYLAWEW, Yohannes Eneyew – VERDOODT, Valerie – LIEVENS, Eva: General Comment No. 25 on Children's Rights in Relation to the Digital Environment:

³⁰ Information Commissioner's Office: Age appropriate design: a code of practice for online services (UK Age Appropriate Design Code). London: ICO, 2020.

Implications for Children's Right to Privacy and Data Protection in Africa. In: Human Rights Law Review, Roč. 24, č. 3 (september 2024). doi: 10.1093/hrlr/ngae018.

2. Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, UN Doc. CRC/C/GC/25 (2 March 2021), paras. 11, 99.
3. Committee on the Rights of the Child: General comment No. 25 (2021) on children's rights in relation to the digital environment, 2 March 2021, para. 5.
4. Committee on the Rights of the Child: Report of the 2014 Day of General Discussion "Digital Media and Children's Rights". United Nations, 2014.
5. Council of Europe, Committee of Ministers: Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Recommendation CM/Rec(2018)7, adopted 4 July 2018). Strasbourg: Council of Europe.
6. Information Commissioner's Office: Age appropriate design: a code of practice for online services (UK Age Appropriate Design Code). London: ICO, 2020.
7. DADI, Afework Fekadu – DACHEW, Berihun Assefa – TESSEMA, Gizachew Assefa: Problematic internet use: A growing concern for adolescent health and well-being in a digital era. In: Journal of Global Health, Roč. 14 (2024), s. 03034. doi: 10.7189/jogh.14.03034.
8. GARAYOVÁ, Lilla: Protecting children's rights in the age of digitalisation: Legal implications for the best interests of the child. In: Pakistan Journal of Life and Social Sciences, Roč. 22, č. 2 (2024), s. 7351–7366. doi: 10.57239/PJLSS-2024-22.2.00555.
9. LIVINGSTONE, Sonia – THIRD, Amanda – LANSDOWN, Gerison: Children vs adults: negotiating UNCRC General Comment No. 25 on children's rights in the digital environment. In: MURRAY, Andrew – GILL, Lex (eds.): Research Handbook on Law and Technology. Cheltenham: Edward Elgar, 2024, doi: 10.4337/9781800887206.00042.
10. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).
11. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu digitálnych služieb a o zmene smernice 2000/31/ES (Akt o digitálnych službách – Digital Services Act).
12. Office of the Commissioner for Children and Young People (NICCY): Advice on Ofcom's consultation on a safer online life for women and girls – practical guidance for tech companies.

13. THIRD, Amanda – MOODY, Lucy: Our rights in the digital world: A report on the children's consultations to inform UN CRC General Comment 25. London – Sydney: 5Rights Foundation and Western Sydney University, 2021.
14. UN Committee on the Rights of the Child: Concluding Observations, CRC/C/FIN/CO/5-6, 26 May 2023: Finland. In: United Nations.
15. UN Committee on the Rights of the Child: Concluding Observations, CRC/C/GBR/CO/5, 3 June 2016: United Kingdom of Great Britain and Northern Ireland.
16. UN Committee on the Rights of the Child: Concluding Observations, CRC/C/SVK/CO/6, 26 February 2025: Slovak Republic. United Nations.
17. UN Committee on the Rights of the Child: Concluding Observations, CRC/C/ZAF/CO/3-6, 11 March 2024: South Africa. United Nations.
18. UN Committee on the Rights of the Child: Concluding Observations: United Kingdom, 2 June 2023.
19. UN Committee on the Rights of the Child: Concluding Observations: United Kingdom, 2 June 2023. Children's Legal Centre Wales
20. UN General Assembly: Convention on the Rights of the Child. In: United Nations, Treaty Series, vol. 1577, p. 3, 20 November 1989.
21. United Nations, Committee on the Rights of the Child: General Comment No. 25 (2021) on children's rights in relation to the digital environment, adopted on 2 March 2021.
22. WeProtect Global Alliance: Analysis of the sexual threats children face online. In: 2023 Global Threat Assessment. WeProtect, 2023.

Kontaktné údaje

doc. JUDr. PhDr. Lilla Garayová, PhD. LL.M

lilla.garayova@paneurouni.com

Ústav medzinárodného a európskeho práva, Paneurópska vysoká škola

INTERNATIONAL LEGAL REGULATION OF REMOTE SENSING OF THE EARTH FROM SPACE AND ITS APPLICATION FOR ENVIRONMENTAL PROTECTION

Liudmyla Golovko¹

Abstract: Remote sensing of the Earth undoubtedly has a number of advantages: it provides the possibility of comprehensive monitoring of the objects studied according to all indicators, speed, the ability to obtain data over large areas including the data from hard-to-reach places. This indicates the need for proper legal regulation, including at the international level. The purpose of the article is to analyze the current international legal regulation of remote sensing of the Earth and its use for environmental protection, identify its possible shortcomings, and propose topics *de lege ferenda*. When writing the article, general theoretical methods were mainly used. Analysis, synthesis and theoretical generalization helped to assess the sufficiency of international legal regulation of the remote sensing of the Earth. The necessity of adoption of an international treaty in this sphere was identified. This treaty should define states' and private entities' responsibilities, establish standards for data dissemination, liability for damage caused during Earth sensing other than the fall of a satellite, etc. Analysis of the courts' decisions in which results of the remote sensing of the Earth were used as evidence could also have practical implications.

Keywords: remote sensing, international environmental law, protection of environment, evidence in environmental litigation

Introduction

As of May 2025, the satellite tracking website "Orbiting Now" lists 12,149 active satellites in various Earth orbits ². Remote sensing is widely used in different spheres: in agriculture to monitor crop health ³, its growth, identify diseases and make more informed decisions in its harvesting; environmental protection to monitor changes in

¹VEGA 1/0713/23 "International legal protection of environmental rights – quo vadis?".

² How Many Satellites are in Space? (2025). URL: <https://nanoavionics.com/blog/how-many-satellites-are-in-space/>

³ LOTTERING, R., PEERBHAY, K., ADELABU, S. (2025). Remote Sensing Applications in Agricultural, Earth and Environmental Sciences. *Applied Sciences*, 15(8), 4537. <https://doi.org/10.3390/app15084537>

climate change ⁴, detect wildfires, monitor desertification, endangered species, illegal fishing ⁵; disaster management and urban planning to obtain information concerning natural disasters, to obtain information on land use, to identify areas where recovery activities are needed ⁶, etc.

Of course, we have given only a few examples. The possibilities of using the results of land sounding are unlimited. And they require legal regulation both at the national and international levels. The aim of the article is to analyze the current international regulation of remote sensing, identify its possible shortcomings and topics *de lege ferenda*. Special attention will be paid to the international legal regulation of the use of remote sensing images as evidence in environmental legal proceedings.

International legal regulation of remote sensing of the Earth

The Outer Space Treaty is the basic legal framework for the activities of states in outer space and on celestial bodies. According to article III of the Outer Space Treaty each state has the right to use the outer space, including the Moon and other celestial bodies for peaceful purposes in accordance with international law? ⁷ This means that each state has the right conduct remote sensing.

The current model of international space law was created at a time when the use of space for private purposes was not expected. If it was envisaged, then as a distant prospect on a small scale. Therefore, all international obligations related to space activities are placed on states. The 1975 Convention on Registration of Objects Launched into Outer Space requires each state to record in a national registry all objects, which it launches into a space. According to article II, each launching state must also inform the Secretary-General of the United Nations of the establishment of such a registry. If two or more states take part in a launch, they shall decide jointly which of them shall register the object. According to article IV, each state of registration must provide the UN

⁴ VASHCHENKO, Y. (2021). Access to Modern Energy Services Through the Prism of Children's Rights: An Overview from the Perspectives of the Convention on the Rights of the Child and the Policy and Law Approaches of Certain EU Member States and Ukraine. *International Comparative Jurisprudence*, Volume 7, Issue 1, p. 75–87. DOI: <http://dx.doi.org/10.13165/j.icj.2021.06.006>

⁵ YEMELIANENKO, K., LADYCHENKO, V., YARYNKO, B. (2024). International legal and national mechanisms for overcoming the environmental consequences of the armed aggression of the Russian federation against Ukraine. *Law of Ukraine*, Vol. 10 (1), p. 151–165.

⁶ NOVAK, T., MELNYK, V., KOVALCHUK, I., PAKHOMOVA, A., NASTINA, O. (2024). Legal Support for Sustainable Agroecological Development: Evidence from Ukraine. *European Journal of Sustainable Development*, 13(2), 247. DOI: <https://doi.org/10.14207/ejsd.2024.v13n2p247>

⁷ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. (1966). URL: <https://www.unoosa.org/oosa/en/ourwork/space/aw/treaties/outerspacetreaty.html>

Secretary-General details about each space object entered in its registry as soon as possible⁸.

According to Article VI of the Outer Space Treaty, states are responsible for national activities in outer space, including the Moon and other celestial bodies, whether carried out by a governmental organization or a nongovernmental institution. They are also obliged to ensure that national activities are carried out in accordance with the provisions contained in the Outer Space Treaty. Activities of non-governmental institutions in outer space, including the Moon and other celestial bodies, shall be authorized and continuously monitored by the State Party concerned. When activities in outer space, including the Moon and other celestial bodies, are carried out by an international organization, the international organization and the States Parties that are members of that organization are responsible for compliance with this Treaty.

The State on whose registry an object launched into outer space is registered retains jurisdiction and control over that object and its entire crew for as long as it is in outer space or on a celestial body. Ownership of objects and their components launched into outer space, including objects that have landed or been constructed on a celestial body, is not affected by their stay in outer space or on a celestial body or by their return to Earth. Such objects or components found beyond the borders of the State on whose registry they are registered must be returned to that State (Article 8 of the Outer Space Treaty).

However, none of the above-mentioned treaties regulates the issue of remote sensing of the Earth. The only international document that regulates this issue is Resolution adopted by the UN GA No. 41/65 Principles Relating to Remote Sensing of the Earth from Outer Space⁹. The document contains 15 principles that countries should follow when conducting remote sensing of the Earth.

According to Principle I, the term "remote sensing" means "the sensing of the Earth's surface from space by making use of the properties of electromagnetic waves emitted, reflected or diffracted by the sensed objects, for the purpose of improving natural resources management, land use and the protection of the environment"¹⁰. As we can see, when developing the document, the countries envisaged the use of remote sensing of the Earth for the purpose of protecting the environment, natural resources, as well as in the field of land use.

⁸ Convention on Registration of Objects Launched into Outer Space. United Nations, Treaty Series, vol. 1023, UNGA Resolution No. 41/65 Principles Relating to Remote Sensing of the Earth from Outer Space. (1965).

URL: <https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html>

⁹ UN GA Resolution № 41/65 Principles Relating to Remote Sensing of the Earth from Outer Space. (1965). URL: <https://digitallibrary.un.org/record/126423?v=pdf>

¹⁰ Ibid.

However, the list is not exhaustive. Nowadays, remote sensing of the earth is carried out in various fields, ranging from disaster forecasting, spatial planning of the land, agriculture and ending with military purposes. Therefore, we are observing an expansion of the scope of applications of remote sensing of the Earth beyond the framework outlined in the resolution.

A separate problematic issue is the exchange of information obtained as a result of remote sensing of the Earth. We agree with I. Zabara, who claims that the main problem among others remains the problem of uncontrolled dissemination of remote sensing data and information, which can harm the economic, military and other vital interests of states. Such a vision follows from the positions of individual states that have enshrined in their national legislation provisions on free user access to digital sensing data¹¹. What information can and should be provided and to whom should be clearly regulated at the international level. Resolution No. 41/65, which is not binding, only contains provisions that the state being observed has a right to access primary data, processed data and analyzed information about its territory for a reasonable price (principle XII), and provisions on providing information the state being observed that may prevent damage to the environment (principle X), or in the event of natural disasters (principle XI), which is clearly not enough.

A separate issue that requires international regulation is the establishment of liability for damage caused by remote sensing of the Earth. Resolution No. 41/65 does not regulate this issue. However, the issue of liability for damage caused by remote sensing of the Earth is covered by the Outer Space Treaty of 1967 and the Liability Convention of 1972¹².

According to article VII of the Outer Space Treaty, every State which launches or procures the launch of objects into outer space, including the Moon and other celestial bodies, and every State from whose territory or facility an object is launched, is internationally responsible for damage caused by such objects or their components to another State or its natural or legal persons on Earth, in airspace or in outer space, including the Moon and other celestial bodies.

The Liability Convention establishes the absolute liability of states for damage caused by a space object on the surface of the earth. Therefore, in the event of the fall of a satellite carrying out remote sensing of the earth, the state in whose registry the object is registered must pay compensation (article 3).

However, given the specificity of earth sensing activities, there is a need for legal regulation of a much wider range of issues and liability for damage caused during

¹¹ ZABARA, I. (2018). Remote sensing of the earth: past and present international legal regulation of obtaining and using information. *Information and law*, № 1 (24), P. 36- 43. P. 41

¹² UN GA Resolution 2777 (XXVI). Convention on International Liability for Damage Caused by Space Objects. (1972). URL: <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html>

earth sensing other than the fall of a satellite. One must agree with the authors who consider it necessary to regulate liability for damage caused by the provision of inaccurate information ¹³. A number of authors consider it necessary to regulate at the international level the activities of private individuals who carry out remote sensing of the earth ¹⁴. Iryna Ryzhenko believes it is necessary to retain absolute responsibility of states for damage caused by space objects, at the same time she states, that it is necessary to ensure compensation for losses due to the negative consequences of space activities. According to her, national legislation should provide for a regime of mandatory insurance against damage caused to third parties, regardless of whether space activities are carried out by entities under public or private law of each specific country, since these losses must be compensated by the government of the country carrying out space activities, and regardless of whether they will be paid abroad or on the territory of this state ¹⁵.

Trevor Kehrler also points out the obsolescence of the Convention's norms and speaks of the need to regulate liability for cyber attacks at the international level ¹⁶. Joel A. Dennerley speaks about the need to take into account the circumstances of each case when establishing liability for the damage caused ¹⁷.

It is necessary to amend the international legal regulation of the institution of liability in space in general and during the remote sensing of the Earth in particular. The current international legal regulation in this area is outdated and does not meet the needs of the day.

The use of remote sensing data as evidence in court proceedings

An important issue to consider is the admissibility of satellite imagery as evidence in cases concerning violations of environmental law. At the international level, this question remains unresolved. Nevertheless, in several jurisdictions - including the United States, the United Kingdom, and EU member states satellite images have

¹³ KIM, Y.-J. (2024). Commercial Use of Satellite Remote Sensing Data and Civil Liability, *Laws*, 13, 77. URL: <https://www.mdpi.com/2075-471X/13/6/77>

¹⁴ ZEMBLICKI, B., ORALOVA, Y. (2021). Private Entities in Outer Space Activities: Liability Regime Reconsidered
URL:

<https://www.sciencedirect.com/science/article/pii/S0265964621000199>

¹⁵ RYZHENKO, I. (2018). State Participation in Space Activities: Some Legal Approaches and Implications, *Advanced Space Law*, Volume 2, p. 50 - 62. P. 61

¹⁶ KEHRER, T. (2024). Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space. *Chicago Journal of International Law*, Vol. 20 (1). URL: <https://chicagounbound.uchicago.edu/cjil/vol20/iss1/5/>

¹⁷ JOEL, A. Dennerley, State Liability for Space Object Collisions: The Proper Interpretation of 'Fault' for the Purposes of International Space Law, *European Journal of International Law*, Volume 29, Issue 1, February 2018, Pages 281-301, <https://doi.org/10.1093/eil/chy003>

already been used in court as supporting evidence in such cases. The following section will examine selected cases in order to analyze national practices in using this type of evidence and the legal challenges that have emerged.

United States v. Reserve Mining Company (No. 5-72 Civil 19) was the first case in the United States in which images obtained through remote sensing were used as evidence in court. In this case, the Reserve Mining Company continuously discharged large amounts of minute amphibole fibers into Lake Superior and into the air of Silver Bay, causing severe environmental damage, particularly to water resources. The court found that by refusing to construct a proper disposal system, the company had violated the Federal Water Pollution Control Act and Minnesota regulations. Satellite photographs played a decisive role in establishing the company's liability. Images of green water in the western arm of the lake showed widespread dispersion and demonstrated upwelling phenomena, thereby proving that the pollution could not be attributed to natural processes ¹⁸.

This case set an important precedent by recognizing satellite imagery as admissible and reliable evidence in environmental litigation.

In the case *Dow Chemical Co. v. United States* (1986), the U.S. Supreme Court had to decide whether the Environmental Protection Agency's (EPA) warrantless aerial photography of a plant's territory violated the Fourth Amendment of the U.S. Constitution. The court emphasized that the open areas of industrial plant complex must be distinguished from private property where individuals have a reasonable expectation of privacy protected by the Amendment ¹⁹. The district court had originally ruled that the EPA's aerial surveillance violated the Fourth Amendment, but this decision was reversed by the Court of Appeals, which held that the EPA's aerial observation of the plant did not exceed its statutory investigatory authority, and that the photography of 2,000-acre plant complex without a warrant was lawful under U.S. law. The Supreme Court affirmed the Court of Appeals' decision. This case illustrates that concerns about privacy invasion are one of the reasons why the use of satellite imagery has not yet become widespread as admissible evidence in court. At the same time this decision shows that even such a sensitive issue as the protection of privacy is not an obstacle to the use of this type of evidence in environmental cases because the expectation of privacy is much higher for individuals than for industrial facilities that may contribute to environmental pollution.

In the United Kingdom, there has also been a growing tendency to use remote sensing images as evidence in court proceedings. In February 2012, the European

¹⁸ *United States v. Reserve Mining Company* № 5-72 Civil 19 (D. Minn. April 20, 1974; May 11, 1974). URL: <https://www.elr.info/sites/default/files/litigation/4.20573.htm>. Para 30.

¹⁹ *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986). URL: <https://supreme.justia.com/cases/federal/us/476/227/>

Maritime Safety Agency detected pollution in waters near Cornwall with the help of satellite imagery. The vessel responsible was identified as the tanker Maersk Kiera, registered to Singapore Private Ltd. The tanker initially denied its responsibility but later admitted to cleaning its tank and discharging waste (palm oil and tank cleaning solution) but claimed that this had occurred outside the 12 nautical miles from the shore, where such discharges are permitted. However, satellite images demonstrate that the pollution had taken place within the 12 nautical mile zone, making this discharge unlawful²⁰. The owner of the tanker was found guilty. This case demonstrates that satellite imagery can serve as decisive evidence in criminal proceedings, enabling authorities to identify and hold marine polluters accountable. There have also been a number of cases in which remote sensing images were used as evidence in disputes concerning land boundaries²¹. Such cases usually arise when information in the real estate cadaster is missing or when existing records contain contradictions.

Some countries have explicitly recognized the use of satellite images as evidence in environmental litigation in national legislation. For example, Japan adopted the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data in 2016. The Act allows remote sensing data to be used in the public interest, including for environmental protection, disaster response, emergencies, and land use monitoring²². According to article 18(3) of the Act, such data may also be used in litigation or other court proceedings, in execution of judicial decisions, and in investigation of criminal cases.

Despite the adoption of this law, there is no evidence of the use of satellite imagery in environmental cases before Japanese courts. Remote sensing continues to be the main tool for environmental monitoring (for example, in detecting illegal dumping sites in hard-to-access areas²³, but such data are not yet applied in court proceedings. The main obstacles to the judicial use of satellite images include the

²⁰ Satellite images as primary evidence in UK court. (2012). URL: <https://emsa.europa.eu/csn-menu/csn-service/oil-spill-detection-examples/286-oil-spill-detection-examples/1873-oil-spill-detection-examples-maersk-kiera-february-2012.html>

²¹ Aerial photos as evidence in the case. (2025). URL: <https://ongeo-intelligence.com/blog/aerial-photos-as-evidence-in-the-case>

²² Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data. (2016). URL: <https://www.japaneselawtranslation.go.jp/en/laws/view/4344/en>

²³ KOSAKO, Akinori, MIYAZAKI, Sanae, INOUE, Ushio, TASAKI Tomohiro, OSAKO Masahiro, TAMURA

Masayuki. 2009), Detection of Illegal Dumping Sites by Using Vegetation Index and Land Surface Feature from High Resolution Satellite Images. *Journal of The Remote Sensing Society of Japan*, Volume 29, Issue 3, p.

497-514, URL: https://www.jstage.jst.go.jp/article/rssj/29/3/29_3_497/_article/-char/en

need to establish their reliability, the need for expert confirmation, etc.²⁴ The development of international standards for the use of satellite imagery in environmental litigation could help overcome these difficulties in practice.

Brazil also has legislation regulating the use of satellite imagery in judicial proceedings. In environmental cases, this type of evidence is governed by the Resolution 433/2021, adopted by the National Council of Justice²⁵. The adoption of such provisions enhances legal certainty and facilitates the work of the courts.

At the same time, there are examples when data obtained from remote sensing were not accepted by the court due to poor quality of images presented. One such case is the 2005 judgement of the Administrative Court in Minden, Germany. In this case, satellite images were submitted as evidence to determine the size of land plots, but the court dismissed them, considering them inaccurate because of defects in the satellite technology²⁶. This case demonstrates that courts will accept satellite imagery as evidence only if it is accurate and if its technical reliability can be verified.

As we can see, there is a growing tendency to use remote sensing data as evidence in environmental litigation in different states, and some states have begun to enshrine this possibility in national legislation. At the same time, such tendency requires proper legal regulation, for example, addressing private rights, potential unreliability of this type of evidence, and quality requirements for images used in court. In our view, the adoption of international standards in this area would be useful. Such standards would also help raise awareness among judges and law enforcement officials about the use of remote sensing evidence, because the lack of understanding of what remote sensing is and how it works is one of the reasons why judges do not accept remote sensing data as evidence.

Conclusion

The current international legal framework governing remote sensing of the Earth is outdated and insufficient. A large number of questions, such as protection of privacy, activities of private actors, exchange of information, liability for inaccurate data or

²⁴ KENNETH J. Markowitz. (2002). Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence. *Duke Environmental Law & Policy Forum*, Spring 2002. P. 219-264. URL: <https://scholarship.law.duke.edu/delpf/vol12/iss2/1> P. 220

²⁵ Brazilian National Council of Justice creates national environmental policy of the judiciary. (2022). URL:

<https://www.demarest.com.br/brazilian-national-council-of-justice-creates-national-environmental-policy-of-the-judiciary/>

²⁶ Space Generation Advisory Council. Marie-Claire Brujin. The use of Remote Sensing Data as Legal Evidence for Environmental Protection across Europe. (2024). URL: [https://spacegeneration.org/the-use-of-](https://spacegeneration.org/the-use-of-remote-sensing-data-as-legal-evidence-for-environmental-protection-across-europe)

[remote-sensing-data-as-legal-evidence-for-environmental-protection-across-europe](https://spacegeneration.org/the-use-of-remote-sensing-data-as-legal-evidence-for-environmental-protection-across-europe)

indirect harm, etc. is not regulated. Taking into account the widespread use of remote sensing results, ranging from environmental monitoring and disaster management to commercial and military uses, proper international legal regulation is required. Considering that the GA Resolution 41/65 is of a recommendatory nature and does not regulate a number of issues, it is necessary to adopt an international treaty on remote sensing of the Earth, which should define states' and private entities' responsibilities, establish standards for data dissemination, liability for damage caused during Earth sensing other than the fall of a satellite, etc.

Currently, remote sensing of the Earth is regulated by national law, and with regard to regulation at the international level, by soft law. It is necessary to adopt an international treaty which would comprehensively regulate the issue of remote sensing of the earth, in particular, it should contain provisions on the exchange of information, protection of the rights of individuals, liability for damage, liability for providing inaccurate information, etc. Adoption of international standards in the sphere of use of data obtained from remote sensing as evidence in court proceedings is also necessary. These standards should include such questions as requirements for the quality of images which can be used as evidence, preconditions for the use of remote sensing data as evidence, the issue of protection of the right to privacy, grounds for exclusion from the use of remote sensing data as evidence, etc.

The presence of internationally recognized standards in this area will contribute to the increased use of this type of evidence in environmental litigation, as currently the attitude of states towards the possibility of its use in court is not uniform. The use of processed satellite images as evidence in environmental disputes remains limited even in the vast majority of EU Member States although this type of evidence has significant potential to contribute to environmental protection and to help bring to justice those who violate environmental legislation.

Bibliography

1. JOEL, A. Dennerley, State Liability for Space Object Collisions: The Proper Interpretation of 'Fault' for the Purposes of International Space Law, *European Journal of International Law*, Volume 29, Issue 1, February 2018, Pages 281-301, <https://doi.org/10.1093/eil/chy003>
2. KEHRER, T. (2024). Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space. *Chicago Journal of International Law*, Vol. 20 (1). URL: <https://chicagounbound.uchicago.edu/cjil/vol20/iss1/5/>
3. KENNETH J. Markowitz. (2002). Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence. *Duke Environmental Law & Policy Forum*, Spring 2002. P. 219-264. URL: <https://scholarship.law.duke.edu/delpf/vol12/iss2/1> P. 220

4. KIM, Y.-J. (2024). Commercial Use of Satellite Remote Sensing Data and Civil Liability, *Laws*, 13 (77). URL: <https://www.mdpi.com/2075-471X/13/6/77>
5. KOSAKO, Akinori, MIYAZAKI, Sanae, INOUE, Ushio, TASAKI Tomohiro, OSAKO Masahiro, TAMURA Masayuki. 2009), Detection of Illegal Dumping Sites by Using Vegetation Index and Land Surface Feature from High Resolution Satellite Images. *Journal of The Remote Sensing Society of Japan*, Volume 29, Issue 3, p. 497-514, URL: https://www.jstage.jst.go.jp/article/rssj/29/3/29_3_497/_article/-char/en
6. LOTTERING, R., PEERBHAY, K., ADELABU, S. (2025). Remote Sensing Applications in Agricultural, Earth and Environmental Sciences. *Applied Sciences*, 15(8), 4537. <https://doi.org/10.3390/app15084537>
7. NOVAK, T., MELNYK, V., KOVALCHUK, I., PAKHOMOVA, A., NASTINA, O. (2024). Legal Support for Sustainable Agroecological Development: Evidence from Ukraine. *European Journal of Sustainable Development*, 13(2), 247. DOI: <https://doi.org/10.14207/ejsd.2024.v13n2p247>
8. RYZHENKO, I. (2018). State Participation in Space Activities: Some Legal Approaches and Implications, *Advanced Space Law*, Volume 2, p. 50 - 62.
9. VASHCHENKO, Y. (2021). Access to Modern Energy Services Through the Prism of Children's Rights: An Overview from the Perspectives of the Convention on the Rights of the Child and the Policy and Law Approaches of Certain EU Member States and Ukraine. *International Comparative Jurisprudence*, Volume 7, Issue 1, p. 75–87. DOI: <http://dx.doi.org/10.13165/j.icj.2021.06.006>
10. YEMELIANENKO, K., LADYCHENKO, V., YARYNKO, B. (2024). International legal and national mechanisms for overcoming the environmental consequences of the armed aggression of the Russian federation against Ukraine. *Law of Ukraine*, Vol. 10 (1), p. 151–165.
11. ZABARA, I. (2018). Remote sensing of the earth: past and present international legal regulation of obtaining and using information. *Information and law*, № 1 (24), P. 36- 43.
12. ZEMBLICKI, B., ORALOVA, Y. (2021). Private Entities in Outer Space Activities: Liability Regime Reconsidered. *Space Policy*, Volume 56. URL: <https://www.sciencedirect.com/science/article/pii/S0265964621000199>

Contact details

doc. Mgr. Liudmyla Golovko, PhD.

liudmyla.golovko@flaw.uniba.sk

Comenius University, Faculty of Law

Department of International Law and International Relations

VOJNOVÁ PROPAGANDA: JEJ ZÁKAZ V MEDZINÁRODNOM PRÁVE A JEHO IMPLEMENTÁCIA V SLOVENSKOM PRÁVNOM PORIADKU¹

WAR PROPAGANDA: ITS PROHIBITION UNDER INTERNATIONAL LAW AND ITS IMPLEMENTATION IN SLOVAK LEGAL ORDER

Lukáš Mareček²

Abstrakt: Príspevok analyzuje pozitívoprávny zákaz vojnovnej propagandy v medzinárodnom práve, jeho historické korene a aktuálny právny rámec. Začína prijatím Medzinárodného dohovoru o používaní vysielania v záujme mieru (1936), ktorého význam však oslabila druhá svetová vojna. Kľúčovým prameňom zákazu sa stal článok 20 ods. 1 Medzinárodného paktu o občianskych a politických právach (ICCPR) z roku 1966, ktorý ustanovuje absolútnu a nederogovateľnú povinnosť štátov zákonom zakázať akúkoľvek vojnovú propagandu.

Text rozoberá výklad uvedeného ustanovenia v súlade s princípmi medzinárodného práva vrátane výkladu podľa *travaux préparatoires*, všeobecných komentárov CCPR, doktríny, judikatúry medzinárodných a regionálnych súdov, ako aj jazykovej analýzy autentických znení. Konštatuje, že vojnová propaganda zahŕňa úmyselné šírenie nenávisťných či manipulatívnych posolstiev smerujúcich k vyvolaniu alebo podpore prebiehajúceho medzinárodného ozbrojeného konfliktu, pričom nie je nutné preukázať priamu kauzálnu súvislosť s konkrétnym dôsledkom.

Príspevok zdôrazňuje, že zákaz vojnovnej propagandy nie je len povinnosťou štátu prijať zákon, ale aj právom jednotlivca domáhať sa ochrany pred takýmito prejavmi. V kontexte Slovenskej republiky je zákaz vojnovnej propagandy implementovaný prostredníctvom trestného činu ohrozenia mieru podľa § 417 Trestného zákona. Tento výklad musí byť medzinárodno-konformný, v súlade so záväzkami SR podľa ICCPR.

¹ Podporené Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17Ro5-04-V01-00002 (CUSEC - Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality).

² Katedra medzinárodného práva a medzinárodných vzťahov, Právnická fakulta, Univerzita Komenského v Bratislave

Autor upozorňuje, že vojnová propaganda predstavuje spoločensky mimoriadne nebezpečné konanie, ktoré nemôže byť tolerované a vymyká sa ochrany slobody prejavu.

Kľúčové slová: vojnová propaganda; medzinárodné právo; informačná vojna; dezinformácie; trestný čin ohrozenia mieru

Abstract: The article analyzes the positive law prohibition of war propaganda in international law, its historical roots, and its current legal framework. It begins with the adoption of the International Convention Concerning the Use of Broadcasting in the Cause of Peace (1936), whose significance was diminished by the outbreak of the Second World War. The key source of the prohibition became Article 20(1) of the International Covenant on Civil and Political Rights (ICCPR) of 1966, which establishes an absolute and non-derogable obligation for states to prohibit any war propaganda by law.

The text examines the interpretation of this provision in accordance with the principles of international law, including *travaux préparatoires*, General Comments of the Human Rights Committee (CCPR), legal doctrine, jurisprudence of international and regional courts, and a linguistic analysis of the authentic language versions. It concludes that war propaganda includes the intentional dissemination of hateful or manipulative messages aimed at inciting or supporting an ongoing international armed conflict, and that it is not necessary to prove a direct causal link to a specific consequence.

The article emphasizes that the prohibition of war propaganda is not only a duty of the state to enact legislation, but also an individual right to seek protection against such expressions. In the context of the Slovak Republic, the prohibition is implemented through the criminal offense of endangering peace under § 417 of the Criminal Code. This interpretation must be internationally conforming, in line with Slovakia's obligations under the ICCPR.

The author stresses that war propaganda constitutes extremely dangerous conduct for society, cannot be tolerated, and falls outside the protection of freedom of expression.

Key words: war propaganda; international law; information warfare, disinformation; crime of threat to the peace

Úvod

Moderná vojny neprebíha len na fyzických bojiskách, ale línia konfliktov posúva do informačného priestoru. Podľa niektorých odhadov dnes fyzické nepriateľské akcie

predstavujú iba 10–20 % vojnových operácií, pričom zvyšných 80–90 % tvoria aktivity v oblasti informačnej vojny.³ Táto forma boja zahŕňa šírenie strategicky manipulovaných naratívov, ktoré majú za cieľ ovplyvniť verejnú mienku, polarizovať spoločnosť a podkopať demokratické inštitúcie.

Jedným z najvýraznejších príkladov tohto fenoménu je ruská invázia na Ukrajinu v roku 2022. V reakcii na ňu došlo k zákazu šírenia ruských médií ako RT či Sputnik. Vzniklo však nové, decentralizované a ťažšie regulovateľné pole pôsobnosti - diplomatické kanály na sociálnych sieťach. Štúdia Willaerta a Tutersa⁴ dokumentuje, ako ruské veľvyslanectvá a konzuláty využívali verejné online kanály na šírenie propagandistických naratívov s cieľom oslabiť podporu Západu pre Ukrajinu.

Informačná vojna je systematicky organizovaná a využíva široké spektrum taktík. Od šírenia dezinformácií a manipulácií až po tzv. malinformáciu, teda zámerné prekrúcanie pravdivých informácií. Tento typ informačného útoku cieľi predovšetkým na emočné a ideologické predsudky recipientov, čím posilňuje ich náchylnosť na polarizačné a toxické obsahy.⁵ Hoci je informačná vojna širším fenoménom, článok sa venuje právnej regulácii jedného z jej prejavov – propagácie vojny.

Jej zakázaná forma je zameraná na ovplyvňovanie verejnej mienky v prospech ozbrojeného konfliktu vedeného v rozpore s medzinárodným právom. Ide o nebezpečný fenomén, ktorý má potenciál viesť k porušovaniu ľudských práv, vrátane práva na život, k narúšaniu suverenity štátov a potenciálne aj k páchaniu vojnových zločinov.

Poznanie jej nebezpečnosti viedlo medzinárodné spoločenstvo k rozhodnutiu zakotviť explicitný zákaz šírenia vojenskej propagandy zakotvený v článku 20 ods. 1 Medzinárodného paktu o občianskych a politických právach (ICCPR), ktorý štátom ukladá povinnosť zákonom zakázať akúkoľvek vojenskú propagandu. Článok poukazuje na záväzok štátov prijať primerané opatrenia na obranu pred informačnými útokmi, ktorých cieľom je legitimizovať agresiu alebo manipulovať verejnosť v prospech vojenských konfliktov. Tento záväzok sa nestretol s aplikáciou na úrovni Výboru pre ľudské práva v konkrétnych veciach a vyvodzovanie

³ Thomas T (2016) The evolution of Russian military thought: integrating hybrid, new-generation, and new-type thinking. *J Slav Military Stud* 29:554–575. Cit podľa PADALKO, Halyna et al.: Investigation of machine learning approaches to classify war-related content during Russian full-scale invasion of Ukraine. In: *Social Network Analysis and Mining*. Vol. 15, No. 73 (2025), s. 1.

⁴ WILLAERT, Tom – TUTERS, Marc: From denazification to the Golden Billion: an inductive analysis of the Kremlin's weaponisation of digital diplomacy on Telegram. In: *Humanities & Social Sciences Communications*. Vol. 12, No. 989 (2025).

⁵ PADALKO, Halyna et al.: Investigation of machine learning approaches to classify war-related content during Russian full-scale invasion of Ukraine. In: *Social Network Analysis and Mining*. Vol. 15, No. 73 (2025).

zodpovednosti na národnej úrovni je minimálne sporadické, ak nie vôbec absentujúce. Dôvodom pre jeho zakotvenie bola pritom skúsenosť minulých generácií so svetovými vojnami, ktorým chceli predísť pre blaho tých budúcich.

Cieľom tohto príspevku je preskúmať interpretačné dimenzie zákazu vojenskej propagandy v medzinárodnom práve. Opiera sa o medzinárodnoprávne dokumenty, rozhodovaciú prax medzinárodných a regionálnych súdov, ako aj o relevantnú právnu doktrínu. V ostatnej časti sa príspevok zameriava na implementáciu tohto zákazu v právnom poriadku Slovenskej republiky, a to prostredníctvom skutkovej podstaty trestného činu ohrozenia mieru podľa § 417 Trestného zákona, ktorý musí byť vykladaný v súlade so záväzkami Slovenska vyplývajúcimi z medzinárodného práva.

Pramene zákazu vojnovej propagácie a jeho výkladu

Pozitívnoprávny zákaz vojnovej propagandy⁶ siaha k prijatiu **Medzinárodného dohovoru o používaní vysielania v záujme mieru** (International Convention Concerning the Use of Broadcasting in the Cause of Peace) z roku 1936, s platnosťou od roku 1938.

V zmysle tohto dohovoru sa Vysoké zmluvné strany zaviazali zabezpečiť, aby vysielanie zo staníc z ich území nepredstavovalo podnecovanie k vojne proti inej Vysokej zmluvnej strany, alebo k činom, ktoré k nej môžu pravdepodobne viesť. Zaviazali sa zakázať a v prípade potreby bez meškania zastaviť vysielanie, ktoré môže podnietiť obyvateľstvo k narušeniu vnútorného poriadku, bezpečnosti územia Vysokej zmluvnej strany. Taktiež aj výroky o ktorých osoby zodpovedné za vysielanie vedeli alebo mali vedieť, že sú nepravdivé, a ak boli takéto výroky odvysielané, aby sa vykonala náprava.

Československo ho podpísalo, avšak ratifikovalo až v roku 1985. Slovenská republika do zmluvy nesukcesovala. Celkovo je rozsah jeho Vysokých zmluvných strán nízky. Napriek jeho platnosti rozvinutiu jeho praktického významu zamedzilo najmä vypuknutie druhej svetovej vojny.

Valné zhromaždenie OSN však napriek tomu tento Dohovor v roku 1954 vyzdvihlo a považovalo za „významný prvok v oblasti slobody informácií“⁷ a požiadalo Generálneho tajomníka OSN o vypracovanie návrhu protokolu, ktorý by, okrem iného, aktualizoval protokol, aby zodpovedal novým reáliám doby. Od zámeru prijatia tohto protokolu bolo upustené.⁸

Štáty sa rozhodli namiesto toho zákaz vojnovej propagandy zakotviť v Medzinárodnom pakte o občianskych a politických právach z roku 1966 (ICCPR), čo

⁶ V príspevku používame termíny vojnová propaganda a vojnová propagácia synonymicky.

⁷ A/RES/841 (IX), 17 December 1954.

⁸ KAERNEY, Michael G.: *The Prohibition of Propaganda for War in International Law*. Oxford: Oxford University Press, 2007, pp. 28–33.

môžeme považovať za **najvýznamnejší zmluvný prameň** zákazu vojnovnej propagandy na univerzálnej úrovni. Jeho významným prvkom, oproti zmienenému dohovoru je aj prítomnosť inštitucionálnej a procesnej roviny, ktorá môže byť využitá.

Okrem ICCPR je možné zákaz nachádzať aj na regionálnej úrovni, konkrétne v čl. 13 Amerického dohovoru o ľudských právach.⁹

Vedie sa aj diskusia o tom, či je zákaz vojnovnej propagandy súčasťou **medzinárodného obyčajového práva**. *Opinio juris* je možné podložiť či už prijatím predmetných dohovorov, ako aj s poukazom napr. na Deklaráciu zásad priateľských vzťahov z roku 1970,¹⁰ kde je v kontexte elaborácie zásady zákazu použitia sily, alebo hrozby použitím sily, uvedená aj povinnosť štátov zdržať sa propagácie agresívnej vojny. Táto povinnosť bola potvrdená v roku 1975 aj v Záverečnom akte Helsinskej konferencie.¹¹ Podobne vojnovú propagáciu odsúdili aj rezolúcie VZ OSN z rokov 1947 a 1950.¹² Problémom pre vyslovenie záveru o sformovaní obyčajovej povahy tohto zákazu môže byť nachádzanie dostatočnej praxe, ktorá by *opinio juris* sprevádzala, či už na medzinárodnej alebo národnej úrovni. Samotné *opinio juris* môže byť spochybnené prítomnosťou výhrad¹³ k čl. 20 ods. 1 ICCPR. Možno tak

⁹ „Any propaganda to war... shall be considered as offenses punishable by law.“ Čl. 13 ods. 5 Americký dohovor o ľudských právach z roku 1969.

¹⁰ „In accordance with the purposes and principles of the United Nations, States have the duty to refrain from propaganda for wars of aggression.“ A/RES/2625(XXV), 24 October 1970.

¹¹ To promote, by all means which each of them considers appropriate, a climate of confidence and respect among peoples consonant with their duty to refrain from propaganda for wars of aggression or for any threat or use of force inconsistent with the purposes of the United Nations and with the Declaration on Principles Guiding Relations between Participating States, against another participating State. Helsinki Final Act (1975).

¹² „Condemns all forms of propaganda, in whatsoever country conducted, which is either designed or likely to provoke or encourage any threat to the peace, breach of the peace, or act of aggression“ A/RES/110 (II), 3 November 1947, potvrdené následne A/RES/381(V), 17 November 1950.

¹³ **Denmark:** „Reservation is further made to Article 20, paragraph 1. This reservation is in accordance with the vote cast by Denmark in the XVI General Assembly of the United Nations in 1961 when the Danish Delegation, referring to the preceding article concerning freedom of expression, voted against the prohibition against propaganda for war“ ; Hungary „Reservation: Article 20, paragraph 1, with reference to the fact that a prohibition against propaganda for war could limit the freedom of expression.“ Sweden „Sweden reserves the right not to apply ... the provisions of article 20, paragraph 1, of the Covenant.“ ; **Switzerland:** Switzerland reserves the right not to adopt further measures to ban propaganda for war, which is prohibited by article 20, paragraph 1.; **United States of America:** „That article 20 does not authorize or require legislation or other action by the United States that would restrict the right of free speech and association protected by the Constitution and laws of the United States.“ ; **Iceland:** Reservation: Article 20, paragraph 1, with reference to the fact that a prohibition against propaganda for war could limit the freedom of expression. **Belgium:** The Belgian Government declares that it does not consider itself obligated to enact legislation in the field covered by article 20,

identifikovať rozličné názory doktríny v tejto otázke.¹⁴ Ostáva, že prameňom tohto zákazu je predovšetkým medzinárodná zmluva, najmä ICCPR.

Pri výklade tohto ustanovenia ICCPR nie je možné sa oprieť o rozhodovaciu činnosť Výboru pre ľudské práva (CCPR) zriadeného na dohliadanie nad dodržiavaním ICCPR – **rozhodovacia činnosť CCPR v individuálnych veciach vo vzťahu k čl. 20 ods. 1 ICCPR absentuje.**

Pri jeho výklade je tak možné oprieť sa o:

- 1) Prípravné materiály (*travaux préparatoires*).
- 2) Všeobecné komentáre (*general comments*) CCPR.

paragraph 1, and that article 20 as a whole shall be applied taking into account the rights to freedom of thought and religion, freedom of opinion and freedom of assembly and association proclaimed in articles 18, 19 and 20 of the Universal Declaration of Human Rights and reaffirmed in articles 18, 19, 21 and 22 of the Covenant.; **Finland:** With respect to article 20, paragraph 1, of the Covenant, Finland declares that it will not apply the provisions of this paragraph, this being compatible with the standpoint Finland already expressed at the 16th United Nations General Assembly by voting against the prohibition of propaganda for war, on the grounds that this might endanger the freedom of expression referred in article 19 of the Covenant."; Iceland „5. Article 20, paragraph 1, with reference to the fact that a prohibition against propaganda for war could limit the freedom of expression. This reservation is consistent with the position of Iceland at the General Assembly at its 16th session. Other provisions of the Covenant shall be inviolably observed."; **Luxemburg:** „(d) The Government of Luxembourg declares that it does not consider itself obligated to adopt legislation in the field covered by article 20, paragraph 1, and that article 20 as a whole will be implemented taking into account the rights to freedom of thought, religion, opinion, assembly and association laid down in articles 18, 19 and 20 of the Universal Declaration of Human Rights and reaffirmed in articles 18, 19, 21 and 22 of the Covenant."" **Netherlands:** „Article 20, paragraph 1 "The Kingdom of the Netherlands does not accept the obligation set out in this provision in the case of the Netherlands.""; **New Zealand:** „The Government of New Zealand having legislated in the areas of the advocacy of national and racial hatred and the exciting of hostility or ill will against any group of persons, and having regard to the right of freedom of speech, reserves the right not to introduce further legislation with regard to article 20." ; **Norway:** „Subject to reservations to article 10, paragraph 2 (b) and paragraph 3 "with regard to the obligation to keep accused juvenile persons and juvenile offenders segregated from adults" and to article 14, paragraphs 5 and 7 and to article 20, paragraph 1." ; **Sweden:** „Sweden reserves the right not to apply the provisions of article 10, paragraph 3, with regard to the obligation to segregate juvenile offenders from adults, the provisions of article 14, paragraph 7, and the provisions of article 20, paragraph 1, of the Covenant." ; Swiss „(f) Reservation concerning article 20; **United Kingdom:** „The Government of the United Kingdom interpret article 20 consistently with the rights conferred by articles 19 and 21 of the Covenant and having legislated in matters of practical concern in the interests of public order (ordre public) reserve the right not to introduce any further legislation. The United Kingdom also reserve a similar right in regard to each of its dependent territories."

¹⁴ K diskusii napr. ASWAD, Evelyn: Propaganda for War & International Human Rights Standards In: *Chicago Journal of International Law*. Vol. 24 No. 1 (2023). Online: <https://cjl.uchicago.edu/sites/default/files/2023-07/24ChiJIntlL1.pdf>. KEARNEY, Michael: The Prohibition of Propaganda for War in the International Covenant on Civil and Political Rights In: *Netherlands Quarterly of Human Rights*. Vol. 23, No. 4 (2005). Online: <https://journals.sagepub.com/doi/abs/10.1177/016934410502300402?utm>.

- 3) Doktrínu.
- 4) Rozhodnutia orgánov, najmä:
 - a) Valné zhromaždenie OSN.
 - b) Súdny dvor EÚ.
 - c) Orgány medzinárodnej trestnej spravodlivosti:
 - i) Medzinárodný vojenský tribunál v Norimbergu (IMT).
 - ii) Medzinárodný trestný tribunál pre Rwandu (ICTR).
- 5) Analógiu s judikatúrou vo veciach nenávistných prejavov a limitmov slobody prejavu.
- 6) Implementáciu v národnej legislatíve.

Tieto sa priebežne využívané aj pri spracovaní tohto článku.

Na základe komparatívnej jazykovej analýzy je možné konštatovať, že autentické jazykové verzie (čínska, anglická, francúzska, ruská a španielska, čl. 53 ICCPR) sú v zhode a nevykazujú podstatné odchýlky. V jednotlivých jazykových verziách je možné identifikovať určité dôrazy, ktoré ale nemenia obsah článku. V objekte je v ruskej jazykovej verzii opísaný neutrálne „propaganda vojny“ a v iných zdôraznená aktivnosť podporovania v zmysle „propaganda v prospech vojny“. Pri modalite iný dôraz možno badať pri francúzskom imperatíve „je zakázaná“ oproti „má byť zakázaná“ v ostatných jazykových verziách. Napokon pri inštrumente čínska jazyková verzia dodáva „prostriedkami práva/zákona“ zatiaľ čo ostatné bez pridania tohto podstatného mena.

	Čínština ¹⁵	Angličtina	Francúzština	Ruština	Španielčina
Objekt	任何鼓吹战争的 宣传 any propaganda that advocates war.	Any propaganda for war	Toute propagande en faveur de la guerre	Всякая пропаганда войны	Toda propaganda en favor de la guerra
Modalita	应禁止 should/shall be prohibited	shall be prohibited	est interdite	должна быть запрещена	estará prohibida
Inštrument	以法律禁止之 prohibited by means of law.	by law	par la loi	законом	por la ley

Tabuľka 1 – Porovnanie autentických jazykových verzií čl. 20 ods. 1 ICCPR. Zdroj: autor.

¹⁵ Pri rozbere boli využité nástroje umelej inteligencie.

Slovenská jazyková verzia „Akákoľvek vojnová propagácia je zakázaná zákonom“¹⁶ je v obsahovej zhode s autentickými jazykovými verziami. Pri objekte sa prikláňa k ruskej jazykovej verzii, pri modalite k francúzskej a pri modalite k väčšine autentických jazykových verzií. Možno konštatovať, že oficiálny preklad do slovenského jazyka je korektný.

Akákoľvek vojnová propagácia...

Podľa CCPR sa zákaz vojnovnej propagácie sa vzťahuje „na **všetky formy** propagandy ohrozujúcej alebo spôsobujúcej akt agresie alebo porušenie mieru v rozpore s chartou OSN.“¹⁷

Definícia vojnovnej propagácie v medzinárodnom práve absentuje. Čl. 30 ods. 1 a 2 Viedenského dohovoru o zmluvnom práve z roku 1969 stanovujú, že medzinárodná zmluva sa musí vykladať dobromyseľne, v súlade s obvyklým významom, ktorý sa dáva výrazom v zmluve v ich celkovej súvislosti, a takisto s prihliadnutím na predmet a účel zmluvy. Celkovou súvislosťou sa rozumie aj každá listina vyhotovená jednou alebo viacerými stranami v súvislosti s uzavretím zmluvy a prijatá ostatnými stranami ako listina vzťahujúca sa na zmluvu (*travaux préparatoires*).¹⁸ Z historického pohľadu, ako aj z *travaux préparatoires* k čl. 20 ICCPR, vyplýva, že **materiálnym prameňom zakotvenia zákazu vojnovnej propagácie bola skúsenosť fašistickej a nacistickej propagácie vojny z 30. a 40. rokov minulého storočia.**¹⁹

Z prípravných materiálov na ICCPR vyplýva, že propagandou sa rozumie „podnecovanie vojny“, ako aj „opakované a vytrvalé vyjadrovanie názoru“ s cieľom vytvoriť „atmosféru nenávisťi a neporozumenia medzi obyvateľmi dvoch alebo viacerých krajín, aby ich to nakoniec priviedlo k ozbrojenému konfliktu“.²⁰ Podľa doktríny môže ísť o „úmyselné, cielené ovplyvňovanie jednotlivcov využívaním rôznych komunikačných kanálov na šírenie predovšetkým nesprávnych alebo prehnaných tvrdení o skutočnostiach“ vrátane „negatívnych alebo zjednodušených

¹⁶ Vyhláška MZV č. 120/1976 Zb.

¹⁷ „The prohibition under paragraph 1 extends to all forms of propaganda threatening or resulting in an act of aggression or breach of the peace contrary to the Charter of the United Nations.“ CCPR: General comment no. 11.

¹⁸ NOWAK, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd rev. ed. Kehl am Rhein: N.P. Engel, 2005, s. 472.

¹⁹ „The Special Rapporteur notes that article 20 of the Covenant was drafted against the historical background of the horrors committed by the Nazi regime during the Second World War“ Ods. 47, Report of the Special Rapporteur on freedom of religion or belief, Asma Jahangir, and the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Doudou Diène, further to Human Rights Council decision 1/107 on incitement to racial and religious hatred and the promotion of tolerance, A/HRC/2/3, 20 September 2006.

²⁰ FINA, Audrey: A critique of the UN Strategy and Guidance on 'Hate Speech': Some Legal Considerations. In: *Netherlands Quarterly of Human Rights*, Vol 41, No. 4 (2023). s. 207.

hodnotových úsudkov“, ktoré sú porovnateľné s „provokáciou, podnecovaním alebo nabádaním“. ²¹

S ohľadom na zásadu dobromyseľného výkladu zmluvného dojednaní v jeho celkovej súvislosti tiež vplýva, že zákazom vojnovej propagácie štáty nemali v úmysle zakázať akademickú diskusiu o bezpečnostných otázkach alebo propagáciu použitia sily v súlade s Chartou OSN. ²² Ale mali v úmysle zakázať vojnovú propagáciu, ktorá je porovnateľná s fašistickou a nacistickou propagáciou útočnej vojny, ktorá nemá oporu v medzinárodnom práve. Z prípravných materiálov vyplýva, že štáty nemali formuláciou zákazu vojnovej propagandy v úmysle pokryť aj propagáciu vnútroštátneho ozbrojeného konfliktu, ²³ ale ide o len **zákaz propagácie medzinárodného ozbrojeného konfliktu**. ²⁴ Ten je v súčasnom medzinárodnom práve definovaný ako faktický stav ozbrojeného konfliktu medzi štátmi, bez ohľadu na to či došlo k formálnemu vyhláseniu vojny. ²⁵ Avšak je nutné podotknúť, že prípravné materiály sú len jedným z interpretačných prostriedkov a za jazykového znenia (akákoľvek) môže vyplývať aj širší výklad. ²⁶

Propagácia vojny fašistami a nacistami, podľa právneho názoru Medzinárodného vojenského tribunálu v Norimbergu, neustala začiatkom vojny, ale bola esenciálna aj pre jej pokračovanie. ²⁷

²¹ NOWAK, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd rev. ed. Kehl am Rhein: N.P. Engel, 2005, ods. 628. Cit. podľa FINA, Audrey: A critique of the UN Strategy and Guidance on 'Hate Speech': Some Legal Considerations. In: *Netherlands Quarterly of Human Rights*, Vol 41, No. 4 (2023). s. 207.

²² „The provisions of article 20, paragraph 1, do not prohibit advocacy of the sovereign right of self defence or the right of peoples to self determination and independence in accordance with the Charter of the United Nations.“ CCPR: General comment no. 11.

²³ Aj kebyže nešlo o vojnovú propagáciu v zmysle čl. 20 ods. 1 ICCPR, **propagácia narušenia územnej celistvosti z vnútra taktiež prekračuje limity slobody prejavu** – viď prípady ECHR Sürek (no. 1) proti Turecku, Özgür Gündem proti Turecku a Medya FM Reha Radyo ve İletişim Hizmetleri A. Ş. proti Turecku.

²⁴ NOWAK, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd rev. ed. Kehl am Rhein: N.P. Engel, 2005, s. 473. JOSEPH, Sarah – CASTAN, Melissa: *The International Covenant on Civil and Political Rights*. Oxford: Oxford University Press, 2013, s. 628. FINA, Audrey: A critique of the UN Strategy and Guidance on 'Hate Speech': Some Legal Considerations. In: *Netherlands Quarterly of Human Rights*, Vol 41, No. 4. s. 208. Slovenské trestné právo sa však môže vykladať aj širšie, ako zahrňujúce aj nemedzinárodné ozbrojené konflikty. STRÉMY, Tomáš a kol.: *Trestný zákon: komentár*, 2016.

²⁵ SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, s. 379-380.

²⁶ FINA, Audrey: A critique of the UN Strategy and Guidance on 'Hate Speech': Some Legal Considerations. In: *Netherlands Quarterly of Human Rights*, Vol 41, No. 4. s. 208.

²⁷ ...For the correct definition of the role of defendant Hans Fritzsche it is necessary, firstly, to keep clearly in mind the importance attached by Hitler and his closest associates (as Göring, for example)

Z výkladu tohto dojednania nemožno usúdiť, že by sa začatím vojny menila „trestuhodnosť“ vojnovnej propagácie. Vojnová propagácia je spoločensky rovnako nebezpečným konaním, ak smeruje k začatiu vojny, ako aj v prípade, ak podporuje jej pokračovanie alebo zintenzívnenie.²⁸ Uvádzaný výklad čl. 20 ods. 1 Medzinárodného paktu vyplýva aj z recentnej judikatúry Súdneho dvora EÚ vo vzťahu k agresii Ruskej federácie voči Ukrajine: „209. Článok 20 ods. 1 uvedeného paktu pritom stanovuje, že „akákoľvek vojnová propagácia je zakázaná zákonom“. V tejto súvislosti treba poznamenať, že skutočnosť, že zákaz „vojnovnej propagácie“ je zakotvený v inom odseku ako zákaz akejkoľvek „národn[ej], rasov[ej] alebo nábožensk[ej] nenávis[ti], ktorá predstavuje podnecovanie k diskriminácii, nepriateľstvu alebo násiliu“, ktorý je zakotvený v odseku 2 toho istého článku, sa má vykladať v tom zmysle, že jeho cieľom je priznať „vojnovnej propagácii“ absolútnu závažnosť. V prejednávanej veci treba na jednej strane uviesť, že žalobkyňa vykonávala propagandistickú činnosť v rámci prebiehajúcej vojny vyvolanej aktom štátu, ktorý medzinárodné spoločenstvo označuje za „agresiu“ ... v rozpore so zákazom použitia sily stanoveným v článku 2 ods. 4 Charty Organizácie Spojených národov. V tejto súvislosti treba pripomenúť, že rezolúciou 110 (II), ktorá bola potvrdená rezolúciou 381 (V), Valné zhromaždenie Organizácie Spojených národov odsúdilo „akúkoľvek propagandu vedenú v ktorejkoľvek krajine, ktorá má za cieľ alebo môže vyvolať či podnietiť akúkoľvek hrozbu pre mier, porušenie mieru alebo akt agresie“. Na druhej strane treba uviesť, že rozsah zákazu stanoveného v článku 20 ods. 1 uvedeného paktu, ktorý sa týka „akejkoľvek“ vojnovnej propagandy, zahŕňa nielen podnecovanie k budúcej vojne, ale aj sústavné, opakované a koordinované vyhlásenia na podporu prebiehajúcej vojny, ktorá je v rozpore s medzinárodným právom, najmä ak takéto vyhlásenia pochádzajú od média priamo alebo nepriamo kontrolovaného agresorským štátom.“²⁹

Citovaný rozsudok Súdneho dvora EÚ bol vydaný v súvislosti s uplatňovaním reštriktívnych opatrení. Ich zavedenie je odôvodnené tým, že „keďže propaganda a

to propaganda in general and to radio propaganda in particular. This was considered one of the most important and essential factors in the success of conducting an aggressive war. In the Germany of Hitler, propaganda was invariably a factor in preparing **and** conducting acts of aggression...” International Military Tribunal (Nuremberg), Judgment, p. 538.

²⁸ Valné zhromaždenie OSN: „1. Condemns all forms of propaganda, in whatsoever country conducted, which is either designed or likely to provoke **or encourage** an threat to the peace, breach of the peace, or act of aggression.“ A/RES/110 (II), 3 November 1947.

²⁹ Ods. 209-210. CJEU: Judgment of the General Court (Grand Chamber) of 27 July 2022. RT France v Council of the European Union. Case T-125/22. „Article 20(1) of that covenant, which refers to ‘any’ propaganda for war, includes not only incitement to a future war, but also continuous, repeated and concerted statements in support of an ongoing war, contrary to international law, especially where those statements come from a media outlet under the direct or indirect control of the aggressor State.“

dezinformačné kampane môžu [sú spôsobilé, are capable] narušiť základy demokratických spoločností a sú neoddeliteľnou súčasťou nástrojov vedenia modernej vojny, predmetné reštriktívne opatrenia patria tiež do rámca plnenia cieľov, ktoré Únii stanovuje článok 3 ods. 1 a 5 ZEÚ.³⁰

A contrario, šíriteľ propagandy, ktorý nemôže – nie je spôsobilý – narušiť základy demokratických spoločností, by nemal byť postihovaný reštriktívnymi opatreniami. Tento záver je v súlade aj s vyššie uvedeným materiálnym prameňom čl. 20 ods. 1 ICCPR. Zákazom vojnovej propagandy by sa tak nemali postihovať výroky, ktoré sú nižšej spoločenskej závažnosti. Napríklad vyjadrené v súkromí, bez širšieho spoločenského dopadu, respektíve bez spôsobilosti narušiť základy demokratických spoločností.

Vyhodnocovanie, či predmetný výrok alebo iná šírená informácia je „nástrojom vedenia modernej vojny“ alebo len „bežné šírenie dezinformácií v občianskej spoločnosti“ najmä, ak konanie nie je spojené s príslušným úmyslom, môže slúžiť ako nástroj pre odlišenie prejavov, ktoré musí štát zakázať a potláčať v zmysle čl. 20 ods. 1 ICCPR. Úmysel vyplýva nepriamo aj z názoru Súdneho dvora EÚ, ktorý vojnovú propagandu vníma ako nástroj vedenia modernej vojny. Zodpovednosť za používanie nástrojov vojny (per analogiam s konvenčnými nástrojmi vojny) nastáva v prípade ich úmyselného používania s rozpore s pravidlami vojny, alebo pri zanedbaní potrebnej opatrnosti, nie v prípade náhodného či nepredvídaného následku. V prípade neprítomnosti úmyslu by nešlo o pôvodcu propagandy, ale daná osoba by bola pravdepodobne sama obeťou propagandy, ktorú šíri ďalej. Štát má povinnosť zamedziť šíreniu propagandy, nech ju šíri ktorákoľvek osoba (či už pôvodca alebo niekto iný) a vo vzťahu k pôvodcovi by mali prísť v úvahu aj represívne opatrenia.

ICTR uviedol: „Moc médií vytvárať a ničiť základné ľudské hodnoty so sebou prináša veľkú zodpovednosť. Tí, ktorí takéto médiá kontrolujú, sú zodpovední za jej dôsledky.“³¹ Podobne aj VZ OSN v roku 1946 uviedlo, že právo na informácie „si vyžaduje ako nevyhnutný prvok ochotu a schopnosť využívať svoje privilégia **bez zneužívania**. Vyžaduje si ako základnú disciplínu morálnu povinnosť vnímať fakty bez predsudkov a šíriť vedomosti **bez zlého úmyslu**.“³² Šírenie vojnovej propagandy je zneužívaním práva so zlým úmyslom, ktoré nemôže (nesmie) byť tolerované. A tak, vojnovou propagandou nebude šírenie hoci nepravdivé informácie, avšak v omyle, resp. bez prináležiaceho zlého úmyslu.

³⁰ Ods. 53. 1. CJEU: Judgment of the General Court (First Chamber, Extended Composition) of 26 March 2025. A2B Connect BV and Others v Council of the European Union. Case T-307/22.

³¹ Ods. 945, ICTR: Prosecutor v. Nahimana et al. (Media case). Case No. ICTR-99-52-T, Trial Judgement 03 Dec 2003.

³² „requires as an indispensable element the willingness and capacity to employ its privileges without abuse. It requires as a basic discipline the moral obligation to see the facts without prejudice and to spread knowledge without malicious intent,“ A/RES/59(I), 14 December 1946.

Opierajúc sa o judikatúru vo veciach nacistickej propagandy (nie výlučne len vojrovej) „...rozsudok [IMT] výslovne neuvádza priamu kauzálnu súvislosť medzi Streicherovým³³ publikovaním a akýmikoľvek konkrétnymi činmi vraždy. Skôr charakterizuje jeho prácu ako jed „vstreknutý do mysli tisícov Nemcov, ktorý ich prinútil nasledovať politiku prenasledovania a vyhladzovania Židov národných socialistov“³⁴ Naproti tomu v prípade Fritzsche³⁵ „Tribunál zistil, že hoci niekedy šíril nepravdivé správy, nebolo preukázané, že vedel, že sú nepravdivé“³⁶, a napokon bol oslobodený.

Z uvedeného vyplýva, že aj v kontexte čl. 20 ods. 1 ICCPR by malo mať rozhodujúci význam vedomé a úmyselné šírenie nepravdivých či manipulatívnych tvrdení v prospech vojny, nie preukázanie kauzality so škodlivým následkom. **Nie je rozhodujúce preukázanie príčinnej spôsobilosti medzi propagáciou vojny a konkrétnym následkom.** Má sa tak považovať za ohrozovací delikt.

Napriek formulácii, ktorá môže evokovať, že nejde o formulovanie ľudského práva, ale záväzku štátu prijať príslušný zákonný zákaz, je možné oprieť sa analogicky na výklad CCPR vo veci nadväzujúceho odseku dva čl. 20 ICCPR, v ktorom potvrdil, že nejde „len“ o záväzok štátu, ale o individuálne právo jednotlivca, ktorého sa môže pred CCPR domáhať voči štátu. Ako sme uviedli vyššie, pre naplnenie znakov vojrovej propagandy nie je nevyhnutné preukázať príčinnú súvislosť s konkrétnym škodlivým následkom.

Ak čl. 20 ICCPR má zložiť nielen povinnosť štátu, ale aj individuálne právo na ochranu pred propagovaním vojny, tak je dôležité, aby bol určený prah ujmy potrebnej na aktívnu legitimáciu jednotlivca pred CCPR, ktorú musí sťažovateľ preukázať. Touto ujmou, opäť analogicky s čl. 20 ods. 2 ICCPR, nemusia byť len konkrétne incidenty motivované nenávisťou, ale postačuje aj pocit ohrozenia či všeobecný pocit úzkosti. Teda **postačuje, že takéto výroky vyvolajú ohrozenie a úzkosť v psychike obetí.**³⁷ Teda v prípade vojrovej propagandy by postačovalo, že ide o výroky, ktoré sú spôsobilé vyvolať v obetiach dôvod pre pocit úzkosti, resp. o zachovanie mieru, resp. pocit ohrozenia pre obavy o zachovanie mieru.

... je zakázaná ...

³³ Julius Sebastian Streicher (1885-1946), vydavateľ novin *Der Stürmer*.

³⁴ Ods. 981, ICTR: Prosecutor v. Nahimana et al. (Media case). Case No. ICTR-99-52-T, Trial Judgement 03 Dec 2003.

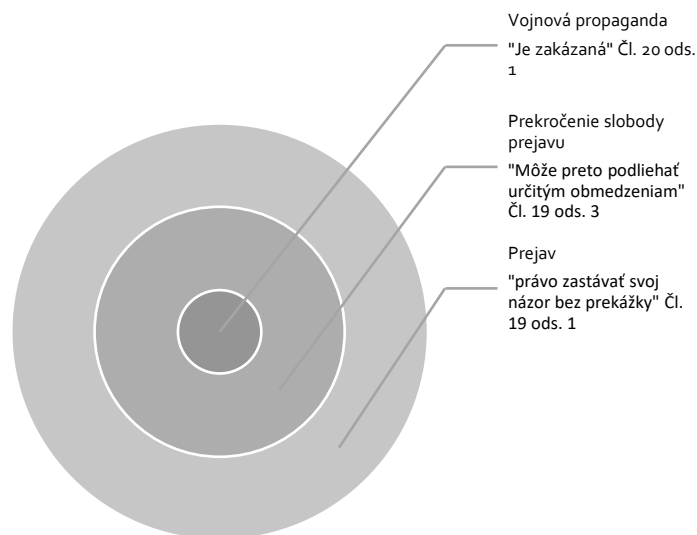
³⁵ August Franz Anton Hans Fritzsche (1900-1953).

³⁶ Ods. 982, ICTR: Prosecutor v. Nahimana et al. (Media case). Case No. ICTR-99-52-T, Trial Judgement 03 Dec 2003.

³⁷ TEMPERMAN, Jeroen: The International Covenant on Civil and Political Rights and the “Right to be Protected against Incitement”. In: *Journal of Law, Religion and State*. No. 7 (2019). s. 100 a nasl.

Ak výrok nespadá do rámca čl. 20 (ods. 1 alebo 2), neznamená to, že ide o výrok, ktorý môže byť šírený. Ak nejde o výrok naplňajúci kvalifikačné kritériá vojnovej propagácie, tak v takom prípade by sa zásah štátu proti takémuto výroku (resp. jeho pozitívny záväzok) posudzoval prizmou zásad aplikovateľných (najmä zásady proporcionality) na čl. 19 ICCPR a nie prizmou imperatívneho zákazu v zmysle čl. 20 ICCPR. Výklad čl. 19 nie je súčasťou tohto príspevku. Možno ale konštatovať, že to čo je chránené slobodou prejavu v zmysle čl. 19, nebude môcť byť vyhodnotené ako vojnová propaganda (argumentum a minori ad maiorem).

Z komentára CCPR vyplýva, že tieto zákazy sú plne kompatibilné so slobodou prejavu tak, ako sú obsiahnuté v čl. 19, ktoré so sebou nesú osobitné povinnosti a zodpovednosť.³⁸ Teda ak dôjde ku konštatovaniu, že výrok naplnil intenzitu vojnovej propagácie, možno automaticky usudzovať kompatibilitu jeho zákazu s čl. 19 ICCPR.



Obrázok 1, zdroj: autor

Zároveň je povinnosť zákazu vojnovej propagácie vyložená CCPR ako nederogovateľná, čím sa zákaz vojnovej propagácie posúva do kategórie absolútnych práv definovaných v čl. 4 ICCPR,³⁹ kam patrí napríklad zákaz mučenia či

³⁸ „In the opinion of the Committee, these required prohibitions are fully compatible with the right of freedom of expression as contained in article 19, the exercise of which carries with it special duties and responsibilities“ CCPR: General comment no. 11.

³⁹ „No declaration of a state of emergency made pursuant to article 4, paragraph 1, may be invoked as justification for a State party to engage itself, contrary to article 20, in propaganda for war, or in advocacy of national, racial or religious hatred that would constitute incitement to discrimination, hostility or violence.“ General Comment no. 29.

zákaz otroctva. Možno tak vojnovú propagáciu definovať ako **absolútny zákaz**, resp. ako nederogovateľnú povinnosť štátu potláčať vojnovú propagandu, v čom sa táto kategória odlišuje napríklad od výrokov podliehajúcich čl. 19 ICCPR.

V inom komentári sa potvrdzuje, že „štáty musia rešpektovať slobodu prejavu, vrátane právo vyhľadávať, prijímať a šíriť informácie a myšlienky všetkého druhu bez ohľadu na hranice. Toto právo zahŕňa vyjadrovanie a prijímanie oznámení každej formy myšlienok a názorov, ktoré je možné preniesť na iných, s výhradou ustanovení článku 19 odseku 3 a článku 20. Zahŕňa politickú diskusiu, komentáre k vlastným a k verejným záležitostiam, kampaň, diskusiu o ľudských právach, žurnalistiku, kultúrne a umelecké prejavy, vyučovanie a náboženské diskusie. Môže zahŕňať aj komerčnú reklamu. Rozsah pôsobnosti odseku 2 zahŕňa aj prejavy, ktoré možno považovať za hlboko urážlivé, hoci takéto prejavy môžu byť obmedzené v súlade s ustanoveniami článku 19 odseku 3 a článku 20“.⁴⁰

„Pakt nepovoľuje všeobecný zákaz vyjadrovania chybného názoru alebo nesprávnej interpretácie minulých udalostí. **Obmedzenia** práva na slobodu presvedčenia by sa nikdy nemali ukladať a pokiaľ ide o slobodu prejavu, nemali **by presahovať rámec toho, čo je povolené** v odseku 3 alebo **požadované** podľa článku 20.“⁴¹ Články 19 a 20 sú navzájom kompatibilné a dopĺňajú sa. **Činy, ktoré sú predmetom článku 20, podliehajú obmedzeniu podľa článku 19 odseku 3. Obmedzenie, ktoré je odôvodnené na základe článku 20, preto musí byť v súlade aj s článkom 19 odsekom 3.** Činy, ktoré sú predmetom článku 20, odlišuje od iných činov, ktoré môžu podliehať obmedzeniu podľa článku 19 odseku 3, to, že pre činy, ktoré sú predmetom článku 20, pakt uvádza konkrétnu reakciu požadovanú od štátu: ich zákaz zákonom. Len v tomto rozsahu možno článok 20 považovať za lex specialis vo vzťahu k článku 19. Len vo vzťahu ku konkrétnym formám prejavu uvedeným v článku 20 sú zmluvné štáty povinné mať zákonné zákazy. V každom prípade, v ktorom štát obmedzuje slobodu prejavu, je potrebné odôvodniť zákazy a ich ustanovenia v prísnom súlade s článkom 19.“⁴²

V istom zmysle možno povedať, že zatiaľ čo pri čl. 19 otázka znie, či štát môže do slobody prejavu zasiahnuť a či jeho prípadný zásah bol oprávnený, pri vojrovej propagande by mala byť otázka kladená opačne a východiskom je povinnosť štátu prijať opatrenia na jej zákaz a ak by sa tak nestalo vysvetliť prečo takýto prejav toleroval.

⁴⁰ General Comment no. 34.

⁴¹ Porovnaj aj „By virtue of Article 20 of the ICCPR, certain speech not only may but in fact must be restricted.“ Ods. 985, ICTR: Prosecutor v. Nahimana et al. (Media case). Case No. ICTR-99-52-T, Trial Judgement

03 Dec 2003.

⁴² General Comment no. 34.

Definovanie zakázaného konania v ľudskoprávnom dokumente, dokonca jeho povýšenie na absolútny zákaz, môže pôsobiť kontraintuitívne. Avšak ide o technicky jednoduchšie vyjadrenie ľudskoprávnej normy, ktorá zakazuje konanie, ktorého môže spôsobiť následok spočívajúci v rozsiahlom ľudskom utrpení spôsobenom vedením vojny, ktorého obvyklou súčasťou je porušovanie ľudských práv, najmä práva na život. Zákaz vojnovnej propagandy sa preto objavuje aj vo všeobecnom komentári CCPR dedikovanom výkladu práva na život.⁴³ Pozitívnym vyjadrením zákazu vojnovnej propagandy, by tak bolo jeho začlenenie do **práva na mier**, alebo práva na ochranu života a ostatných ľudských práv pred vojnou. Vieme ale, že právo na mier je stále skôr *in status nascendi*, o to viac v roku 1966, keď bol prijatý ICCPR. Zákaz vojnovnej propagácie však možno vnímať ako jeho čiastkový prejav, na ktorom sa štáty boli schopné dohodnúť.

... zákonom.

ICCPR nestanovuje **formu implementácie zákonného zákazu**, avšak zo zásady *pacta sunt servanda* vyplýva, že musí ísť o prijatie nástroja, ktorý je dostatočne účinný na efektívne plnenie záväzku. Štát je povinný „prijatť zákon podľa ktorého je propaganda... v rozpore s verejným poriadkom a ktorý stanovuje primeranú sankciu v prípade jeho porušenia.“⁴⁴ Takýmto prostriedkom poskytujúcim primeranú sankciu pri tak spoločensky nebezpečnom konaní je predovšetkým, hoci nie výlučne, trestnoprávna forma implementácie zákazu.⁴⁵

⁴³ „The Committee observes that war and other acts of mass violence continue to be a scourge of humanity and take the lives of thousands of innocent human beings every year. Under the Charter of the United Nations the threat or use of force by any State against another State, except in exercise of the inherent right of self-defence, is already prohibited. The Committee considers that States have the supreme duty to prevent wars, acts of genocide and other acts of mass violence causing arbitrary loss of life. Every effort they make to avert the danger of war, especially thermonuclear war, and to strengthen international peace and security would constitute the most important condition and guarantee for the safeguarding of the right to life. In this respect, the Committee notes, in particular, **a connection between article 6 and article 20**, which states that the law shall prohibit any propaganda for war (para. 1) or incitement to violence (para. 2) as therein described.“ Ods. 2 CCPR: General Comment No. 6: Article 6 (Right to Life), 1982. Podobne aj „A particular connection exists between article 6 and article 20, which prohibits any propaganda for war and certain forms of advocacy constituting incitement to discrimination, hostility or violence. Failure to comply with these obligations under article 20, may also constitute a failure to take the necessary measures to protect the right to life under article 6.“ Ods. 59. CCPR: General Comment no. 36.

⁴⁴ „For article 20 to become fully effective there ought to be a law making it clear that propaganda... are contrary to public policy and providing for an appropriate sanction in case of violation.“ CCPR: General comment no. 11.

⁴⁵ NOWAK, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd rev. ed. Kehl am Rhein: N.P. Engel, 2005, s. 470, 474.

Zo správ Slovenskej republiky adresovaných Výboru pre ľudské práva vyplýva, že **Slovenská republika sa rozhodla predmetný záväzok implementovať práve trestnoprávnou cestou, a to prostredníctvom trestného činu ohrozenia mieru.**

Ustanovenie § 417 TrZ je prevzatím skutkovej podstaty trestného činu zo zákona č. 165/1950 Zb. na ochranu mieru,⁴⁶ ktorý je v zmysle správ Slovenskej republiky adresovanej Výboru pre ľudské práva⁴⁷ **implementáciou čl. 20 ods. 1 Medzinárodného paktu o občianskych a politických právach z roku 1966** (ďalej len „ICCPR“).⁴⁸ Preto je potrebné predmetné ustanovenie vykladať medzinárodno-konformne, tzn. spôsobom zabezpečujúcim súlad s obsahom záväzkov Slovenskej republiky vyplývajúcich z ICCPR. Pri určovaní obsahu týchto medzinárodných záväzkov je vhodné prihliadať na interpretačné zdroje k ICCPR, vrátane všeobecných komentárov Výboru pre ľudské práva, ktoré sú uznávaným referenčným materiálom pri výklade tohto paktu.

Medzinárodno-konformný výklad je súčasťou ustálenej interpretačnej metodológie Ústavného súdu SR.⁴⁹ Mrva a Turčan uvádzajú, že podstata medzinárodno-

⁴⁶ Vid' dôvodová správa vládneho návrhu Trestného zákona. „K XII. hlave K 1. dielu K § 425 Trestný čin proti mieru bol doposiaľ obsiahnutý v osobitnom zákone na ochranu mieru č.165/1950 Zb., ktorý sa navrhuje zrušiť.“

⁴⁷ Ods. 77 „In keeping with this article [art. 20] of the Covenant, any propaganda for war is prohibited under Act No. 165/1950 Coll. on the safeguarding of peace...” Initial report of Slovakia on Implementation of the International Covenant on Civil and Political Rights 13/02/1996, CCPR/C/81/Add.9, 13 February 1996. Online: <https://www.mzv.sk/documents/30297/2698925/19960213%20Civil%20and%20Political%20Rights%20-%20Initial%20report%20of%20Slovakia%20on%20Implementation%20of%20the%20International%20Covenant%20on%20Civil%20and%20Political%20Rights.pdf/fe07a826-11d3-42fb-b68b-ff1730f69756>. Ods. 407 a nasl.: „[Regarding art. 20] In § 417, the Criminal Code defines promoting war as a criminal offence against peace according to which any person who intentionally disturbs peace by inciting to war, promoting war in any manner or otherwise supporting war propaganda shall be liable to a term of imprisonment of between one and ten years. An offender shall be liable to a term of imprisonment of between ten and twenty-five years or life imprisonment when such crime was committed in association with a foreign power or foreign official or in the capacity of a member of a dangerous group or in a crisis situation.” Third periodic report of Slovakia on Implementation of the International Covenant on Civil and Political Rights 20/10/2009. CCPR/C/SVK/3, 20 October 2009. Online: <https://www.mzv.sk/documents/30297/2698925/20091020%20Civil%20and%20Political%20Rights%20-%20Third%20periodic%20report%20of%20Slovakia%20on%20Implementation%20of%20the%20International%20Covenant%20on%20Civil%20and%20Political%20Rights.pdf/e66b4b4c-aad5-42fa-b990-94ae5444e061>

⁴⁸ Vyhláška MZV č. 120/1976 Zb.

⁴⁹ Vid' napr. PL. ÚS 16/2018-104, PL. ÚS 8/2016-131, PL. ÚS 6/2019-78, III. ÚS 8/2023-28, PL. ÚS 2/2016-108 a iné.

konformného výkladu spočíva v tom, že „...povinnosť interpretovať... vnútroštátne právo SR s ohľadom na príslušnú právnu úpravu obsiahnutú v medzinárodnej zmluve. Pre prípad rozporu medzi vnútroštátnou právnu úpravou a právnu úpravou obsiahnutou v medzinárodnej zmluve... musí súd preskúmať, či je možné vnútroštátny zákon vykladať v súlade s medzinárodnou zmluvou, a teda zabezpečiť medzinárodno-konformný výklad práva.“⁵⁰ Iným slovom, v prípade, ak právny predpis pripúšťa dvojaký výklad, tak má orgán aplikovať ten výklad, ktorým je naplnená dikcia medzinárodnej zmluvy.⁵¹ **Povinnosť medzinárodno-konformného výkladu vyplýva z čl. 1 ods. 2 Ústavy SR.**⁵² Orgány aplikácie práva preto majú vykladať slovenské právo tak, aby vyjadrili ústavnú povinnosť uznávať a dodržiavať medzinárodnoprávne normy, ktorými je Slovenská republika viazaná. Pri výklade § 417 TrZ nie je možné prihliadnuť na aplikačnú prax

Záver

Propagovanie vojny je jav, ktorý sa zintenzívňuje v kontexte vedenia informačnej vojny. Predmetom článku bola výhradne právna rovina jednej z jej najzávažnejších podôb — propagácie vojny. Vnímanie jej závažnosti viedlo aj k explicitnému vyňatiu z rámca slobody prejavu.

⁵⁰ MRVA, Michal – TURČAN, Martin: Interpretácia a argumentácia v práve“ Bratislava: Wolters Kluwer, 2016.

⁵¹ Per analogiam I. ÚS 338/06.

⁵² „Čl. 1 ods. 2... smeruje k vnútroštátnym orgánom, aby vždy konali v dobrej viere s úmyslom rešpektovať medzinárodné záväzky SR... Slovenská republika, a teda aj všetky orgány, ktoré ju vnútroštátne reprezentujú, musia zohľadňovať medzinárodné záväzky, ktoré štát viažu. To je nevyhnutné nielen pri tvorbe vnútroštátnej legislatívy, ale aj v procese jej interpretácie a následnej aplikácie vo vnútroštátnych vzťahoch... všetky orgány vnútroštátnej aplikácie práva by sa mali snažiť vždy čo najširšie zohľadniť slovenské medzinárodné záväzky a v ich svetle vykladať ustanovenia vnútroštátneho práva. Mali by sa snažiť odstrániť potencionálne konflikty medzi nimi, resp. ich takýmto prístupom minimalizovať (v tzv. medzinárodne konformnom výklade vnútroštátnych právnych noriem).“ OROSZ, Ladislava – SVÁK, Ján a kol.: Ústava Slovenskej republiky: Komentár, zväzok I. Bratislava: Wolters Kluwer, 2021, s. 38-39. Tiež aj DRGONEC, Ján: Ústavné právo hmotné. Bratislava: C. H. Beck, 2018, s. 84. „Čl. 1 ods. 2 ústavy sa týka všetkých medzinárodných záväzkov Slovenskej republiky bez ohľadu na ich obsah a ustanovuje povinnosť ich plnenia. Každý medzinárodný záväzok Slovenskej republiky má svoj konkrétny obsah... V dôsledku toho sa príslušná vnútroštátna právna úprava (zákon) môže dostať do nesúladu s takýmto medzinárodným záväzkom a o takomto ich nesúlade je ústavný súd oprávnený konať aj v konaní o súlade právnych predpisov...“ Uznesenie Ústavného súdu SR sp. zn. PL. ÚS 44/03 z 21. októbra 2003. Pozri aj GIBA, Marián a kol.: Ústavné právo. Bratislava: Wolters Kluwer, 2019, s. 82-88. BARANÍK, K.: Ústava na hviezdnom nebi. Vzťah Ústavy Slovenskej republiky k medzinárodnému právu. Praha: Leges, 2020, s. 177. ČORBA, J.: Prednosť medzinárodných zmlúv pred zákonom In *Justičná revue*, č. 6-7 (2002), s. 704-705. KROŠLÁK, D. a kol.: Ústavné právo. Bratislava: Wolters Kluwer, 2016, s. 128-129.

V príspevku bolo poukázané nato, že hoci sa zákaz vojnovej propagandy stal súčasťou medzinárodného práva už pred druhou svetovou vojnou a je možné identifikovať názory aj o jeho obvyčajovej povahe, dokonca ako súčasti základnej zásady zákazu použitia sily a hrozby použitím sily, za najvýznamnejší a nespochybniteľný prameň jej zákazu je možné považovať čl. 20 ods. 1 Medzinárodného paktu o občianskych a politických právach, ktorého výkladu bola venovaná prioritná pozornosť. Túto úlohu sťažuje absencia rozhodovacej praxe Výboru pre ľudské práva v individuálnych veciach.

Vojnovú propagandu je možné chápať ako úmyselné konanie spočívajúce v propagovaní medzinárodného ozbrojeného konfliktu v rozpore s medzinárodným právom. Či pod ňu spadá aj zákaz propagovania ozbrojeného konfliktu nemajúceho medzinárodný charakter nie je jednoznačný. To neznamená, že ide o prejavy chránené slobodou prejavu.

Zákaz sa týka tak propagovania budúceho ozbrojeného konfliktu, ako aj už prebiehajúceho ozbrojeného konfliktu, ako to vyplýva aj z recentnej judikatúry Súdneho dvora EÚ.

Nie je nevyhnutné preukázanie príčinnej súvislosti medzi vojnovou propagandou a konkrétnym následkom. Postačuje, že ide o spôsobilé konanie. Toto by aktivovalo záväzok štátu takúto propagandu zakázať v zmysle ICCPR. Čl. 20 ods. 1 však nie je len záväzkom štátu, ale môže vytvárať aj konkrétne oprávnenie jednotlivca. Tento zákaz je podľa CCPR nederogovateľný, čím sa zaradzuje do skupiny dojednaní ako je zákaz mučenia. Závažnosť vojnovej propagandy vyplýva aj z prípravných materiáloch na ICCPR. Ide o prejavy, pri ktorých štát nielenže má oprávnenie zasiahnuť, ale povinnosť. Tým sa odlišujú zásahy štátu pri čl. 19 kde sa posudzuje primeranosť zásahu a čl. 20, kde by otázka mala byť kladená opačne – prečo štát nezasiahol, ak takúto povinnosť mal.

Pre aktívnu legitimáciu konkrétneho sťažovateľa v prípadnom konaní pred Výborom pre ľudské práva by však bolo potrebné preukázať ujmu. Použijúc analógiu s čl. 20 ods. 2 ICCPR by ňou mohol byť aj všeobecný pocit úzkosti alebo pocit ohrozenia. V zmysle všeobecných komentárov CCPR je potrebné zákaz vojnovej propagandy chápať vo vzťahu k ochrane práva na život. Zákazom určitého konania sa chránia ostatné práva jednotlivca v zmysle ICCPR.

ICCPR síce stanovuje povinnosť zákazu vojnovej propagandy, avšak nedefinuje bližšie aké zákonné prostriedky nato štát využije. Možno len uviesť, žeby malo ísť o prostriedky ktoré sú dostatočne účinné na jeho presadenie. Zo správ Slovenskej republiky vyplýva, že svoj záväzok implementuje skutkovou podstatou trestného činu ohrozenia mieru definovanou v § 417 Trestného zákona. Táto by sa preto mala aj primerane vykladať s ohľadom na medzinárodnoprávny záväzok.

Zoznam použitej literatúry

1. Americký dohovor o ľudských právach z roku 1969.
2. Medzinárodný pakt o občianskych a politických právach z roku 1966.
3. A/RES/2625(XXV), 24 October 1970.
4. A/RES/841 (IX), 17 December 1954.
5. A/RES/381(V), 17 November 1950.
6. A/RES/59(I), 14 December 1946.
7. Helsinki Final Act (1975).
8. CCPR: General Comment no. 36.
9. CCPR: General Comment no. 34.
10. CCPR: General Comment no. 29.
11. CCPR: General comment no. 11.
12. CCPR: General Comment no. 6.
13. Vyhláška MZV č. 120/1976 Zb.
14. CJEU: Judgment of the General Court (First Chamber, Extended Composition) of 26 March 2025. A2B Connect BV and Others v Council of the European Union. Case T-307/22.
15. CJEU: Judgment of the General Court (Grand Chamber) of 27 July 2022. RT France v Council of the European Union. Case T-125/22.
16. ICTR: Prosecutor v. Nahimana et al. (Media case). Case No. ICTR-99-52-T, Trial Judgement 03 Dec 2003.
17. International Military Tribunal (Nuremberg), Judgment, 1.10.1946.
18. ECHR: Medya FM Reha Radio ve İletişim Hizmetleri A.Ş. v. Turkey (App. no.32842/02), 14 November 2006.
19. ECHR: Özgür Gündem v. Turkey (App. no. 23144/93), 16 March 2000.
20. ECHR: Sürek (No. 1) v. Turkey (App. no. 26682/95), 8 July 1999.
21. III. ÚS 8/2023-28.
22. PL. ÚS 6/2019-78.
23. PL. ÚS 16/2018-104.
24. PL. ÚS 8/2016-131.
25. PL. ÚS 2/2016-108.
26. I. ÚS 338/06.
27. PL. ÚS 44/03.
28. Third periodic report of Slovakia on Implementation of the International Covenant on Civil and Political Rights 20/10/2009. CCPR/C/SVK/3, 20 October 2009.
29. Initial report of Slovakia on Implementation of the International Covenant on Civil and Political Rights 13/02/1996, CCPR/C/81/Add.9, 13 February 1996.

30. ASWAD, Evelyn: Propaganda for War & International Human Rights Standards In: *Chicago Journal of International Law*. Vol. 24 No. 1 (2023).
31. BARANÍK, K.: *Ústava na hviezdnom nebi. Vzťah Ústavy Slovenskej republiky k medzinárodnému právu*. Praha: Leges, 2020.
32. ČORBA, J.: Prednosť medzinárodných zmlúv pred zákonom. In: *Justičná revue*, č. 6-7 (2002).
33. DRGONEC, Ján: *Ústavné právo hmotné*. Bratislava: C. H. Beck, 2018.
34. FINA, Audrey: A critique of the UN Strategy and Guidance on 'Hate Speech': Some Legal Considerations. In: *Netherlands Quarterly of Human Rights*, Vol 41, No. 4 (2023).
35. GIBA, Marián a kol.: *Ústavné právo*. Bratislava: Wolters Kluwer, 2019.
36. JOSEPH, Sarah – CASTAN, Melissa: *The International Covenant on Civil and Political Rights*. Oxford: Oxford University Press, 2013.
37. KAERNEY, Michael G.: *The Prohibition of Propaganda for War in International Law*. Oxford: Oxford University Press, 2007.
38. KROŠLÁK, D. a kol.: *Ústavné právo*. Bratislava: Wolters Kluwer, 2016.
39. MRVA, Michal – TURČAN, Martin: *Interpretácia a argumentácia v práve*. Bratislava: Wolters Kluwer, 2016.
40. NOWAK, Manfred. *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 2nd rev. ed. Kehl am Rhein: N.P. Engel, 2005.
41. OROSZ, Ladislava – SVÁK, Ján a kol.: *Ústava Slovenskej republiky: Komentár, zväzok I*. Bratislava: Wolters Kluwer, 2021.
42. PADALKO, Halyna et al.: Investigation of machine learning approaches to classify war-related content during Russian full-scale invasion of Ukraine. In: *Social Network Analysis and Mining*. Vol. 15, No. 73 (2025).
43. SCHMITT, Michael N. – VIHUL, Liis (eds.): *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
44. TEMPERMAN, Jeroen: The International Covenant on Civil and Political Rights and the "Right to be Protected against Incitement". In: *Journal of Law, Religion and State*. No. 7 (2019).
45. WILLAERT, Tom – TUTERS, Marc: From denazification to the Golden Billion: an inductive analysis of the Kremlin's weaponisation of digital diplomacy on Telegram. In: *Humanities & Social Sciences Communications*. Vol. 12, No. 989 (2025).

Kontaktné údaje

JUDr. Lukáš Mareček, PhD.

lukas.marecek@flaw.uniba.sk

Katedra medzinárodného práva a medzinárodných vzťahov

Právnická fakulta Univerzity Komenského v Bratislave

LIMITY DIGITALIZÁCIE V KONTEXTE ZÁKLADNÉHO PRÁVA POUŽÍVAŤ HOTOVOŠŤ

LIMITS OF DIGITALIZATION IN THE CONTEXT OF THE FUNDAMENTAL RIGHT TO USE CASH

Vincent Bujňák¹

Abstrakt: Národná rada ako delegovaný ústavodarca rozšírila dvadsiatou druhou novelou slovenskej Ústavy katalóg základných práv a slobôd o nové právo. Je ním právo používať hotovosť, zaradené medzi hospodárske, sociálne a kultúrne práva. Keďže takéto právo sa do ústavného textu doplnilo relatívne nedávno (2023), doposiaľ k nemu nemal možnosť zaujať stanovisko v niektorom type konania ani Ústavný súd Slovenskej republiky. Zároveň je neobvyklé nielen z hľadiska medzinárodných dokumentov, ale tiež optikou komparatívneho ústavného práva. Príspevok v tejto súvislosti overuje platnosť hypotézy, že ústavná fixácia práva používať hotovosť má konkrétny normatívny dopad, pričom pri obmedzovaní daného základného práva sa má používať modifikovaný test proporcionality. Pri overovaní tejto hypotézy autor vychádza z doterajšej rozhodovacej činnosti Ústavného súdu Slovenskej republiky z iných typov konania. Na základe týchto zdrojov bola platnosť hypotézy potvrdená s tým, že základné právo používať hotovosť má relatívny charakter a môže byť preto obmedzené. Pri jeho obmedzovaní sa však nemá používať tzv. štvorkrokový prísny test proporcionality, ale osobitný test racionality. Praktický prínos príspevku spočíva v tom, že identifikuje prípady dvoch právnych úprav, pri ktorých existuje riziko ich nesúladu s novým základným právom, a to konkrétne pri absolútnom vylúčení hotovosti pri platení parkového a pri vylúčení hotovosti pri platení poisťného v Sociálnej poisťovni.

Kľúčové slová: hospodárske práva, sociálne práva, právo používať hotovosť, Ústava Slovenskej republiky, test proporcionality, test racionality.

Abstract: The National Council, acting as constituted power, expanded the catalogue of fundamental rights and freedoms by the Twenty-Second Amendment to the Slovak Constitution. This amendment introduced a new right: the right to use cash, classified among economic, social, and cultural

¹ Katedra ústavného práva, Právnická fakulta Univerzity Komenského v Bratislave.

rights. Since it was incorporated into the constitutional text only recently (in 2023), the Slovak Constitutional Court has not yet had the opportunity to address it in any type of proceedings. At the same time, such provision is unusual not only in the light of international human rights documents, but also from the perspective of comparative constitutional law. The paper examines the validity of the hypothesis that the constitutional entrenchment of the right to use cash produces a concrete normative effect, and that any restriction of this fundamental right should be assessed through a modified proportionality test. In testing this hypothesis, the author relies on the prior jurisprudence of the Slovak Constitutional Court in other types of proceedings. Based on these sources, the hypothesis is confirmed: the fundamental right to use cash is of a relative nature and may therefore be subject to limitations. However, such limitations should not be reviewed under the so-called four-step strict proportionality test, but rather through a specific rationality test. The practical significance of the paper lies in identifying two areas of legislation that may be repugnant to this newly entrenched fundamental right: the absolute exclusion of cash payments for parking fees and the exclusion of cash payments for social insurance contributions.

Key words: economic rights, social rights, right to use cash, Constitution of the Slovak Republic, proportionality analysis, rationality test.

Úvod

Súčasťou ústavného poriadku Slovenskej republiky je po vzore iných demokratických a právnych štátov aj osobitná ústavná úprava základných práv a slobôd. Ich katalóg sa nachádza v druhej hlave slovenskej ústavy, pričom jeho znenie bolo vytvárané s ohľadom na Všeobecnú deklaráciu ľudských práv a predovšetkým Listinu základných práv a slobôd, schválenú v rámci ústavného zákona č. 23/1991 Zb. Federálnym zhromaždením Českej a Slovenskej Federatívnej Republiky.² Práve túto listinu možno považovať za spoločné ústavné dedičstvo oboch nástupníckych štátov bývalej federácie.³ Hoci už pri schvaľovaní slovenskej ústavy sa znenie v určitých oblastiach od textu listiny odlišovalo, výraznejšie modifikácie priniesla až novelizačná činnosť delegovaného ústavodarcu v nasledujúcich obdobiach. Medzi tieto

² PETRANSKÁ ROLKOVÁ, Natália.: Ústava Slovenskej republiky a jej dvadsaťpäť rokov (1992 – 2017). Bratislava: Kancelária Národnej rady Slovenskej republiky, 2017, s. 35.

³ Pozri OROSZ, Ladislav.: Listina základných práv a slobôd ako súčasť ústavného systému Slovenskej republiky. In: Listina a súčasnosť. Sborník příspěvků sekce ústavního práva, přednesených na mezinárodní vědecké konferenci Olomoucké právnické dny 2010. Olomouc: Iuridicum Olomoucense, o. p. s., 2010, s. 156.

novelizácie je potrebné zaradiť aj dvadsiatu druhú novelu ústavy, teda ústavný zákon č. 241/2023 Z. z. Národná rada ním cez čl. 39a zaradila medzi hospodárske, sociálne a kultúrne práva aj (i) garanciu vydávania hotovosti ako zákonného platidla, ďalej (ii) právo vykonať platbu za nákup tovarov a poskytnutie služieb v hotovosti zákonným platidlom, a napokon (iii) právo vykonať hotovostnú operáciu v banke alebo pobočke zahraničnej banky. Pre tieto práva možno použiť strešný pojem „právo používať hotovosť“, lebo všetky tri sú jeho podstatnými komponentmi. Aby totiž mohla byť hotovosť používaná, musí byť v ustanovenej forme vydávaná, použiteľná a jednoducho distribuovateľná.

Ideové východiská

Základné právo uvedené v čl. 39a ústavy je už na prvý pohľad netradičné a na rozdiel od iných základných práv bez obdoby v medzinárodných ľudskoprávných zmluvách a dokumentoch. I keď zmienka o razbe mincí je prítomná napríklad v Ústave Spojených štátov, je zahrnutá ako kompetencia kongresu, a nie základné právo.⁴ Na druhej strane platí, že diskusie o uznaní práva používať hotovosť ako základného práva neboli obmedzené iba na Slovenskú republiku. Návrh na jeho ústavné ukotvenie bol neúspešne podaný v Rakúsku,⁵ neskôr tiež v Českej republike, Rumunsku a Slovinsku.⁶ Naopak, k úspešnému schváleniu obdoby práva používať hotovosť došlo v Maďarsku prostredníctvom 15. dodatku k tamajšej ústave, ktorý upravil XIII. článok nasledovne: *„Každý má právo na vlastníctvo a dedenie, ako aj na platbu v hotovosti. Vlastníctvo so sebou nesie spoločenskú zodpovednosť.“*⁷

⁴ Podľa článku 1 oddielu 8 Ústavy Spojených štátov má kongres právomoc raziť peniaze, upravovať ich hodnotu, domáci i zahraničný kurz a stanoviť jednotky mier a váh. Pozri MIERNICKI, Martin: Cash, accounts, and central bank digital currencies: a legal view on the introduction of account- and token-based digital central bank money. In: Law and Financial Markets Review, roč. 17, č. 2, 2023, s. 107.

⁵ GSTÖTTNER, Susanne, LACHMAYER, Konrad: Austria. In: The 2020 International Review of Constitutional Reform. Austin: Program on Constitutional Studies at the University of Texas in collaboration with the International Forum on the Future of Constitutionalism, 2021, s. 22.

⁶ Pozri kapitoly venujúce sa týmto štátom v publikácii BARROSO, Luís Roberto, ALBERT, Richard (eds.): The 2023 International Review of Constitutional Reform. Austin: Constitutional Studies Program at the University of Texas in collaboration with the International Forum on the Future of Constitutionalism, 2024, s. 115, 307 a 335.

⁷ Šiesty recitál v návrhu 15. dodatku uvádza zdôvodnenie tohto kroku: *„Hotovosť je také zákonné platidlo, ktoré je vo svojej fyzickej forme nezávislé od digitálnych systémov, bánk a iných tretích strán. Iba zachovanie obehu hotovosti môže zaisťovať, že fungovanie hospodárstva sa nestane úplne závislým od elektronických finančných systémov, ktoré môžu byť z technických alebo trhových dôvodov zraniteľné. (...) Zakotvenie tohto práva na úrovni základného zákona tiež zaručuje, že možnosť platby v hotovosti ostane dostupná pre každého, čím sa zabráni možnosti finančného vylúčenia.“* Zaujímavosťou je, že sprievodné dokumenty k uvedenému dodatku explicitne odkazovali aj na slovenskú ústavnú fixáciu. Pozri parlament.hu/irom42/11152/11152.pdf.

Pokiaľ dochádza k uznaniu určitého nového základného práva, je nevyhnutné vysvetliť jeho ideové východiská. Myšlienka ústavnej fixácie ochrany používania hotovosti má svoj pôvod v Rakúsku. Keď sa v roku 2016 na úrovni EÚ diskutovalo o zavedení limitu pre hotovostné platby nad 5 000 eur a o zrušení 500-eurovej bankovky, práve z Rakúska sa ozývali hlasné nesúhlasné stanoviská, napríklad aj od predstaviteľov etablovanej politickej strany ÖVP. Tí zdôrazňovali, že hotovosť je kúskom „*razenej slobody*“, pričom v digitálnom veku podľa nich má byť právo na súkromie a anonymitu pri platbách garantované a chránené. Slovanami neskoršieho ministra pre vedu, výskum a hospodárstvo H. Mahrera: „*Nikto sa nemá starať do toho, čo konzumujem, kde nakupujem alebo aké filmy sledujem.*“⁸

Mohlo by sa javiť, že tieto myšlienky sa v podmienkach Slovenskej republiky neuchytili, lebo Národná rada schválila ešte niekoľko rokov predtým bez väčšej spoločenskej odozvy zákon č. 394/2012 Z. z. o obmedzení platieb v hotovosti. Platba v hotovosti nad 5 000 eur sa ním zakázala, a pri platbách medzi fyzickými osobami – nepodnikateľmi bol limit navýšený na 15 000 eur. Vláda ako predkladateľ návrhu zákona prízvukovala, že úprava predstavuje „*príspevok nielen k obmedzeniu podvodných konaní v daňovej oblasti, ale aj ako opatrenie na boj proti praniu špinavých peňazí, na boj proti korupcii a trestnej činnosti, či pri ochrane pred financovaním terorizmu*“.⁹ V roku 2023 už na úrovni Národnej rady pri prerokúvaní návrhu ústavného zákona zaznievali „rakúske“ argumenty, keď jeho predkladatelia poukazovali na snahy vedúce k postupnému obmedzeniu platieb v hotovosti a prepojenie navrhovaného základného práva s právom na súkromie.¹⁰

Prepojenie práva používať hotovosť so základným právom na súkromie je zdôrazňované aj v iných štátoch. Príkladom je Z. Koudelka, podľa ktorého je možnosť slobodne sa rozhodnúť platiť svoje dlhy v hotovosti jedným z nevyhnutných predpokladov pre zachovanie základného súkromia a autonómie jednotlivcov nielen voči štátu, ale voči všetkým, vrátane blízkych osôb. Rovnako poukazuje na právo užívať majetok, lebo bezhotovostné platby zo svojej podstaty umožňujú absolútnu kontrolu nad majetkom jednotlivca, k čomu ako príklad uvádza zablokovanie účtov protestujúcich kanadských vodičov kamiónov v roku 2022.¹¹ Možno k tomu doplniť,

⁸ JILCH, Nikolaus: ÖVP will Bargeld in der Verfassung. In: Die Presse, 14. februára 2016. Dostupné na diepresse.com/4923994/oevp-will-bargeld-in-der-verfassung.

⁹ Parlamentná tlač 235 (VI. volebné obdobie).

¹⁰ Vtedajší predseda výboru pre financie a rozpočet poukazoval na tzv. digitálne euro. Pozri stenografický záznam z 88. schôdze Národnej rady (17. marec 2023, VIII. volebné obdobie).

¹¹ KOUDELKA, Zdeněk: Zústavnění práva na hotovost. In: Právo na nedigitální život. Sborník z kulatého stolu, který proběhl dne 11. února 2025 v Senátu Parlamentu ČR pod záštitou senátního Ústavně-právního výboru. Praha: Nová vlna, 2025, s. 29. K podrobnostiam pozri EATON, Piers, GASPARD, Valere: A convoy, an emergencies act, and a state of exception: How Canada's Emergencies Act contradicts Carl Schmitt's critiques of deliberative democracy. In: British Journal of Canadian Studies, roč. 36, č. 2, s. 133 – 156.

že nové základné právo má súvis aj so zmluvnou autonómiou, lebo bezhotovostná platba si štandardne vyžaduje predchádzajúci zmluvný vzťah s platobnou inštitúciou,¹² resp. dodávateľom určitej služby. Inými slovami, pokiaľ je napríklad možné uhradiť parkovné len platobnou kartou, prostredníctvom aplikácie alebo SMS-kou, potom je k tomu nevyhnutné využívať najčastejšie služby banky a (resp. alebo) mobilného operátora.

Korektné aplikačné uchopenie práva používať hotovosť

Pri overovaní hypotézy, že ústavná fixácia práva používať hotovosť má konkrétny normatívny dopad, je potrebné vychádzať v prvom rade z nálezu ústavného súdu sp. zn. PL. ÚS 12/01 zo 4. decembra 2007. Daná vec sa okrem iného týkala ústavnej normy prítomnej (rovnako ako čl. 39a) v druhej hlave ústavy. Podľa čl. 15 ods. 1 druhej vety ústavy je ľudský život hodný ochrany už pred narodením. Na dané ustanovenie nazeral prvý komentár k ústave tak, že má charakter len etickej normy, a azda môže pôsobiť ako interpretačné pravidlo k niektorým ďalším článkom ústavy.¹³ Takéto nazeranie bolo Ústavným súdom odmietnuté: „*Vyložiť druhú vetu čl. 15 ods. 1 ústavy len ako proklamáciu je však v zásadnom rozpore so súčasnou koncepciou ústavy, ktorá nie je dokumentom obsahujúcim normatívne irelevantné proklamácie, ktorých význam je určený až ďalšou zákonodarcovou činnosťou, ale je skutočným súborom priamo aplikovateľných noriem, princípov a hodnôt, ktoré majú svoj konkrétny normatívny dopad (pozri najmä čl. 152 ods. 4 ústavy).*“ Čl. 15 ods. 1 druhá veta bola označená za ústavnú hodnotu, spôsobilú byť predmetom vyvažovania s inými základnými právami, prípadne ďalšími ústavnými hodnotami.

Druhým identifikovaným prípadom z rozhodovacej činnosti Ústavného súdu je vec sp. zn. PL. ÚS 13/2022 z 13. decembra 2022. Tá sa týkala v tom čase relatívne nového čl. 55a, doplneného do ústavného textu prostredníctvom ústavného zákona č. 422/2020 Z. z. s účinnosťou od 1. januára 2021. Delegovaný ústavodarca do tohto článku zakotvil, že Slovensko chráni dlhodobú udržateľnosť svojho hospodárenia, ktoré sa zakladá na transparentnosti a efektívnosti vynakladania verejných prostriedkov. Na podporu cieľov podľa predchádzajúcej vety ústavný zákon upravuje pravidlá rozpočtovej zodpovednosti, pravidlá rozpočtovej transparentnosti a pôsobnosť Rady pre rozpočtovú zodpovednosť. Ústavný súd zopakoval svoj prístup z veci sp. zn. PL. ÚS 12/01, i keď čl. 55a nie je súčasťou druhej, ale tretej hlavy ústavy. Slovami P. Matušku, ekonomické aspekty tohto článku nemajú len deklaratórny

¹² Pozri rozsudok Krajského súdu Žilina sp. zn. 30 S/138/2020 z 30. augusta 2022, 27. bod.

¹³ Čič, Milan a kolektív: Komentár k Ústave Slovenskej republiky. Martin: Matica slovenská, 1997, s. 88.

účinnok – naopak, disponujú konkrétnym ústavnoprávnym obsahom.¹⁴ Imperatív rozpočtovej zodpovednosti je opäť spôsobilým predmetom vyvažovania, konkrétne s ústavnou hodnotou reprezentatívnej demokracie.¹⁵

Napokon posledný identifikovaný prípad vzišiel z konania o výklade ústavy podľa čl. 128, konkrétne povinnosti hlavy štátu zabezpečovať svojim rozhodovaním riadny chod ústavných orgánov. Ústavný súd zopakoval závery z vecí sp. zn. PL. ÚS 12/01 a sp. zn. PL. ÚS 13/2022, no pri ústavnej norme kompetenčného charakteru prejavil aj určitú zdržanlivosť. Interpretovaná povinnosť podľa neho charakterizuje funkciu prezidenta bez toho, aby malo samostatné kompetenčné účinky, aké má čl. 102 ústavy: „*Formulácia „svojím rozhodovaním zabezpečuje riadny chod ústavných orgánov“ znamená, že prezident rozhoduje na uvedený účel, len ak mu priamo ústava alebo zákon na základe ústavy a v jej medziach (čl. 2 ods. 2 ústavy) zveruje určitú pôsobnosť, ktorú rozhodovacia činnosť prezidenta nemôže relevantne prekročiť.*“¹⁶

Z troch citovaných nálezov Ústavného súdu má posledný prípad k čl. 39a najďalej, keďže základné právo používať hotovosť nie je kompetenčnou ústavnou normou vzťahujúcou sa na konkrétny orgán verejnej moci. Z tohto dôvodu platí záver, že čl. 39a nie je normatívne irelevantnou proklamáciou, ktorého význam je určený až ďalšou zákonodarcovou činnosťou, ale priamo aplikovateľnou normou s konkrétnym normatívnym dopadom. Je vhodné zdôrazniť, že prístup k čl. 39a ústavy rozhodne nesmie byť založený na tom, či ho interpretujúci subjekt vníma kladne alebo záporne. Uvedený záver tiež znamená, že čl. 39a sa môže stať referenčným kritériom aj v konaní pred ústavným súdom, okrem iného tiež v konaní o súlade právnych predpisov.

Metodika obmedzovania práva používať hotovosť

V zmysle čl. 51 ods. 1 ústavy sa vymedzených základných práv možno domáhať len v medziach vykonávacích zákonov. Sú medzi nimi aj všetky základné práva obsiahnuté v čl. 38 až 42 ústavy, čo zahŕňa novovytvorený čl. 39a. Ústava v zmysle rozhodovacej činnosti ústavného súdu k čl. 51 ods. 1 poskytuje zákonodarcovi v porovnaní s inými skupinami základných práv a slobôd väčší priestor pre voľnú úvahu na účely určenia v akom rozsahu, kvalite a za akých podmienok ich bude garantovať. Preto sa pri obmedzovaní automaticky nepoužíva test proporcionality, ale štvorkrokový test racionality. Prvý krok pozostáva z vymedzenia esenciálneho obsahu (jadra) posudzovaného práva. Ďalším krokom je vyhodnotenie, či obmedzenie do

¹⁴ MATUŠKA, Peter: Postavenie ústavného súdu pri ochrane ekonomických aspektov ústavného práva. In: Právny obzor, 108, 2025, č. 4, s. 384.

¹⁵ Ústavný súd následne zopakoval prístup založený na normatívnom význame čl. 55a aj v 91. bode odôvodnenia v náleze sp. zn. PL. ÚS 7/2024 z 18. decembra 2024.

¹⁶ Nález sp. zn. PL. ÚS 16/2023 z 20. novembra 2024, 52. bod.

definovaného esenciálneho obsahu zasahuje, ale nie. Ak je odpoveď záporná, pristupuje sa k tretiemu kroku (identifikácia legitímneho cieľa) a napokon sa v záverečnom kroku zvažuje, či je zákonný prostriedok použitý na jeho dosiahnutie rozumný (racionálny), aj keď nie nevyhnutne najlepší, najvhodnejší, najúčinnjší či najmúdrejší. Prísny test proporcionality je aplikovaný vtedy, keď sa v zmysle druhého kroku testu racionality obmedzenie dotýka esenciálneho obsahu základného práva. Zásah musí vtedy splniť nielen všetky časti testu proporcionality, ale tiež je potrebné v rámci zdôvodnenia preukázať úplnú výnimočnosť situácie, ktorá by takýto zásah ospravedlňovala.¹⁷

Obmedzovanie práva používať hotovosť má svoje špecifiká z dôvodu osobitnej limitačnej klauzuly, prítomnej v čl. 39a ods. 2 ústavy. Pri schvaľovaní ústavného zákona č. 241/2023 Z. z. sa v druhom čítaní dosiahol kompromis, sledujúci vylúčenie rizika šikanózneho výkonu nového základného práva. Cieľom bolo, aby mohol platbu v hotovosti odmietnuť ten, kto na prijímanie hotovosti nie je usposobený, alebo kto hotovosť jednoducho neprijíma od nikoho. Delegovaný ústavodarca sa snažil tento cieľ dosiahnuť formuláciou „prijatie platby možno odmietnuť len z primeraných alebo všeobecne uplatňovaných dôvodov“. Za primerané boli označené bezpečnostné dôvody (zníženie rizika trestného činu) alebo technické dôvody (automat hotovosť neprijíma).¹⁸ Pôvodná verzia návrhu predpokladala, že podmienky a obmedzenia práva používať hotovosť ustanoví zákon v rámci všeobecnej limitačnej klauzuly, ktorá sa napokon stala tretím odsekom čl. 39a. Všeobecná limitačná klauzula mala pokryť predovšetkým zákon č. 394/2012 Z. z. o obmedzení platieb v hotovosti, pričom kontrola pôvodu peňazí v spojení s hodnotou stabilného a transparentného ekonomického prostredia bola vyzdvihnutá ako legitímny cieľ.¹⁹

Korektné spôsoby obmedzovania práva používať hotovosť možno identifikovať v spojení s relevantnými časťami práva Európskej únie²⁰ (keďže na rozdiel od Českej republiky, Maďarska či Poľska používa Slovensko jednotnú európsku menu²¹), neopomínajúc rozhodovaciu činnosť Súdneho dvora EÚ. Slovom Ústavného súdu, povinnosť Slovenskej republiky vykladať a uplatňovať vnútroštátne právo vrátane príslušných ustanovení ústavy v zmysle a duchu práva Európskej únie vyplýva aj zo zásady lojálnej spolupráce zakotvenej v čl. 4 ods. 3 Zmluvy o Európskej únii, ktorá inter alia požaduje, aby členské štáty prijali všetky opatrenia všeobecnej alebo

¹⁷ Nález sp. zn. PL. ÚS 2/2020 z 2. februára 2022, 22. a 25. bod.

¹⁸ Odôvodnenie schváleného pozmeňujúceho a dopĺňujúceho návrhu zo 4. mája 2023 (parlamentná tlač 1472, VIII. volebné obdobie).

¹⁹ Parlamentná tlač 1472 (VIII. volebné obdobie).

²⁰ Z primárneho práva je nutné spomenúť čl. 128 ods. 1 ZFEÚ, ďalej čl. 16 ods. 1 Protokolu (č. 4) o štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky, a taktiež zo sekundárneho práva Nariadenie Rady (ES) č. 974/98 z 3. mája 1998 o zavedení eura.

²¹ K podrobnostiam pozri zákon č. 659/2007 Z. z. o zavedení meny euro v Slovenskej republike.

osobitnej povahy, aby zabezpečili plnenie záväzkov vyplývajúcich z práva Európskej únie.²² Súdny dvor k postaveniu zákonného platidla uviedol, že sa nevyžaduje absolútne, ale len principiálne akceptovanie eurobankoviek ako platobného prostriedku: „Na druhej strane nie je na použitie eura ako jednotnej meny a presnejšie na zachovanie účinnosti postavenia hotovosti označenej v euro ako zákonného platidla navyše ani nevyhnutné, aby normotvorca Únie vyčerpávajúcim a jednotným spôsobom stanovil výnimky z tejto základnej povinnosti, pokiaľ je všeobecne zaručená možnosť pre každého dlžníka, aby splnil peňažnú povinnosť platbou v hotovosti. (...) výlučná právomoc Únie v oblasti menovej politiky (...) nemá vplyv na právomoc členských štátov, ktorých menou je euro, upravovať spôsoby plnenia peňažných povinností, či už verejnoprávných alebo súkromnoprávných, najmä pokiaľ takáto právna úprava nezasahuje do zásady, podľa ktorej musí byť vo všeobecnosti možné splniť peňažnú povinnosť platbou v hotovosti.“²³ Primeraným dôvodom pre odmietnutie hotovosti bude konanie v dobrej viere, konkrétne napríklad pri maloobchodnej transakcii situácia, keď maloobchodník nedisponuje mincami, alebo ak je nominálna hodnota bankovky neprimeraná k dlžnej sume.²⁴

V záujme ústavne korektného obmedzenia základného práva používať hotovosť navrhujeme pri identifikácii esenciálneho obsahu (jadra) a eventuálneho zásahu doň zvažovať tri kritériá. Prvým je (i) kritérium pôvodcu obmedzenia. Pokiaľ je ním subjekt disponujúci verejnomocenskými oprávneniami, účel základného práva vedie k zúženej miere úvahy oproti vzťahom založeným na princípe zmluvnej autonómie. Nasleduje (ii) kritérium povahy činnosti, ktorej sa obmedzenie týka. Pri bežnej ľudskej činnosti by miera úvahy mala byť opäť zúžená. Napokon posledným kritériom by mala byť (iii) možnosť zastupiteľnosti. Pokiaľ je použitie hotovosti pri konaní v dobrej viere dostupné bez väčších prekážok u iného subjektu, potom by mali orgány verejnej moci zvážiť, či je ich ingerencia skutočne nevyhnutná.

Pochybnosti o súlade právnych predpisov nižšieho stupňa právnej sily

Spôsobilosť práva používať hotovosť stať sa referenčným kritériom v konaní o súlade právnych predpisov má za následok, že právne predpisy nižšieho stupňa právnej sily sa môžu stať protiústavnými. Z aplikačnej praxe sme identifikovali dva takéto prípady. Tým prvým je zákon č. 461/2003 Z. z., umožňujúci do 4. apríla 2020 prostredníctvom § 146 ods. 2 písm. c) platiť poistné (vrátane poistného dobrovoľne

²² Nález sp. zn. PL. ÚS 16/2018 z 2. apríla 2020, 72. bod.

²³ Rozsudok Súdneho dvora (veľká komora) z 26. januára 2021 v spojených veciach C 422/19 a C 423/19 (Johannes Dietrich a Norbert Häring proti Hessischer Rundfunk), 55. a 56. bod. S rozsudkom sme sa oboznámili prostredníctvom KRIESE, Leo.: Central Bank Digital Currency. A Technical, Legal and Economic Analysis. Cham: Springer, 2023, s. 76.

²⁴ Tamtiež, 8. bod (citujúci odporúčanie 2010/191/EÚ).

poistených osôb) Sociálnej poisťovni v hotovosti. Počas pandémie najprv parlament zákonom č. 66/2020 Z. z. nariadil, aby sa toto pravidlo neuplatňovalo, a následne zákonom č. 125/2022 Z. z. možnosť platenia poistného Sociálnej poisťovni v hotovosti úplne vypustil.²⁵ Parlament tak učinil s odôvodnením, ktoré by bolo možné použiť ako šablónu proti hotovostnému styku vo všeobecnosti: *„Bezhotovostný platobný styk možno považovať za jeden z nástrojov, ktorým sa dá eliminovať podiel šedej ekonomiky, t. j. nelegálneho pohybu peňazí, ktoré štát nemá registrované vo svojich záznamoch. Do šedej ekonomiky, v rámci legálneho platobného styku, patrí aj platenie bankovkami a práve bezhotovostným platobným stykom sa dá jej podiel eliminovať. Za nevýhody hotovostného platobného styku možno považovať aj nebezpečenstvo krádeže, možnosť výskytu chýb pri počítaní, možnosť výskytu falošných peňazí v obeh, dodatočné náklady na zabezpečenie bezpečnosti (trezory, ozbrojená ochrana), možnosť šírenia ochorení, potreba osobného kontaktu a pod.“*²⁶ Keďže relevantné orgány verejnej moci nekonzultovali prijatie návrhu s Európskou centrálnou bankou, tá sa k vypusteniu možnosti platiť poistné v hotovosti vyjadrila so zásadnou kritikou ex post. Slovenské orgány verejnej moci podľa nej dostatočne neposúdili proporcionalitu nového obmedzenia platieb v hotovosti a deklarované ciele verejného záujmu boli konkretizované len vágnym spôsobom, bez konkrétneho posúdenia vplyvu.²⁷ S takýmto hodnotením sa možno stotožniť s doplnením, že mimo obdobia pandémie je argumentácia založená na šírení ochorení mimoriadne ťažkopádna. Sociálna poisťovňa je ako subjekt disponujúci verejnomocenskými oprávneniami na prijímanie hotovosti usporiadaná, a nie sú známe jej výhrady k prijímaniu hotovosti pri iných činnostiach.

Druhým príkladom je nemožnosť úhrady tzv. parkovného v hotovosti. Podľa § 6a ods. 1 zákona č. 135/1961 Zb. o pozemných komunikáciách môže obec na účely organizovania dopravy na svojom území ustanoviť všeobecne záväzným nariadením úseky miestnych ciest na dočasné parkovanie motorových vozidiel, pričom v ňom ustanoví aj výšku úhrady, spôsob jej platenia a spôsob preukázania jej zaplatenia. Sú známe prípady, keď mesto hotovostnú platbu za parkovanie neprípúšťa.²⁸ Vo

²⁵ S týmto problémom sme sa oboznámili vďaka PONIŠT, Viliam: Porušenie konzultačnej povinnosti s Európskou centrálnou bankou ako relevantný dôvod na podanie ústavnej sťažnosti podľa čl. 127 ods. 5 Ústavy SR? In: Konanie o súlade právnych predpisov – návrhové oprávnenie a účinky rozhodnutí ústavného súdu - XIII. ústavné dni. Košice: Univerzita Pavla Jozefa Šafárika, 2025, s. 176.

²⁶ Parlamentná tlač 760 (VIII. volebné obdobie).

²⁷ Pozri 3. časť stanoviska Európskej centrálnej banky k obmedzeniu úhrad poistného na verejné sociálne poistenie v hotovosti zo 7. marca 2023 (CON/2023/7). Dostupné na eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52023AB0007&qid=1720687424448.

²⁸ Pozri všeobecne záväzné nariadenie č. 16/2024 o dočasnom parkovaní motorových vozidiel na vymedzených úsekoch miestnych ciest na území mesta Žilina a argumentáciu mesta: *„Hotovostná platba nie je možná, nakoľko náklady na obstaranie a prevádzku parkomatov na hotovosť sú výrazne vyššie.“* Dostupné na parkovanie.zilina.sk/casto-kladene-otazky/.

výsledku to znamená, že ak osoba nie je v zmluvnom vzťahu s platobnou inštitúciou alebo mobilným operátorom, potom parkovné nedokáže uhradiť. To platí aj vtedy, keď tak osoba (predovšetkým v pokročilom veku) urobiť jednoducho nedokáže z dôvodu absencie potrebných zručností (napríklad pri používaní aplikácií) alebo jednoducho nechce. Ak Ústavný súd tvrdí, že vedenie motorového vozidla spadá pod základné právo na súkromný život ako nemateriálna hodnota, ktorej každodenný výkon v súčasných podmienkach určuje kvalitu života jednotlivca,²⁹ potom sa neprípustnosť hotovostnej platby za parkovné dokáže v konkrétnych prípadoch prejavovať vo forme tzv. mraziaceho účinku (*chilling effect*), najmä vtedy, keď je alternatíva ťažko dostupná.

Limity ústavodarcu pri potenciálnom vypustení čl. 39a

Samostatný problém vyplývajúci zo zavedenia práva používať hotovosť medzi základné práva predstavuje otázka prípustnosti jeho eventuálneho zrušenia v budúcnosti. Úvahy smerujúce k tomu cieľu sa začali objavovať po ex post stanovisku Európskej centrálnej banky z 11. januára 2024. Podľa nej „v rozsahu, v akom sa v článku 39a ods. 1 a 2 ústavy používa znenie odlišné od jeho normatívnych zdrojov v práve Únie, potenciálne vytvára vlastný regulačný obsah, čo by nebolo v súlade s výlučnou právomocou Únie v oblasti menovej politiky členských štátov, ktorých menou je euro“.³⁰

Európska centrálna banka preto odporučila, aby sa čl. 39a ods. 1 a 2 v častiach zaoberajúcich sa garanciou vydávania hotovosti ako zákonného platidla a práva uskutočňovať platby v hotovosti buď vypustili, prípadne upravili vo forme odkazu na právo EÚ. K vypusteniu by došlo buď cez ústavný zákon, alebo derogačným nálezom ústavného súdu.³¹ Ústava však v čl. 12 ods. 1 druhej vete zakotvuje imperatív nezrušiteľnosti základných práv a slobôd, pričom nepoužíva pojem „základné ľudské práva a slobody“ v zmysle druhého oddielu druhej hlavy ústavy, ale strešný pojem pre celú druhú hlavu. Pod neho patria tiež hospodárske, sociálne a kultúrne práva. Pokiaľ by sa presadil výklad, že imperatív nezrušiteľnosti sa vzťahuje iba na základné práva a slobody z pôvodného textu ústavy, potom by to znamenalo nielen zrušiteľnosť práva používať hotovosť, ale tiež volebného práva cudzincov podľa čl. 30 ods. 1 druhej vety ústavy či práva každého zamestnanca, aby jeho odmena za vykonanú prácu nebola nižšia ako minimálna mzda v zmysle čl. 36 ods. 2 ústavy.³² Alternatíva v

²⁹ Nález sp. zn. PL. ÚS 18/2020 z 25. septembra 2024, 10. bod.

³⁰ Pozri časť 3. 3. z stanoviska Európskej centrálnej banky k ústavnému zákonu o hotovosti ako zákonnom platidle a o prístupe k hotovosti z 11. januára 2024 (CON/2024/1).

³¹ ČELLÁR, Miroslav: Zmeny ústavy vo svetle práva Európskej únie. In: Dvadsať rokov dialógu medzi Ústavou a právom Európskej únie. Zborník príspevkov z konferencie Bratislavské právnické forum 2024. Praha: Wolters Kluwer ČR, a. s., 2024, s. 89.

³² K ich zavedeniu došlo ústavným zákonom č. 90/2001 Z. z., resp. ústavným zákonom č. 99/2019 Z. z.

podobe derogačného nálezu ústavného súdu zase naráža okrem čl. 12 ods. 1 druhej vety aj na čl. 125 ods. 4 druhú vetu ústavy, čiže na zákaz preskúmavania ústavných zákonov.³³ Napokon je vhodné pripomenúť, že zrušenie základného práva orgánom, ktorého ústavným poslaním je základné práva a slobody chrániť, by pôsobilo značne kontroverzne. Iné riešenie tohto problému ponúkol M. Winkler a spočíva napríklad v gramatickom a eurokonformnom výklade čl. 39a ods. 1 ústavy („*textáciu v ZFEÚ v lepšom prípade v rámci kompetencie slovenských autorít dopĺňajú a v horšom reprodujú*“) alebo v použití argumentácie, že čl. 39a ods. 2 ústavy zase predstavuje prípustnú úpravu spôsobu plnenia peňažných povinností v súlade s rozsudkom Súdneho dvora EÚ vo veci *Hessischer Rundfunk*.³⁴

Záver

Právo používať hotovosť, zakotvené s účinnosťou od 1. júla 2023 v čl. 39a Ústavy Slovenskej republiky, je nepochybne nezvyčajnou súčasťou katalógu základných práv a slobôd. Ideové východiská jeho vytvorenia a bezprostredná spätosť so základným právom na ochranu súkromia však dokazujú, že dôvodom pre jeho povýšenie na základné právo bola práve digitalizácia pri používaní platobných prostriedkov. Vychádzajúc z rozhodovacej činnosti Ústavného súdu platí, že po svojom ústavnom zafixovaní má právo používať hotovosť v zmysle čl. 39a konkrétny normatívny dopad, prejavujúci sa okrem iného aj v tom, že je spôsobilé stať sa referenčným kritériom v konaní pred Ústavným súdom, predovšetkým v konaní o súlade právnych predpisov. Právo používať hotovosť je obmedziteľné za splnenia jednotlivých častí testu racionality, pričom prísny test proporcionality sa aplikuje pri zásahu do jadra tohto práva, za súčasnej existencie výnimočných okolností. Pokiaľ všeobecne záväzný právny predpis právo používať hotovosť nerešpektuje nad rámec mantinelov testu racionality alebo proporcionality, potom je z pohľadu dotknutého jednotlivca k dispozícii podnet verejnému ochrancovi práv, ktorý má aktívnu legitimáciu na začatie konania o súlade právnych predpisov v zmysle čl. 130 ods. 1 písm. h) ústavy. Je nám známe, že takýto podnet už bol tomuto ústavnému orgánu doručený práve vo vzťahu k vyššie uvedenému príkladu parkovného bez možnosti jeho úhrady v hotovosti. Zaradenie práva používať hotovosť medzi základné práva a slobody napokon vedie aj k záveru o aplikovateľnosti ústavnej garancie nezrušiteľnosti, ktorá ale môže byť uchopená buď absolútne (nepripustnosť zrušenia)

³³ K extrémnym situáciám, keď si ústavný súd vyhradil právomoc ústavný zákon preskúmať, porovnaj uznesenie sp. zn. PL. ÚS 8/2022 z 25. mája 2022 a k doktrínálnemu chápaniu GIBA, Marián a kol.: Ústavné právo. 2. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2025, s. 295.

³⁴ WINKLER, Martin: Právo na hotovosť z pohľadu slovenského a európskeho práva. In: 15 rokov eura na Slovensku a jeho ďalšie perspektívy. Bratislava: Národná banka Slovenska, 2024, s. 69.

alebo relatívne (prípustnosť zrušenia za rovnakých podmienok ako pri iných základných právach, doplnených do druhej hlavy ex post).

Zoznam použitej literatúry

1. BARROSO, Luís Roberto, ALBERT, Richard (eds.): The 2023 International Review of Constitutional Reform. Austin: Constitutional Studies Program at the University of Texas in collaboration with the International Forum on the Future of Constitutionalism, 2024, 410 s. ISBN 978-1-7374527-6-8.
2. ČELLÁR, Miroslav: Zmeny ústavy vo svetle práva Európskej únie. In: Dvadsať rokov dialógu medzi Ústavou a právom Európskej únie. Zborník príspevkov z konferencie Bratislavské právnické forum 2024. Praha: Wolters Kluwer ČR, a. s., 2024, s. 82 – 90. ISBN 978-80-286-0057-0.
3. ČIČ, Milan a kolektív: Komentár k Ústave Slovenskej republiky. Martin: Matica slovenská, 1997, 598 s. ISBN 80-7090-444-5.
4. EATON, Piers, GASPARD, Valere: A convoy, an emergencies act, and a state of exception: How Canada's Emergencies Act contradicts Carl Schmitt's critiques of deliberative democracy. In: British Journal of Canadian Studies, roč. 36, č. 2, s. 133 – 156.
5. GIBA, Marián a kol. Ústavné právo. 2. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2025, 448 s. ISBN 978-80-571-0746-0.
6. GSTÖTTNER, Susanne, LACHMAYER, Konrad: Austria. In: The 2020 International Review of Constitutional Reform. Austin: Program on Constitutional Studies at the University of Texas in collaboration with the International Forum on the Future of Constitutionalism, 2021, s. 21 – 25. ISBN 978-1-7374527-0-6.
7. KOUDELKA, Zdeněk.: Zústavnění práva na hotovost. In: Právo na nedigitální život. Sborník z kulatého stolu, který proběhl dne 11. února 2025 v Senátu Parlamentu ČR pod záštitou senátního Ústavně-právního výboru. Praha: Nová vlna, 2025, s. 27 - 42. ISBN 978-8053048101.
8. KRIESE, Leo: Central Bank Digital Currency. A Technical, Legal and Economic Analysis. Cham: Springer, 2023, 220 s. ISBN 978-3031447372.
9. MATUŠKA, Peter: Postavenie ústavného súdu pri ochrane ekonomických aspektov ústavného práva. In: Právny obzor, 108, 2025, č. 4, s. 382 - 399.
10. MIERNICKI, Martin: Cash, accounts, and central bank digital currencies: a legal view on the introduction of account- and token-based digital central bank money. In: Law and Financial Markets Review, roč. 17, č. 2, 2023, s. 88 – 115.
11. OROSZ, Ladislav: Listina základných práv a slobôd ako súčasť ústavného systému Slovenskej republiky. In: Listina a súčasnosť. Sborník příspěvků sekce ústavního práva, přednesených na mezinárodní vědecké konferenci Olomoucké

právnické dny 2010. Olomouc: Iuridicum Olomoucense, o. p. s., 2010, s. 151 – 166. ISBN 978-80-87382-31-8.

12. PETRANSKÁ ROLKOVÁ, Natália: Ústava Slovenskej republiky a jej dvadsaťpäť rokov (1992 – 2017). Bratislava: Kancelária Národnej rady Slovenskej republiky, 2017, 408 s. ISBN 978-80-89052-90-5.
13. PONIŠT, Viliam: Porušenie konzultačnej povinnosti s Európskou centrálnou bankou ako relevantný dôvod na podanie ústavnej sťažnosti podľa čl. 127 ods. 5 Ústavy SR? In: Konanie o súlade právnych predpisov – návrhové oprávnenie a účinky rozhodnutí ústavného súdu - XIII. ústavné dni. Košice: Univerzita Pavla Jozefa Šafárika, 2025, s. 172 - 191. ISBN 978-80-574-0413-2.
14. WINKLER, Martin: Právo na hotovosť z pohľadu slovenského a európskeho práva. In: 15 rokov eura na Slovensku a jeho ďalšie perspektívy. Bratislava: Národná banka Slovenska, 2024, s. 55 – 70. ISBN 978-80-8043-262-1.

Kontaktné údaje

Mgr. Vincent Bujňák, PhD.

vincent.bujnak@flaw.uniba.sk

Katedra ústavného práva

Právnická fakulta Univerzity Komenského v Bratislave

JE SPOTREBITEĽ EŠTE SLOBODNÝ VO SVOJOM ROZHODOVANÍ? PRÁVNE DÔSLEDKY DIGITÁLNEHO OVPLYVŇOVANIA

IS THE CONSUMER STILL FREE IN THEIR DECISION-MAKING? LEGAL CONSEQUENCES OF DIGITAL INFLUENCE

Lea Mezeiová¹

Abstrakt: Digitalizácia spotrebiteľských zmluvných vzťahov prináša nový fenomén – neviditeľné ovplyvňovanie rozhodovania spotrebiteľa prostredníctvom algoritmov, personalizovaných ponúk a vopred nastavených zmluvných podmienok, využívajúcich nástroje umelej inteligencie. Predkladaný príspevok skúma, do akej miery je spotrebiteľ slobodný vo svojom rozhodovaní pri uzatváraní digitálnych zmlúv v prostredí riadenom umelou inteligenciou. Analyzuje posun od tradičného vnímania spotrebiteľa ako slabšej zmluvnej strany k jeho chápaniu ako programovanej zmluvnej strany, ktorej autonómia je systematicky narúšaná prostredníctvom manipulatívnych dizajnov a netransparentných algoritmických čiernych skriniek. Pozornosť je venovaná analýze súčasného regulačného rámca EÚ, vrátane smernice Omnibus, GDPR a Aktu o umelej inteligencii. Argumentujeme, že hoci tieto predpisy poskytujú základnú ochranu, ich dôraz na transparentnosť je často nedostatočný na boj proti sofistikovaným formám ovplyvňovania. Pozornosť je venovaná tiež právnym dôsledkom algoritmického ovplyvňovania, ako aj výzvam, ktoré tento vývoj predstavuje pre reguláciu a ochranu spotrebiteľa v digitálnom prostredí.

V závere, ako reakciu na nedostatky súčasnej legislatívy, navrhujeme zavedenie nového, proaktívneho nástroja na posilnenie postavenia spotrebiteľa - práva na nepersonalizáciu.

Kľúčové slová: algoritmické ovplyvňovanie, umelá inteligencia, digitálne zmluvy, zmluvná autonómia, ochrana spotrebiteľa, personalizácia

Abstract: The digitalisation of consumer contractual relationships is giving rise to a new phenomenon: the invisible shaping of consumer decision-making through algorithms, personalised offers, and pre-set contractual terms powered by artificial intelligence. This paper examines the extent to which a

¹ Univerzita Komenského v Bratislave, Právnická fakulta

consumer is free in their decision-making when concluding digital contracts in an AI-driven environment. It analyses the shift from the traditional perception of the consumer as the 'weaker party' to their understanding as a 'programmed party,' whose autonomy is systematically eroded by manipulative designs and non-transparent algorithmic black boxes. Attention is focused on an analysis of the current EU regulatory framework, including the Omnibus Directive, GDPR, and the AI Act. We argue that while these regulations provide a foundational layer of protection, their emphasis on transparency is often insufficient to combat sophisticated forms of influence. The paper also addresses the legal consequences of algorithmic influence and the challenges this development poses for regulation and consumer protection in the digital environment. In conclusion, as a response to the shortcomings of current legislation, we propose the introduction of a new, proactive tool to empower the consumer - the right to non-personalisation.

Key words: algorithmic influence, artificial intelligence, digital contracts, contractual autonomy, consumer protection, personalisation

Úvod

Ochrana spotrebiteľa je nepochybne v centre záujmu jednotlivých štátov, ako aj samotnej EÚ. Význam politiky ochrany spotrebiteľa nadobúda osobitnú relevanciu predovšetkým v kontexte súkromnoprávných vzťahov, v ktorých dochádza k stretu viacerých právnych poriadkov súčasne². Spotrebiteľ je v týchto vzťahoch vnímaný ako slabšia zmluvná strana, ktorej postavenie je neraz determinované informačnou, či ekonomickou asymetriou. Právo EÚ z dôvody zvýšenej ochrany slabšej zmluvnej strany postupne vybudovalo komplexný systém právnej ochrany, ktorého cieľom je zabezpečiť vysokú úroveň ochrany spotrebiteľa. Významné míľniky v oblasti ochrany spotrebiteľa reagovali na vznikajúce výzvy v spotrebiteľskej politike. Je totiž nepochybné, že oblasť ochrany spotrebiteľa patrí medzi mimoriadne dynamické oblasti.

Spotrebiteľské právo musí reagovať na výzvy plynúce z rýchleho technologického pokroku a digitalizácie. Výzvy, ktoré prináša digitalizácia, ako napríklad automatizované rozhodovanie, personalizovaná cenotvorba a ponuka, či iné využívanie systémov umelej inteligencie (ďalej aj ako "AI") v zmluvných vzťahoch, si vyžadujú nielen efektívne legislatívne nástroje ochrany spotrebiteľa, ale aj proaktívny prístup k posilneniu postavenia spotrebiteľa.

² LYSINA, P.: Kolízne normy v digitálnom veku: výzvy pre slovenské medzinárodné právo súkromné. In: Acta Facultatis Iuridicae Universitatis Comenianae, roč. 44, č. 1 2025, s. 70

Jedným z aktuálnych cieľov EÚ je bezpečná a udržateľná digitálna transformácia, ktorej stredobodom pozornosti sú ľudia a dodržiavanie základných hodnôt a práv EÚ. Digitálnu transformáciu usmerňuje politický program Digitálne desaťročie³ a Európska deklarácia o digitálnych právach a zásadách⁴, pričom cieľom je vytvoriť spravodlivé online prostredie, v ktorom by bol vplyv digitálnych technológií prínosom pre všetkých a nenarúšal by online práva jednotlivcov, teda aj spotrebiteľov.

V kontexte cieľov stratégie digitálneho desaťročia Európy o spravodlivom online prostredí, je otázne, či je naozaj zabezpečená primeraná ochrana spotrebiteľa v online prostredí a či dokáže čeliť nástrahám digitálneho prostredia. V spotrebiteľských právnych vzťahoch je vo svetle autonómie vôle zmluvných strán umožnená voľba právomoci súdu, ako aj voľba rozhodného práva. Je však autonómia spotrebiteľa skutočne reflektovaná aj v podmienkach neviditeľného ovplyvňovania jeho rozhodovania prostredníctvom algoritmov, personalizovaných ponúk a vopred nastavených zmluvných podmienok, využívajúcich nástroje umelej inteligencie?

V kontexte uvedeného sa predkladaný príspevok zameriava na právne dôsledky algoritmického ovplyvňovania, ako aj výzvy, ktoré so sebou digitalizácia prináša pre reguláciu a ochranu spotrebiteľa v online prostredí. V závere príspevok navrhuje ako možné, podporné riešenie, zavedenie práva na nepersonalizáciu, ako nástroja na posilnenie postavenia spotrebiteľa v digitálnom prostredí, pri rešpektovaní jeho autonómie vôle.

Spotrebiteľ v digitálnom prostredí

Ochrana spotrebiteľa patrí medzi prioritné ciele na úrovni EÚ. V záujme zabezpečenia dodržiavania hodnôt EÚ a práv jednotlivcov v offline aj online prostredí, prijíma EÚ opatrenia v oblasti podpory základných práv a demokratických hodnôt v digitálnej sfére, ako je nediskriminácia, sloboda prejavu, ochrana osobných údajov a vysoká úroveň ochrany spotrebiteľa. V rýchlom sa vyvíjajúcom digitálnom prostredí sa dáta stali kľúčovým prvkom pre podniky, ktorý poháňa inovácie, rast a predstavuje pre spoločnosti konkurenčnú výhodu⁵. V kontexte ochrany osobných údajov je účelom najmä zabezpečiť účinné a jednotné uplatňovanie pravidiel ochrany údajov v celej EÚ a podporovať spoluprácu medzi orgánmi EÚ na ochranu údajov.⁶

³ European Commission: Directorate-General for Communications Networks, Content and Technology, 2030 Digital Decade – Report on the state of the Digital Decade 2023, Publications Office of the European Union, 2023

⁴ European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01 (OJ C, C/23, 23.01.2023, p. 1

⁵ SCHMUNTZSCH, U., SHAJEK, A., HARTMANN, E. a kol.: New Digital Work II: Digital Sovereignty of Companies and Organizations. Cham: Springer, 2025. s. 58

⁶ BIELIKOVA, M.: Vplyv Európskeho výboru pre ochranu údajov na kreovanie kompetencií a vymožitelnosť práva. In: Právny obzor, roč. 106, č. 5 (2023), s.418

Z aktuálnej správy o stave digitálneho desaťročia je však zrejmé, že EÚ svoje ambiciózne ciele nedosahuje v želanej miere.⁷ EÚ poukázala na rastúcu sofistikovanosť hrozieb, medzi ktoré zaradila okrem dezinformácií, kybernetických útokov, deepfakov, aj algoritmické manipulácie. V súvislosti s týmito hrozbami začala Komisia niekoľko formálnych konaní, napríklad proti poskytovateľom služieb TikTok, Meta, Temu, X a AliExpress, zameraných najmä na nelegálny obsah, ochranu maloletých a algoritmickú transparentnosť. Komisia tiež predstavila oznámenie o elektronickom obchode, ktoré stanovuje sériu prierezových opatrení na zabezpečenie toho, aby tovar predávaný online, napríklad na digitálnych trhoch, a najmä predajcami mimo EÚ, bol v súlade s pravidlami EÚ⁸. S cieľom plne rozvinúť potenciál cezhraničného e-commerce v EÚ je nevyhnutné zvýšiť aj dôveru spotrebiteľov a to posilnením presadzovania ich práv aj v digitálnom prostredí.⁹

V súvislosti s využívaním nástrojov umelej inteligencie je to náročná výzva. Ideálnym stavom by malo byť transparentné digitálne prostredie, v ktorom by spotrebiteľ, robil plne informované a slobodné rozhodnutia. Súčasná realita digitálneho prostredia však tento ideálny stav nereflektuje. Extenzívny zber a algoritmické spracovanie osobných údajov vytvorili informačnú a ekonomickú asymetriu, ktorá umožňuje obchodníkom systematicky ovplyvňovať rozhodovacie procesy spotrebiteľa. Spotrebiteľia sú tak ľahko ovplyvniteľní a manipulovateľní algoritmami, čo má významný vplyv na ich slobodu voľby.¹⁰ Umelá inteligencia sa v súčasnosti profiluje ako významný nástroj pre hlbšiu analýzu spotrebiteľského správania.

Jednou z výrazných oblastí uplatnenia AI je personalizovaný marketing. Technológie založené na AI analyzujú individuálne dáta o spotrebiteľoch a generujú prispôbené odporúčania, ponuky a reklamy. Takto nastavené prístupy sa dokážu dynamicky meniť v reálnom čase v závislosti od aktuálnych preferencií, správania alebo emocionálneho stavu spotrebiteľa, čím sa zvyšuje miera interakcie a miera

⁷ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future, Brussels, 16.6.2025, COM/2025/290 final

⁸ Európska komisia, Oznámenie o elektronickom obchode: Komplexný súbor nástrojov EÚ pre bezpečný a udržateľný elektronický obchod Dostupné na: <https://digital-strategy.ec.europa.eu/en/library/e-commerce-communication-comprehensive-eu-toolbox-safe-and-sustainable-e-commerce>

⁹ LONE, S., WELTEVREDEN, J.W.J.: European E-commerce Report. Amsterdam/Brussels: Amsterdam University of Applied Sciences & Ecommerce Europe. 2023, s. 13

¹⁰ LIU, F., LI, Z.: Consumer interest protection in unfair competition in the digital economy. In: Edelweiss Applied Science and Technology, 2025, roč. 9, č. 3, s. 1176

konverzie¹¹ (t. j. podiel spotrebiteľov, ktorí vykonajú požadovanú akciu, napríklad nákup alebo registráciu).

Pokročilé analytické systémy navyše dokážu spracúvať dáta zo sociálnych sietí, hodnotiť spotrebiteľské nálady a následne upravovať marketingovú komunikáciu. Tento prístup sa označuje ako hyperpersonalizovaný marketing.¹² Zvyšujúca sa miera využívania AI v spotrebiteľských vzťahoch nám otvára zásadné etické, ako aj právne otázky súvisiace napríklad s ochranou osobných údajov, či ovplyvňovaním rozhodovania spotrebiteľa práve vytváraním personalizovanej ponuky, pričom cieľom je usmerňovať rozhodnutia spotrebiteľov smerom k preferovaným možnostiam. Dynamický vývoj AI si podľa nášho názoru žiada predovšetkým transparentnú, spravodlivú a najmä efektívnu právnu reguláciu, ktorá prispeje k ochrane spotrebiteľských práv a bude rešpektovať autonómiu vôle jednotlivcov.

Právny rámec ochrany spotrebiteľa v ére AI

V kontexte voľby právomoci súdu a voľby rozhodného práva v spotrebiteľských zmluvách, pri ktorých dochádza k stretu viacerých právnych poriadkov súčasne, sú relevantné nariadenie Európskeho parlamentu a Rady (EÚ) č. 1215/2012 z 12. decembra 2012 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (prepracované znenie) (ďalej len „nariadenie Brusel Ia“)¹³ a nariadenie Európskeho parlamentu a Rady (ES) č. 593/2008 zo 17. júna 2008 o rozhodnom práve pre zmluvné záväzky (ďalej len „nariadenie Rím I“)¹⁴. Je však potrebné zdôrazniť, že hoci predmetné úijné predpisy čiastočne reflektujú rozmach cezhraničného e-commerce, ani tieto však stále dostatočne nezohľadňujú osobitné požiadavky digitálneho veku.¹⁵

Považujeme za dôležité zdôrazniť, že EÚ reagovala na nové výzvy v oblasti spotrebiteľskej politiky. V posledných rokoch EÚ predstavila niekoľko iniciatív, ktorých cieľom bolo prispôsobiť súčasné právne predpisy zmenám na trhu a rozvoju digitálneho sveta. Jednou z týchto iniciatív bola Nová dohoda pre spotrebiteľov¹⁶,

¹¹ IBRAGIMOV, U. R., TASLIM, M., RAMAN, A. M., ABDUMUTALLIEV, A. U.: The rise of behavioral economics: Leveraging AI to understand consumer decision-making. In: AIP Conference Proceedings, 2025, roč. 3306, č. 1, s. 050007-1

¹² Ibid, s. 050007-1

¹³ MANKOWSKI, P., MAGNUS, U.: European Commentaries on Private International Law ECPII. Volume I Brussels Ibis Regulation. Köln: Verlag Dr. Otto Schmidt, 2022, s.447

¹⁴ ROZEHNALOVÁ, N. a kol. Nařízení Řím I a Nařízení Řím II. Komentář. Praha: Wolters Kluwer ČR, 2021, s. 120

¹⁵ LYSINA, P.: Kolízne normy v digitálnom veku: výzvy pre slovenské medzinárodné právo súkromné. In: Acta Facultatis Iuridicae Universitatis Comenianae, roč. 44, č. 1 2025, s. 71

¹⁶ Oznámenie Komisie Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru: Nová dohoda so spotrebiteľom, COM/2018/183 final

ktorej súčasťou bola aj Smernica 2019/2161¹⁷ známa pod názvom „modernizačná smernica“ alebo „smernica o presadzovaní práva a modernizácii“, alebo „smernica Omnibus“, ktorou sa menili štyri spotrebiteľské smernice.¹⁷ Smernica Omnibus posilnila práva spotrebiteľov prostredníctvom modernizácie pravidiel EÚ na ochranu spotrebiteľa, napr. posilnením opatrení na presadzovanie práva a zvýšením požiadaviek na transparentnosť a zároveň uložením ďalších povinností obchodníkom, ktorí podnikajú online a ponúkajú digitálne služby napr. výmenou za osobné údaje (bezplatné služby). Rozšíril sa tým rozsah pôsobnosti rámca na ochranu spotrebiteľa na digitálny tovar, obsah a služby.

Významným prínosom je skutočnosť, že sa práva na ochranu spotrebiteľa uplatňujú aj v prípade bezplatných služieb. Jedným z dôležitých prvkov, ktorý táto modernizačná smernica priniesla, bola informačná povinnosť predávajúceho pri poskytovaní zliav spotrebiteľom. Ďalším prínosom smernice Omnibus, bolo rozšírenie nekalých obchodných praktík¹⁸ o ďalšie prípady,¹⁹ ktoré súvisia aj s nástrahami digitálneho prostredia. Môžeme konštatovať, že platí všeobecný zákaz nekalých obchodných praktík, ktoré skresľujú ekonomické správanie spotrebiteľov.²⁰ Medzi prípady nekalých obchodných praktík môžeme zaradiť napríklad zavádzanie spotrebiteľov vyhlásením, že hodnotenia (recenzie) pochádzajú od spotrebiteľov, ktorí si reálne tovar zakúpili a používali, pričom však neboli podniknuté náležité kroky smerujúce k overeniu, od koho hodnotenia pochádzajú.

Rovnako za nekalú obchodnú praktiku je považované konanie spočívajúce vo zverejňovaní falošných odporúčaní alebo v poverovaní iných osôb poskytovaním falošných recenzií alebo odporúčaní, prípadne skresľovanie spotrebiteľských recenzií alebo odporúčaní na sociálnych sieťach s cieľom propagovať produkty. Neuverejnenie podstatných informácií pri poradi vo vyhľadávaní produktov je tiež možné považovať za nekalú obchodnú praktiku, pričom za podstatné informácie sa tiež považujú informácie o tom, či sú vyhľadávané produkty medzi prvými v poradí v dôsledku platenej reklamy. Uvedené by malo predchádzať situáciám, kedy obchodník poskytuje spotrebiteľovi v reakcii na jeho vyhľadávanie výsledok bez

¹⁷ Smernica 93/13/EHS, Smernica 98/6/ES, Smernica 2005/29/ES, Smernica 2011/83/EÚ

¹⁸ V zmysle čl. 5 ods. 4 smernice č. 2005/29/ES o nekalých obchodných praktikách sa za nekalé obchodné praktiky považujú najmä tie, ktoré: a) sú klamlivé v zmysle článkov 6 a 7, alebo b) sú agresívne v zmysle článkov 8 a 9.

¹⁹ Príloha I k smernici č. 2005/29/ES o nekalých obchodných praktikách

²⁰ DE ELIZALDE, F.: Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law. In: Journal of Consumer Policy (2025) 48, s. 372

²¹ Rozsudok SDEÚ z 19. decembra 2013, Trento Sviluppo srl, C-281/12, ECLI: ECLI:EU:C:2013:859, bod 32

jasného zverejnenia platenej reklamy alebo inej platby, v ktorej dôsledku je umiestnenie tovaru v poradí výsledkov vyhľadávania vyššie.

V kontexte modernizácie spotrebiteľského práva v digitálnej ére nemôžeme opomenúť komplexný súbor nových pravidiel pre digitálne služby, ako sú sociálne médiá, online trhy a iné online platformy, ktoré pôsobia v EÚ a to akt o digitálnych službách²² a akt o digitálnych trhoch²³, ktoré majú chrániť spotrebiteľov a ich základné práva online. Obe nariadenia majú dva hlavné ciele a to vytvoriť bezpečnejší digitálny priestor, ktorý chráni základné práva všetkých používateľov digitálnych služieb a vytvára rovnaké podmienky na podporu inovácií, rastu a konkurencieschopnosti na európskom jednotnom trhu aj na celom svete. Predmetné regulácie kladú dôraz na online platformy, ktorých hlavnou činnosťou je spracúvanie osobných údajov. To znamená, že pokiaľ ide o osobné údaje, existuje vzájomné prepojenie medzi nimi a všeobecným nariadením o ochrane údajov²⁴ (ďalej aj ako „GDPR“), pričom je vecou práva určiť, ako tieto predpisy vzájomne pôsobia v digitálnom priestore EÚ.²⁵

V súvislosti s regulačným rámcom ochrany spotrebiteľa v ére AI, je nevyhnutné spomenúť, že na pôde EÚ bol prijatý vôbec prvý komplexný právny predpis o umelej inteligencii na svete a to Akt o umelej inteligencii²⁶. Aktom o umelej inteligencii sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie, ktorých cieľom je podporiť dôveryhodnú umelú inteligenciu v Európe. V kontexte ochrany spotrebiteľa môžeme konštatovať, že akt o umelej inteligencii napriek svojej originalite nezavádza žiadnu novú reguláciu mimo už existujúceho rámca ochrany. Dopĺňa a rozširuje záruky stanovené v mnohých odvetviach právnych predpisov EÚ a teda aj v oblasti ochrany spotrebiteľa. Akt o umelej inteligencii zakotvuje, že harmonizované pravidlá, ktoré sa ním zavádzajú, by sa mali uplatňovať vo všetkých odvetviach a v

²² Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách), Ú. v. EÚ L 277, 27.10.2022, s. 1 – 102

²³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťažeschopných a spravodlivých trhoch digitálneho sektora a o zmene smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828 (akt o digitálnych trhoch), Ú. v. EÚ L 265, 12.10.2022, s. 1 – 66

²⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88

²⁵ FARINHO, D. S.: Personal Data Processing of Online Platforms' and Search Engines' Users: The case of the EU Digital Services Act. In: Public Governance, Administration and Finances Law Review, (2024). 9(1), s. 37

²⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii), Ú. v. EÚ L, 2024/1689, 12.7.2024

súlade s novým legislatívnym rámcom by nemali byť dotknuté existujúce právne predpisy Únie, najmä pokiaľ ide o ochranu údajov, ochranu spotrebiteľa, základné práva, zamestnanosť, ochranu pracovníkov a bezpečnosť výrobkov, ktoré sa aktom o umelej inteligencii dopĺňajú.

Systémy AI majú významný vplyv na integritu a dôveru v informačný ekosystém, čo zvyšuje nové riziká mylných informácií a manipulácie alebo ovplyvňovania zvlášť zraniteľných osôb a detí, podvodov, predstierania identity a klamania spotrebiteľov.²⁷ AI sa môže stať aj zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky, ktoré sú mimoriadne škodlivé a zneužívajúce a sú v rozpore s hodnotami Únie. Zákazmi takýchto praktík využívajúcich AI sa dopĺňajú ustanovenia smernice o nekalých obchodných praktikách, najmä to, že nekalé obchodné praktiky vedúce k hospodárskej alebo finančnej ujme pre spotrebiteľov sú zakázané za každých okolností bez ohľadu na to, či sú zavedené prostredníctvom systémov AI alebo inak.²⁸ V tejto súvislosti je potrebné zdôrazniť, že profilovanie má aj svoje legálne vymedzenie. Profilovanie je legálne definované v článku 4 bode 4 GDPR ako „akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybov.“²⁹

Jedným z prípadov, kedy sa spotrebiteľ stretáva so systémom AI, je aj prípad personalizovanej cenotvorby a ponuky. Personalizovanú cenotvorbu možno opísať ako cenovú diferenciáciu za identické produkty alebo služby v rovnakom čase, založenú na informáciách, ktoré obchodník má o potenciálnom zákazníkovi (jeho nákupné správanie, lokalita, zariadenie, čas návštevy alebo predchádzajúce interakcie). Táto prax sa stala možnou vďaka tomu, že obchodníci získali osobné údaje, ktoré oni, respektíve algoritmy, ktoré používajú, môžu spracúvať s cieľom porozumieť osobným preferenciám a nákupným zvyklostiam jednotlivcov.³⁰

²⁷ KRIŠTOFÍK, A.: Využitie (asistenčných) systémov založených na strojovom učení v ODR a ich klasifikácia podľa aktu o umelej inteligencii. Právny obzor, 106, 2023, č. 2, s. 120

²⁸ Bod 29 aktu o umelej inteligencii

²⁹ MESARČÍK, M., GYURÁSZ, Z. a kol.: Právo a umelá inteligencia. 1. Vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 224

³⁰ Európsky parlament. Personalised pricing in the Digital Services Act package: At a glance. Brusel: Výbor pre vnútorný trh a ochranu spotrebiteľa (IMCO), 2022. IPOL_ATA(2022)740060. Dostupné online:

<[https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/740060/IPOL_ATA\(2022\)740060_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/740060/IPOL_ATA(2022)740060_EN.pdf)>

Personalizovaná cenotvorba umožňuje obchodníkom lepšie využiť (odvodenú) ochotu zákazníkov zaplatiť a tým zvýšiť svoje zisky.

V zmysle čl. 6 ods. 1 písm. ea) smernice o právach spotrebiteľov (v znení Omnibus smernice) má obchodník povinnosť spotrebiteľa výslovne informovať, ak cena, ktorú mu zobrazuje, je personalizovaná na základe automatizovaného rozhodovania. Táto informačná povinnosť má zabezpečiť transparentnosť a umožniť spotrebiteľovi rozhodnúť sa, či chce za danú cenu nakupovať, alebo sa rozhodne inak. V praxi však ide o čisto formálnu povinnosť, nakoľko spotrebiteľ síce má byť informovaný, že cena je personalizovaná, avšak nemá právo žiadať zverejnenie algoritmu, na základe ktorého mu bola cena určená a nemá možnosť ovplyvniť, na základe akých údajov sa personalizácia vykonala a nie je nijako chránený pred tým, aby mu bola na základe údajov určená nevýhodná cena.

V prípade, že obchodník neinformuje spotrebiteľa, že mu zobrazuje personalizovanú cenu na základe automatizovaného rozhodovania, dochádza k porušeniu predzmluvnej informačnej povinnosti podľa čl. 6 ods. 1 písm. ea) smernice o právach spotrebiteľov. Podľa nášho názoru to však zároveň môže predstavovať nekalú obchodnú praktiku³¹ v zmysle smernice o nekalých obchodných praktikách.³² Ak obchodník zamlčí skutočnosť, že cena je personalizovaná, ide o opomenutie informácie, ktorá môže mať zásadný vplyv na rozhodnutie spotrebiteľa uskutočniť nákup napríklad z dôvodu, že sa domnieva, že ide o štandardnú cenu, a nie špeciálne určenú pre neho.

Ďalším rizikom je, že personalizované ceny môžu byť selektívne nevýhodné pre niektoré skupiny spotrebiteľov (napr. starších, menej digitálne zdatných, menej informovaných), čo môže viesť ku skrytej diskriminácii, čím sa narúša zásada rovnakého zaobchádzania. Podľa nášho názoru povinnosť obchodníka výslovne informovať spotrebiteľa, ak cena, ktorú mu zobrazuje, je personalizovaná na základe automatizovaného rozhodovania, nepredstavuje ochranu spotrebiteľa pred samotnou personalizáciou ceny, ale jedná sa len o povinnosť upozorniť na jej využitie.

³¹ Čl. 7 ods. 1 smernice o nekalých obchodných praktikách stanovuje, že sa obchodná praktika považuje za klamlivú, ak v skutkovej súvislosti, berúc do úvahy všetky jej črty, okolnosti a obmedzenia komunikačného prostriedku, opomenie podstatnú informáciu, ktorú priemerný spotrebiteľ potrebuje v závislosti od kontextu na to, aby urobil kvalifikované rozhodnutie o obchodnej transakcii, a tým zapríčiňuje alebo môže zapríčiniť, že priemerný spotrebiteľ urobí rozhodnutie o obchodnej transakcii, ktoré by inak neurobil.

³² Čl. 7 ods. 2 smernice o nekalých obchodných praktikách stanovuje, že za klamlivé opomenutie sa taktiež považuje, ak obchodník skrýva alebo poskytuje nejasným, nezrozumiteľným, viacvýznamovým alebo nevhodným spôsobom podstatné informácie uvedené v odseku 1, vzhľadom na okolnosti popísané v uvedenom odseku, alebo neoznámí obchodný účel obchodnej praktiky, ak už nie je zrejmý z kontextu, a tam, kde v jednom alebo druhom prípade toto spôsobí alebo je pravdepodobné, že spôsobí, že priemerný spotrebiteľ prijme rozhodnutie o obchodnej transakcii, ktoré by inak neprijal.

Spotrebiteľ nie je chránený pred ekonomicky nevýhodnou cenotvorbou, pokiaľ je mu táto personalizácia riadne oznámená. Takýto formálny prístup môže byť vnímaný ako nedostatočný z pohľadu reálnej ochrany práv slabšej strany.

Záver

Digitálne infraštruktúry a algoritmy sú často opisované ako „čierna skrinka“. V kontexte digitálnej nespravodlivosti, teda nekalých praktík zo strany online platforiem, je to vždy spotrebiteľ alebo spotrebiteľská organizácia, kto nesie dôkazné bremeno. Bez prístupu k relevantným informáciám sú ich šance preukázať porušenie zákona veľmi nízke, čo predstavuje riziko zníženia úrovne digitálnej spravodlivosti v praxi.³³ Hoci SDEÚ v prelomovom rozsudku³⁴ potvrdil, že spotrebiteľ má podľa čl. 15 ods. 1 písm. h) GDPR právo na "zmysluplné informácie o použitej logike", vymožitelnosť tohto práva v praxi zostáva pre jednotlivca náročná.³⁵

Predkladaný príspevok argumentoval, že systematické ovplyvňovanie autonómie vôle spotrebiteľa prostredníctvom personalizácie a manipulatívnych dizajnov predstavuje jednu z najväčších výziev pre moderné spotrebiteľské právo. EÚ sa snaží na tieto hrozby reagovať a prijala sériu dôležitých právnych predpisov, akými sú napr. smernica Omnibus, Akt o digitálnych službách, Akt o digitálnych trhoch, či Akt o umelej inteligencii. Podľa nášho názoru však budú právne predpisy zaostávať za technologickým pokrokom. Efektívna právna úprava je nevyhnutná a AI je potrebné regulovať, avšak domnievame sa, že samotná právna regulácia nestačí.

Súčasný právny nástroj, zameraný prevažne na transparentnosť, sa ukazuje ako nedostatočný na ochranu pred sofistikovanými formami ovplyvňovania. Na otázku položenú v názve tohto príspevku, teda či je spotrebiteľ ešte slobodný vo svojom rozhodovaní, musíme odpovedať, že jeho autonómia vôle je ohrozená.

Myslíme si, že na dosiahnutie vysokej úrovne ochrany spotrebiteľa v digitálnom prostredí nepostačuje reaktívna právna regulácia, ale je nevyhnutné aktívne posilniť postavenie samotného spotrebiteľa. Možným doplnením existujúceho rámca ochrany spotrebiteľa by mohlo byť zavedenie nového práva, práva na nepersonalizáciu.

Uvedené právo by spotrebiteľovi zaručovalo možnosť jednoduchým a ľahko dostupným spôsobom požiadať o zobrazenie neutrálnej, nepersonalizovanej ponuky a štandardného, nemanipulatívneho užívateľského rozhrania. Právo vnímať digitálny

³³ ROTT, P.: Digital Fairness and the Burden of Proof. In: Journal of Consumer Policy (2025) 48, s.298

³⁴ Rozsudok SDEÚ z 27. februára 2025, Dun & Bradstreet Austria, C-203/22, ECLI:EU:C:2025:117, bod 66

³⁵ SDEÚ v uvedenom prípade rozvinul svoju nedávnu judikatúru týkajúcu sa práv osôb dotknutých profilovaním na účely posúdenia ich bonity, Rozsudok SDEÚ zo 7. decembra 2023, SCHUFA Holding a i. (Scoring) C-634/21, EU:C:2023:957

trh bez algoritmického filtra. Právo na nepersonalizáciu by predstavovalo doplnok k súčasnej právnej úprave. Zavedenie tohto práva by posilnilo nielen skutočnú autonómiu vôle spotrebiteľa v digitálnom prostredí, ale aktívne by prispelo k posilneniu digitálnej suverenity jednotlivca.

Zoznam použitej literatúry

1. BIELIKOVÁ, M.: Vplyv Európskeho výboru pre ochranu údajov na kreovanie kompetencií a vymožitelnosť práva. *Právny obzor*, 106, 2023, č. 5, s.416 – 432. <https://doi.org/10.31577/pravnyobzor.2023.5.03>
2. DE ELIZALDE, F.: Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law. In: *Journal of Consumer Policy* (2025) 48, 355–389 (2025). <https://doi.org/10.1007/s10603-025-09584-3>
3. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future, Brussels, 16.6.2025, COM/2025/290 final
4. European Commission: Directorate-General for Communications Networks, Content and Technology, 2030 Digital Decade – Report on the state of the Digital Decade 2023, Publications Office of the European Union, 2023
5. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01 (OJ C, C/23, 23.01.2023)
6. FARINHO, D. S.: Personal Data Processing of Online Platforms' and Search Engines' Users: The case of the EU Digital Services Act. In: *Public Governance, Administration and Finances Law Review*, 9(1), 37–58. <https://doi.org/10.53116/pgafllr.7134>
7. IBRAGIMOV, U. R., TASLIM, M., RAMAN, A. M., ABDUMUTALLIEV, A. U.: The rise of behavioral economics: Leveraging AI to understand consumer decision-making. In: *AIP Conference Proceedings*, 2025, roč. 3306, č. 1, s. 050007-1 – 050007-11. Melville, NY: AIP Publishing. DOI 10.1063/5.0276470. ISBN 978-0-7354-5202-2
8. KRIŠTOFÍK, A.: Využitie (asistenčných) systémov založených na strojovom učení v ODR a ich klasifikácia podľa aktu o umelej inteligencii. *Právny obzor*, 106, 2023, č. 2, s. 116 – 126. <https://doi.org/10.31577/pravnyobzor.2023.2.03>
9. LIU, F., LI, Z.: Consumer interest protection in unfair competition in the digital economy. In: *Edelweiss Applied Science and Technology* 2025, roč. 9, č. 3, s. 1175-1188. ISSN 2576-8484. DOI 10.55214/25768484.v9i3.5445.

10. LONE, Sara – WELTEVREDEN, Jesse W. J.: *European E-commerce Report 2023*. Amsterdam / Brussels: Amsterdam University of Applied Sciences & Ecommerce Europe, 2023. 97 s.
11. LYSINA, P.: Kolízne normy v digitálnom veku: výzvy pre slovenské medzinárodné právo súkromné. In: *Acta Facultatis Iuridicae Universitatis Comenianae*, roč. 44, č. 1 2025, s. 69-94
12. MANKOWSKI, P., MAGNUS, U.: *European Commentaries on Private International Law ECPII. Volume I Brussels Ibis Regulation*. Köln: Verlag Dr. Otto Schmidt, 2022, ISBN 978-3-504-38759-4
13. MESARČÍK, M., GYURÁSZ, Z. a kol.: *Právo a umelá inteligencia*. 1. Vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, ISBN 978-80-7160-715-1, Dostupné online: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/E-KNIHY/Pravo_a_umela_inteligencia_ucebnica_01.pdf
14. Oznámenie Komisie Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru: Nová dohoda so spotrebiteľom, COM/2018/183 final
15. ROTT, P.: Digital Fairness and the Burden of Proof. In: *Journal of Consumer Policy* (2025) 48, 297–314 (2025). <https://doi.org/10.1007/s10603-025-09583-4>
16. ROZEHNALOVÁ, N. a kol. *Nařízení Řím I a Nařízení Řím II. Komentář*. Praha: Wolters Kluwer ČR, 2021, ISBN 978-80-7598-971-0
17. Rozsudok SDEÚ z 27. februára 2025, Dun & Bradstreet Austria, C-203/22, ECLI:EU:C:2025:117
18. Rozsudok SDEÚ z 19. decembra 2013, Trento Sviluppo srl, C-281/12, ECLI: ECLI:EU:C:2013:859
19. Rozsudok SDEÚ zo 7. decembra 2023, SCHUFA Holding a i. (Scoring) C-634/21, EU:C:2023:957
20. SCHMUNTZSCH, U., SHAJEK, A., HARTMANN, E. a kol.: *New Digital Work II: Digital Sovereignty of Companies and Organizations*. Cham: Springer, 2025. 276 s. Online. ISBN 978-3-031-69994-8 (online). DOI 10.1007/978-3-031-69994-8

Kontaktné údaje

JUDr. Lea Mezeiová, PhD.

lea.mezeiova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Katedra medzinárodného práva a medzinárodných vzťahov

OVERENIE VEKU PRI PORNOGRAFII NA INTERNETE: ARGUMENT V PROSPECH VEREJNEJ MORÁLKY¹

AGE VERIFICATION FOR INTERNET PORNOGRAPHY: AN ARGUMENT IN FAVOUR OF PUBLIC MORALITY

Ján Tomašík²

Abstrakt: Tento príspevok sa venuje etickým a právnym aspektom nedávnych legislatívnych opatrení zameraných na obmedzenie prístupu nepľnoletých k pornografickému materiálu na internete. Dostupnosť a flexibilita internetových platforiem v posledných desaťročiach spôsobila nárast konzumácie pornografického materiálu ako aj jeho charakter. Legislatívne telesá v takmer polovici štátov USA a tento rok aj v Spojenom kráľovstve pristúpili k prísnejšej forme implementácie overovania veku. V USA to okrem iného viedlo aj k ukončeniu poskytovania služieb niektorých pornografických platforiem na území daných štátov. Tento článok analyzuje základné parametre tejto legislatívy a reflektuje skeptickú aj podpornú pozíciu k takejto intervencii. Základným argumentom v jej prospech je legitímny verejný záujem na podporovaní takeého morálneho prostredia, ktoré rodičov podporuje v ich povinnosti zabezpečiť svojim deťom vhodnú sexuálnu výchovu. Hoci je teda v princípe takáto legislatíva oprávnená, je nutné venovať pozornosť praktickým otázkam a hodnotovým konfliktom, ktoré môžu jej implementáciu skomplikovať alebo spochybniť jej legitimitu. Stručne bude rozobraný spôsob, akým sa v tomto kontexte vyrovnal Najvyšší súd USA so slobodou prejavu, ako aj problematika ochrany osobných údajov.

Kľúčové slová: overenie veku, pornografia, ochrana detí, bezpečnosť na internete, verejná morálka

Abstract: This article focuses on the ethical and legal aspects of recent legislative measures aimed at restricting minors' access to pornographic material on the internet. The availability and flexibility of internet platforms has led to an increase in the consumption of pornographic material and changed its nature. Legislative bodies in almost half of the US states and, this year, also in

¹ Príspevok je výstupom z grantového projektu VEGA č. 1/0186/24 Náboženské a sekulárne hodnoty v slovenskom práve.

² Katedra teórie práva a filozofie práva, Právnická fakulta, Univerzita Komenského v Bratislave.

the United Kingdom have moved towards a stricter form of age verification. In the US, this has also led to the termination of services provided by some pornographic platforms in the territories of the states concerned. This article analyzes the basic parameters of this legislation and reflects both skeptical and supportive positions on such intervention. The basic argument in its favor is the legitimate public interest in promoting a moral environment that supports parents in their duty to provide their children with appropriate sex education. Although such legislation is justified in principle, attention must be paid to practical issues and value conflicts that may complicate its implementation or call its legitimacy into question. The article briefly discusses how the US Supreme Court has dealt with freedom of expression in this context, as well as the issue of personal data protection.

Key words: age verification, pornography, protection of minors, online safety, public morality

Úvod

V posledných desaťročiach sa zdalo, že zákony týkajúce sa sexuálnej morálky sa stanú právnym tabu. Sexualita má silný aspekt súkromnosti a jej vzťah k verejnému záujmu je preto komplikovaný, hoci sa týka aj základných hodnôt dôležitých pre celú spoločnosť, ako sociálna reprodukcia, ľudská dôstojnosť, a rodinný život. Tiež je zjavné, že v rozličných otázkach súvisiacich so sexualitou široká spoločenská zmluva, a že patria do toho, čo John Rawls nazval rozumnou nezhodou. Aj rozumní ľudia, ako tvrdil, sa na takýchto otázkach nezhodnú, a preto by malo právo a štát ostať v týchto otázkach nezaujaté.³ A aj keď diskurz o týchto otázkach často nedosahuje úroveň sofistikácie Rawlsa a jeho nasledovateľov, všeobecným sentimentom je dať od tejto témy ruky preč.

Toto právne tabu sa však nedávno začalo lámať a súvisí práve s vyvrcholením fenoménu, ktorý naberal na mohutnosti počas posledných dvoch dekád: dostupnosť a šírenie internetovej pornografie. Zatiaľ čo doterajšia regulácia sa efektívne zameriavala predovšetkým na problém detskej pornografie alebo nekonsenzuálnom účinkovaní v pornografických materiáloch, pozornosť sa začína presúvať k ochrane potenciálnych konzumentov, predovšetkým detí. Dvadsaťpäť štátov USA, ako aj Spojené kráľovstvo alebo Francúzsko nedávno pristúpili k sprísneniu podmienok pre vekovú verifikáciu na pornografických stránkach.

V tomto príspevku priblížim kontúry týchto opatrení a odpoviem na vybrané dilemy, ktoré s nimi súvisia. V prvom rade je potrebné venovať sa otázke, či a akú ujmu pôsobí deťom sledovanie pornografie. Rozlišujem tu dve pozície. Skeptická pozícia sa snaží

³ RAWLS, John: Political Liberalism. New York: Columbia University Press, 1996. 576 s.

takpovediac spopulematizovať tento problém a spochybníť, že o problém naozaj ide. Pozícia kritická k pornografii má svoju feministickú a konzervatívnu podobu. Budem tvrdiť, že opatrenia na sprísnenie majú solídny základ v koncepte verejnej morálky a v subsidiárnej povinnosti štátu napomáhať rodičov vo výchove a vzdelaní svojich detí. Na záver posúdim stret tohto verejného záujmu so slobodou prejavu a ochranou osobných údajov a budem tvrdiť, že zákony o vekovej verifikácii požiadavku rozumnej ochrany týchto hodnôt dokážu uspokojiť.

Kontext a podoba verifikačnej legislatívy

Šírenie pornografie na miestach prístupných deťom je protiprávne na celom svete. V zmysle § 372, ods. 1, písm. b) Trestného zákona⁴ by bolo trestné, aby sme na Šafárikovom námestí alebo v električke č. 3 mali pornografický billboard alebo video. Paradoxom súčasnej situácie je, že internetová pornografia je v istom zmysle rozšírenejšia a dostupnejšia ako billboard alebo video v električke. Nie každý jazdí električkou č. 3 alebo prechádza cez Šafárikovo námestie do práce. Ale takmer každý má k dispozícii internet a zariadenie, cez ktoré sa naň môže dostať, prípadne má pri sebe niekoho, kto takúto možnosť má. To platí aj o deťoch.

Správa Komisára pre deti v Anglicku uvádza, že priemerný vek, kedy dieťa prvýkrát uvidí pornografický materiál, je 13 rokov, pričom 10 % mladých ľudí ho uvidí ako 9-ročné alebo mladšie. Správa tiež uvádza, že 79 % detí sa stretlo s násilnou pornografiou pred dovŕšením 18. roku života.⁵ Iná štúdia uvádza, že 20 % detí od 14 do 18 rokov priznáva „návyk“ a 10 % detí priznáva „závislosť“ na pornografii.⁶ Kanadská štúdia odhalila, že priemerný vek prvého kontaktu dieťaťa s pornografiou je 12 rokov, pričom jedna tretina ho má už vo veku 10 rokov.⁷ Podľa prieskumu vykonaného medzi tínedžermi vo veku 13-17 rokov na Slovensku a v Českej republike je priemerný vek prvého kontaktu s pornografiou 11 rokov. Tretina detí sleduje

⁴ § 372 zákona č. 300/2005 Z. z. („Trestný zákon“):

(1) Kto pornografiu

a) ponúka, prenecháva alebo predáva dieťaťu, alebo

b) na mieste, ktoré je deťom prístupné, vystavuje alebo inak sprístupňuje, potrestá sa odňatím slobody až na dva roky.

⁵ CHILDREN'S COMMISSIONER: 'A lot of it is just abuse': Young people and pornography. 2023, s. 5. Dostupné na: <https://assets.childrenscommissioner.gov.uk/wpuploads/2023/02/cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf> (cit. 24.09.2025).

⁶ DIGNIFY.ORG: National Report – Shortened Publication Version. 2023, s. 15. Dostupné na: <https://img1.wsimg.com/blobby/go/9625190e-030a-43c2-8658-061178121cf2/National%20report-%20shortened%20publication%20version.pdf> (cit. 24.09.2025).

⁷ RECOVERY ALBERTA: Fact Sheet: Child & Youth Problematic Online Pornography. 2025. Dostupné na: <https://www.albertahealthservices.ca/assets/info/amh/if-amh-ydt-fact-sheet-child-and-youth-problematic-online-pornography.pdf> (cit. 23.09.2025).

pornografiu 1-krát týždenne alebo častejšie.⁸ Prístup k internetu tu hrá bezpochyby veľkú rolu. V Spojených štátoch malo v roku 2022 smartfón už 95 % tínedžerov,⁹ pričom najväčšia pornostránka Pornhub vo svojej správe uvádza, že až 91 % percent jej premávky tvorí prístup zo smartfónov.¹⁰

Prístup detí k pornografii sa teda v posledných rokoch značne zjednodušil, pričom sa dynamicky vyvíja aj charakter pornografie v porovnaní s jeho modernými časopisovými začiatkami v 20. storočí. Tento technologický a spoločenský vývoj taktiež viedol k tomu, že sa roztvorili nožnice medzi právom na papieri a právom v praxi. Dvanásťročné dieťa si nekúpi erotický časopis alebo film na fyzickom nosiči, ale na pár klikov má k dispozícii takmer nekonečný obsah, často obsahujúci rôznu mieru násilia.

V tomto kontexte sa spomenuté jurisdikcie rozhodli prejsť od módu, ktorý môžeme nazvať vekovým dosvedčením (ang. *age attestation*) – kedy používateľ jednoducho „odklikne“ a dosvedčí, že má 18 rokov – k vekovej verifikácii (ang. *age verification*). Existujú medzi nimi isté rozdiely. Podľa Online Safety Act vo Veľkej Británii (2023, implementácia častí relevantných pre ochranu detí od júla 2025) sa verifikačná povinnosť vzťahuje na všetkých poskytovateľov, ktorí obsah definovaného typu ponúkajú bez určenia hranice podielu. To znamená, že aj niektoré sociálne siete alebo komunikačné aplikácie, na ktorých pornografický obsah predstavuje malú časť celkového obsahu, majú rovnakú verifikačnú povinnosť ako špecificky pornografické stránky. Na druhej strane, americké štáty, ktoré zaviedli vekovú verifikáciu, poväčšine obsahujú klauzulu, podľa ktorej sa verifikačná povinnosť vzťahuje na tých poskytovateľov, ktorých pornografický obsah predstavuje najmenej jednu tretinu celkového obsahu.¹¹

Moderné technológie okrem ľahšieho šírenia umožňujú aj relatívne sofistikované spôsoby identifikácie a verifikácie užívateľa. Britské regulačné teleso Ofcom zodpovedné za implementáciu Online Safety Act uvádza sedem spôsobov, ako je možné verifikovať vek:

- odhad veku analýzou fotografie alebo videa,
- overenie cez bankové údaje,
- digitálne peňaženky alebo iné digitálne identifikačné služby,
- overenie prostredníctvom kreditnej karty,

⁸ TLAKOVÝ HRNIEC: Sledovanie pornografie: Prieskum medzi deťmi. 2024, s. 5-6. Dostupné na: <https://tlakovyhrniec.sk/wp-content/uploads/2024/09/prieskum-deti-web.pdf> (cit.24.09.2025).

⁹ PEW RESEARCH CENTER: Teens, Social Media and Technology 2022. 2022. Dostupné na: <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/> (cit.24.09.2025).

¹⁰ PORNHUB: 2023 Year in Review. Dostupné na: <https://www.pornhub.com/insights/2023-year-in-review> (cit.25.09.2025).

¹¹ Viď napr. Texas HB 1181 Sec.A129B.002.(a).

- analýza používania e-mailu,
- overenie prostredníctvom mobilného operátora,
- alebo kombinácia snímania tváre a snímania identifikačného dokumentu, napríklad teda občianskeho preukazu.

Ofcom upozorňuje, že takýto spôsob overovania veku je vo Veľkej Británii už bežný pre online nakupovanie alkoholu alebo tabaku.¹² Texaský House Bill 1181, ktorý môžeme z dôvodu litigácie pred Najvyšším súdom USA považovať za paradigmatický prípad americkej verifikačnej legislatívy,¹³ vyžaduje identifikáciu buď oficiálne vydaným identifikačným dokumentom alebo prostredníctvom transakčných údajov.¹⁴

Čo robí pornografiu problematickou

Overenie veku teda predstavuje prelomenie súčasného tabu, ktorým je oddelenie práva a sexuálnej morálky. To prirodzene vyvoláva hodnotové spory. V tejto sekcii najprv stručne charakterizujem to, čo nazývam skeptickým prístupom k regulácii pornografie a ukážem cez feministickú a konzervatívnu kritiku pornografie, že napriek skepse existujú dobré argumenty pre rozumný a vyvážený zásah štátu do tejto oblasti.¹⁵

Skeptický prístup spochybňuje problematickosť prístupu detí k pornografii. Zahra Stardust a kolektív tvrdia, že problematizácia pornografie v skutočnosti zastiera jej potenciál pre zdravý sexuálny vývoj človeka. Samotný pojem ochrany považujú za podozrivý a v skutočnosti zneužiteľný na kontrolu istých skupín obyvateľstva. Explicitný obsah môže byť prostriedkom spoznávania vlastnej sexuality a sexuality vo všeobecnosti, vlastnej identity a príležitosťou pre performáciu sexuality a genderu. Naopak, naratív problematizujúci pornografiu stojí podľa autorov na zastaraných naratívoch o objektivizácii a vzbudzuje atmosféru negativity voči sexu. Obmedzovanie prístupu teda vytvára nezdravú kultúru hanby a malo by byť

¹² OFCOM: Age checks for online safety – what you need to know as a user. 2025. Dostupné na: <https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-for-online-safety--what-you-need-to-know-as-a-user> (cit. 27.09.2025).

¹³ Vid' nižšie.

¹⁴ Texas HB 1181 Sec. 129B.003(b)(1)-(2)(A)-(B)

¹⁵ Pre krátkosť priestoru vynechávam inak zaujímavú debatu o „liberálnom“ prístupe k tejto otázke. Právny teoretik Ronald Dworkin vo svojich prácach priznával negatívne dopady pornografie, ale i tak argumentoval v prospech práva na pornografiu. DWORKIN, Ronald: A Matter of Principle. Cambridge: Harvard University Press, 1986, s. 335-372. Pre kritiku Dworkinovho argumentu pozri GEORGE, Robert: Making Men Moral. Oxford: Clarendon Press, 1993, s. 83-109.

nahradené vzdelávaním.¹⁶ Vzdelávanie sa teda zdá v tejto perspektíve vhodnejším nástrojom pre zabezpečenie sexuálneho vývoja ako reštrikcie.¹⁷

Tento prístup je atraktívny svojím dôrazom na nekoercívne spôsoby vzdelávania, zdôrazňuje medzery a technické nedokonalosti regulácií ako napríklad nespoľahlivosť odhadovania veku podľa fotografie s pomocou AI.¹⁸ Na druhej strane neodpovedá na hlavnú motiváciu vekovej verifikácie, ktorou je spochybnenie toho, do akej miery sú informácie obsiahnuté v pornografickom materiáli vhodné pre deti a ich vývoj. Správna sexuálna výchova je iste potrebná a je jasné, že obmedzenie prístupu k pornografii samotné nezaručuje zdravý rozvoj sexuality. Nedáva však priamu odpoveď na ústredný predpoklad a argument v prospech vekovej verifikácie, teda že sledovanie pornografie maloletými predstavuje škodlivý spôsob, akým „spoznávať vlastnú identitu a sexualitu“. Pozitivita k sexu ako opak neurčitej „negativity“ je taktiež ambivalentná, obzvlášť ak vezmeme do úvahy množstvo štúdií, ktoré poukazujú na negatívne dôsledky pornografie.¹⁹

Principiálna kritika pornografie má dve základné podoby: feministickú a konzervatívnu. Feministická autorka Catherine MacKinnon kritizovala pornografiu, pretože vytvárala ženský objekt pre mužské potešenie: „*V pornografii ženy existujú ako prostriedok k cieľu, ktorým je mužská rozkoš.*“²⁰ Takáto objektifikácia žien nie je nutnou súčasťou ľudskej prirodzenosti, ale dôsledkom vývoja historického vývoja ľudskej sexuality pod vplyvom patriarchátu. Pornografia je variáciou podriadenia žien

¹⁶ STARDUST, Zahra – OBEID, Abdul – McKEE, Alan – ANGUS, Daniel: Mandatory age verification for pornography access: Why it can't and won't 'save the children'. In: Big Data & Society, April–June 2024, s. 12–13.

¹⁷ YAR, Majid: Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. In: Policing: An International Journal, roč. 43, č. 1, 2019, s. 183–197.

¹⁸ Stardust a kolektív podporujú svoje závery analýzou nespoľahlivosti jednej konkrétnej metódy verifikácie veku – rozpoznávania veku AI analýzou fotografie alebo videa. V kontexte, kedy americké zákony takúto možnosť rozpoznávania veku neumožňujú a vo Veľkej Británii táto možnosť predstavuje jednu z ôsmich, nie je možné rozumne uzavrieť, že veková verifikácia je neúčinná alebo nespravodlivá.

¹⁹ Na tomto mieste nie je možné urobiť zadosť veľkému množstvu výskumov, ktoré sa tomuto fenoménu venujú. Odkazujem preto aspoň na niekoľko systematických prehľadov literatúry. OWENS, Eric W. – BEHUN, Richard J. – MANNING, Jill C. – REID, Rory C.: The Impact of Internet Pornography on Adolescents: A Review of the Research. In: Sexual Addiction & Compulsivity, roč. 19, č. 1–2, s. 99–122; PETER, Jochen – VALKENBURG, Pati M.: Adolescents and Pornography: A Review of 20 Years of Research. In: Journal of Sex Research, roč. 54, č. 4–5, 2016, s. 509–531; KANG, Xiaoxi – HANDAYANI, Dini O. D. – CHONG, Pei Pei – ACHARYA, U. Rajendra: Profiling of pornography addiction among children using EEG signals: A systematic literature review. In: Computers in Biology and Medicine, roč. 125, 2020, 13 s.

²⁰ MACKINNON, Catharine: Feminism Unmodified: Discourses on Life and law. Cambridge: Harvard University Press, 1987, s. 158.

mužom. Treba si všimnúť, že tento argument ako taký nezávisí od ďalších dôsledkov. Aj keď produkcia pornografie často zahŕňa vykorisťovanie, obchodovanie s ľuďmi a násilie, argument z objektifikácie tvrdí, že už v samotnom akte produkcie a následnej konzumácie pornografie dochádza k neetickému konaniu. Zákaz pornografie podľa MacKinnon nikomu neupiera sexuálnu slobodu, pretože na takú patologickú formu sexuality nemá nikto nárok.²¹

Pozorné porovnanie konzervatívnej a feministickej kritiky by si vyžadovalo viac priestoru, ale základným prvkom konzervatívnej kritiky je, že je extenzívnejšia. Zatiaľ čo pre feministickú kritiku je objektifikácia žien sociálne a historicky podmienená, konzervatívni kritici sa zhodujú s Immanuelom Kantom v tom, že riziko objektifikácie človeka ako sexuálneho prostriedku je univerzálne.²² Z tohto dôvodu nie sú objektom pornografie len ženy, ale aj muži, ktorí v nich účinkujú, pretože aj ich prítomnosť a akty, ktoré vykonávajú sú len prostriedkom pre sexuálne ciele konzumenta.

Robert George teda tvrdí, že ústredná ujma pornografie nie je v tom, že by urážala alebo šokovala ľudí, podobne ako ústrednou ujmov karcinogénnych plynov v ovzduší nie je to, že smrdia. Voľná dostupnosť pornografie, zvlášť pre deti, spočíva v tom, že zhmotňuje a ďalej reprodukuje vnútornú dispozíciu vnímať druhého človeka ako sexuálny objekt, čo je samo o sebe nesprávne. Navyše, ďalej tým komplikuje a sťažuje vytváranie takej dispozície, či návyku alebo cnosti, ktorá by sexualitu integrovala do ľudskej celistvosti, kedy by nešlo iba o iba jednostranné či vzájomné využívanie.²³

Koncept verejnej morálky či morálnej ekológie potom objasňuje úlohu štátu. Vytváranie prostredia vhodné pre takto integrované prežívanie sexuality spočíva predovšetkým v jednotlivcoch a súkromných inštitúciách, ktoré majú bezprostrednejší vplyv na vonkajšie správanie jednotlivca, no najmä na jeho vnútorné dispozície (rodina, škola, cirkev, občianska spoločnosť). V prípade detí táto primárna zodpovednosť náleží práve rodičom, ktorých zodpovednosť za výchovu a vzdelávanie svojich detí dáva základ ich rodičovským právam. Rodič tak má zodpovednosť a aj právomoc vychovávať *svoje* deti v otázkach sexuality a to aj obmedzením ich prístupu k pornografii. Nemá však právomoc zasahovať do toho, ako sa tejto zodpovednosti zhostujú iní rodičia, hoci zanedbanie tejto zodpovednosti môže znamenať, že cez spolužiakov či kamarátov sa dostane pornografický obsah aj k jeho dieťaťu.

²¹ ŠOLTYS, Dominik: Prí(r)učka právneho feminizmu: Pojem, charakteristika, znaky, vývoj a podoby právneho feminizmu. Košice: Univerzita Pavla Jozefa Šafárika, 2023, s. 225. Krátke zhrnutie k pro-pornografickému prúdu feminizmu pozri tamtiež, s. 191, poznámka pod čiarou č. 609.

²² Pozri KANT, Immanuel: Lectures on Ethics. New York: Harper and Row, 1963, s. 164; a FINNIS, John: Natural Law and Natural Rights. Oxford: Oxford University Press, 2011, s. 217.

²³ GEORGE, Robert P.: The Concept of Public Morality. In: American Journal of Jurisprudence, roč. 40, 2000, s. 17-18.

Právomoc zabezpečiť takýmto spôsobom verejnú morálku má len štát.²⁴ Z toho vyplýva, že štát má subsidiárnu povinnosť napomáhať jednotlivcom a komunitám vytvárať a udržiavať morálne prostredie vhodné pre integrálny ľudský rozvoj.²⁵ Koncept verejnej morálky (alebo mravnosti) zakotvený v Ústave SR,²⁶ ako aj v Európskom dohovore o ľudských právach,²⁷ sa tak ukazuje nie len ako relikv z dôb právneho moralizmu, ale reálny nástroj pre napomáhanie práv a povinností občanov. Je tiež dôležité všimnúť si, že hoci to, čo nazývam konzervatívnou pozíciou, poskytuje dobré argumenty pre verifikačnú legislatívu, tento legislatívny vývoj nemožno jednoznačne prisúdiť len politickým prejavom konzervativizmu či náboženstva. V Texase napríklad prešiel HB 1181 takmer jednohlasne; Online Safety Act vo Veľkej Británii prijala labouristická vláda; opäť iný politicko-ideologický kontext by sme identifikovali vo Francúzsku, ktoré vekovú verifikáciu implementuje od júna 2025.

Verejná morálka verzus sloboda prejavu a ochrana osobných údajov

Kontext, v rámci ktorého sú právne zakotvené odkazy na mravnosť alebo morálku sa týka legitímnych základov pre obmedzenie práv. Tento charakter si na seba berú aj právne spory ohľadom vekovej verifikácie.

Sloboda prejavu hrá v týchto sporoch menšiu rolu, ako by sme mohli predpokladať. Hoci akademická a spoločenská diskusia sa týkajú aj toho, či treba deti pred explicitným sexuálnym obsahom chrániť (viď predchádzajúca sekcia), najvýznamnejší právny spor týkajúci sa vekovej verifikácie sa týkal toho, nakoľko sú týmto krokom obmedzené práva dospelých. Navrhovateľ v prípade *Free Speech Coalition vs. Paxton*, ktorý bol rozhodnutý Najvyšším súdom USA tento rok, poukazoval na neproporčnú záťaž, ktorú nesie dospelý tím, že sa musí podrobiť vekovej verifikácii pri obsahu chránenom prvým dodatkom ústavy. Rozhodnutie záviselo od toho, aký test súd pri zvážení tejto otázky použije. Zatiaľ čo prísny test (*strict test*) by uplatnilo v prípade zákona zameraného priamo na obsah chráneného prejavu, väčšina sudcov v pomere 6:3 sa priklonila k strednému testu (*intermediate test*), pretože podľa ustálenej praxe a precedensu je overovanie veku legitímnym spôsobom ochrany maloletých, ktorý kladie na dospelých iba nepriame (*incidental*) bremeno. Ani aplikácia prísneho testu by však nutne nemusela viesť k zrušeniu

²⁴ GEORGE, Robert: *Making Men Moral*. Oxford: Clarendon Press, 1993, s. 27.

²⁵ TOMAŠTÍK, Ján: Perfectionism as a requirement of justice: natural law, political authority, and the common good. In: *Contemporary Political Theory*, roč. 24, 2025, s. 234-239.

²⁶ V kontexte slobody prejavu a šírenia informácií viď čl. 26 ods. 4 Ústavy SR.

²⁷ Napr. čl. 10 ods. 2 Európskeho dohovoru o ľudských právach.

verifikačných zákonov.²⁸ Texaská legislatíva je podľa Najvyššieho súdu jednoducho aplikáciou tejto praxe na digitálnu dobu.²⁹

Súd nereflektoval, že v dôsledku vekovej verifikácie sa niektoré najväčšie pornografické platformy rozhodli na území daných štátov svoje služby neposkytovať kvôli ochrane osobných údajov.³⁰ Zdá sa teda, že nepriamym dôsledkom zásahu štátu je obmedzená možnosť dospelých ľudí mať prístup k obsahu, ku ktorému by sa pri absencii verifikačnej legislatívy dostať mohli. To však stále samo o sebe nestačí na spochybnenie toho, že takýto zásah je oprávnený alebo proporčný. Distribútor pornografického materiálu mal vždy zákonnú povinnosť zabezpečiť, aby takýto materiál nebol ľahko prístupný deťom. V prípade, že túto povinnosť nedokáže splniť, jedinou legálnou alternatívou je takýto materiál stiahnuť z ponuky. Digitálny priestor sa pre pornografické platformy stal veľkou príležitosťou a až do súčasného momentu nebolo dôsledne vyžadované, aby prevzali aj zodpovednosť, ktorú nesú v súvislosti s ich činnosťou na internete.

Nemožno poprieť, že oproti šíreniu „tradičného“ pornografického materiálu na fyzických nosičoch je ochrana osobných údajov pre overení veku na internete väčším rizikom. Ak však platí, že ochrana verejnej morálky aj prostredníctvom obmedzenia prístupu detí k pornografickému obsahu je legitímnym verejným záujmom a veková verifikácia je vo všeobecnosti primeraným prostriedkom na sledovanie tohto záujmu, toto riziko nepredstavuje pre verifikačnú legislatívu principiálny problém. Opäť sa stáva zodpovednosťou prevádzkovateľa služby, aby zvážil svoje možnosti pri plnení svojich zákonných povinností. V prípade verifikačných zákonov v USA ako aj Veľkej Británii sa počíta so zapojením tretích strán, ktoré poskytujú spôsoby verifikácie a ktoré by osobné dáta spracovávali.³¹ Napriek tomu, že existujú isté kontextuálne rozdiely medzi právnym stavom v predmetných amerických štátoch a Veľkou Britániou, ako aj rozdiely v schválených spôsoboch verifikácie (viď vyššie), nie jasné, prečo pri predpoklade použitia tretích strán pozastavil Pornhub ako najväčšia platforma svoju činnosť v štátoch USA, ale nie vo Veľkej Británii – a či tento stav pretrvá. Štát sa má snažiť, aby jeho legislatíva umožňovala adekvátnu ochranu osobných údajov. Ale aj v prípade, že by nebolo možné pri prístupe k pornografii túto ochranu technicky zabezpečiť, neznamená to nespravodlivosť verifikačnej legislatívy. Možno to znamená iba to, že ak skutočne existuje „právo na pornografiu“,³² dodržiavanie zákonných povinností a sledovanie legitímneho

²⁸ ANDUZE, Daniel: Obscenity Revisited: Defending Recent Age-Verification Laws Against First Amendment Challenges. In: Columbia Journal of Law and Social Problems, roč. 58, č. 1, 2024, s. 154.

²⁹ NAJVVŠŠÍ SÚD SPOJENÝCH ŠTÁTOV: Free Speech Coalition, Inc. v. Paxton, s. 1-4.

³⁰ PORNHUB: Age Verification in the US. 2025. Dostupné na: <https://www.pornhub.com/blog/age-verification-in-the-news> (cit.26.09.2025).

³¹ Texas HB 1181 Sec. 129B.003(b)(2); Online Safety Act 2023, Explanatory Notes, Sec. 230, 943.

³² Debatu k tomu viď napr. v odkazoch v poznámke pod čiarou č. 15.

verejného záujmu by si vyžadovalo návrat k „tradičným“ fyzickým nosičom, kde je overenie veku jednoduchšie a riziko zneužitia osobných údajov takmer nulové.

Záver

V tomto príspevku som analyzoval základné prvky nového právneho fenoménu, ktorým je veková verifikácia pri prístupe k internetovej pornografii. Obzvlášť som sa venoval variáciám tejto legislatívy v USA a Veľkej Británii. Tvrdím, že prostredníctvom tohto fenoménu sa do právneho myslenia vracia relevancia inak zaznávaného pojmu verejnej morálky či mravnosti, za ktorú má subsidiárnu (teda pomocnú) zodpovednosť aj štát. Ochrana detí a mladistvých pred pornografickým obsahom predstavuje legitímny verejný záujem, ktorý je v dôsledku rozmachu internetovej pornografie adaptovať na digitálne prostredie. Hoci sú otázky ohľadom slobody prejavu a ochrany osobných údajov relevantné, správne nastavená legislatíva môže konflikty týchto hodnôt uspokojivo vyriešiť. Slovenská republika má benefit sledovať skúsenosti a implementáciu vekovej verifikácie v iných krajinách, mala by si ich osvojiť a príklad USA, Veľkej Británie a ďalších rozumným spôsobom nasledovať.

Zoznam použitej literatúry

1. ANDUZE, Daniel: Obscenity Revisited: Defending Recent Age-Verification Laws Against First Amendment Challenges. In: Columbia Journal of Law and Social Problems, roč. 58, č. 1, 2024, s. 147-192
2. CHILDREN'S COMMISSIONER: 'A lot of it is just abuse': Young people and pornography. 2023. Dostupné na: <https://assets.childrenscommissioner.gov.uk/wpuploads/2023/02/cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf> (cit.24.09.2025)
3. DIGNIFY.ORG: National Report – Shortened Publication Version. 2023. Dostupné na: <https://img1.wsimg.com/blobby/go/9625190e-030a-43c2-8658-061178121cf2/National%20report-%20shortened%20publication%20version.pdf> (cit.24.09.2025)
4. DWORKIN, Ronald: A Matter of Principle. Cambridge: Harvard University Press, 1986. 425 s. ISBN 9780674554610
5. FINNIS, John: Natural Law and Natural Rights. Oxford: Oxford University Press, 2011. 481 s. ISBN 978-0-19-959914-1
6. GEORGE, Robert P.: Making Men Moral. Oxford: Clarendon Press, 1993. 241 s. ISBN 0-19-825424-5
7. GEORGE, Robert P.: The Concept of Public Morality. In: American Journal of Jurisprudence, roč. 40, 2000, s. 17-32

8. KANT, Immanuel: Lectures on Ethics. New York: Harper and Row, 1963. 253 s. ISBN 0061301051
9. MACKINNON, Catharine: Feminism Unmodified: Discourses on Life and law. Cambridge: Harvard University Press, 1987. 315 s. ISBN 9780674298741
10. NAJVYŠŠÍ SÚD SPOJENÝCH ŠTÁTOV: Free Speech Coalition, Inc. v. Paxton
11. OFCOM: Age checks for online safety – what you need to know as a user. 2025. Dostupné na: <https://www.ofcom.org.uk/online-safety/protecting-children/age-checks-for-online-safety--what-you-need-to-know-as-a-user> (cit.27.09.2025)
12. OWENS, Eric W. – BEHUN, Richard J. – MANNING, Jill C. – REID, Rory C.: The Impact of Internet Pornography on Adolescents: A Review of the Research. In: Sexual Addiction & Compulsivity, roč. 19, č. 1–2, 2012, s. 99–122
13. PETER, Jochen – VALKENBURG, Pati M.: Adolescents and Pornography: A Review of 20 Years of Research. In: Journal of Sex Research, roč. 54, č. 4-5, 2016, s. 509-531
14. KANG, Xiaoxi – HANDAYANI, Dini O. D. - CHONG, Pei Pei – ACHARYA, U. Rajendra: Profiling of pornography addiction among children using EEG signals: A systematic literature review. In: Computers in Biology and Medicine, roč. 125, 2020, 13 s
15. PEW RESEARCH CENTER: Teens, Social Media and Technology 2022. 2022. Dostupné na: <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/> (cit.24.09.2025)
16. PORNHUB: 2023 Year in Review. Dostupné na: <https://www.pornhub.com/insights/2023-year-in-review> (cit.25.09.2025)
17. PORNHUB: Age Verification in the US. 2025. Dostupné na: <https://www.pornhub.com/blog/age-verification-in-the-news> (cit.26.09.2025)
18. RAWLS, John: Political Liberalism. New York: Columbia University Press, 1996. 576 s. ISBN 0-231-05249-9
19. RECOVERY ALBERTA: Fact Sheet: Child & Youth Problematic Online Pornography. 2025. Dostupné na: <https://www.albertahealthservices.ca/assets/info/amh/if-amh-ydt-fact-sheet-child-and-youth-problematic-online-pornography.pdf> (cit.23.09.2025)
20. STARDUST, Zahra – OBEID, Abdul – McKEE, Alan – ANGUS, Daniel: Mandatory age verification for pornography access: Why it can't and won't 'save the children'. In: Big Data & Society, April–June, 2024, s. 1-17
21. ŠOLTYS, Dominik: Prí(r)učka právneho feminizmu: Pojem, charakteristika, znaky, vývoj a podoby právneho feminizmu. Košice: Univerzita Pavla Jozefa Šafárika, 2023. 533 s. ISBN 978-80-574-0184-1
22. TLAKOVÝ HRNIEC: Sledovanie pornografie: Prieskum medzi deťmi. 2024, 27 s. Dostupné na: <https://tlakovyhrniec.sk/wp-content/uploads/2024/09/prieskum-deti-web.pdf> (cit.24.09.2025)

23. TOMAŠTÍK, Ján: Perfectionism as a requirement of justice: natural law, political authority, and the common good. In: *Contemporary Political Theory*, roč. 24, 2025, s. 226–244
24. YAR, Majid: Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. In: *Policing: An International Journal*, roč. 43, č. 1, 2019, s. 183-197

Kontaktné údaje

Mgr. Ján Tomašík, PhD.
jan.tomastik@flaw.uniba.sk
Katedra teórie práva a filozofie práva
Právnická fakulta
Univerzita Komenského v Bratislave

BALANSOVANIE MEDZI DISCIPLINÁRNOU ZODPOVEDNOSŤOU A NEZÁVISLOSŤOU SUDCOV V KONTEXTE POĽSKA A SLOVENSKA¹

BALANCING DISCIPLINARY LIABILITY AND JUDICIAL INDEPENDENCE IN THE CONTEXT OF POLAND AND SLOVAKIA

Ema Mikulová²

Abstrakt: Poľsko od roku 2015 s novou vládou započalo zmeny v súdnictve, ktoré negatívne ovplyvnili nezávislosť sudcov. Tieto zmeny sa prejavili aj v rámci vyvodzovania disciplinárnej zodpovednosti sudcov, symbolicky reprezentované Disciplinárnou komorou, prostredníctvom ktorej sa mala dosiahnuť ich poslušnosť. Na druhú stranu, Slovensko od roku 2021 zaznamenalo inštitucionálnu zmenu, kedy právomoc rozhodovať v disciplinárnych veciach sudcov prešla z disciplinárnych senátov zabezpečovaných Súdnu radou na Najvyšší správny súd SR. Príspevok sa preto zameriava na komparáciu zloženia a kreácie disciplinárnych senátov v Poľsku a na Slovensku. Skúmané obdobie v Poľsku sa viaže na turbulentný vývoj po roku 2015, zatiaľ čo na Slovensku sa pre aktuálnosť komparatívnych poznatkov analyzuje stav od roku 2021. Cieľom príspevku je porovnať, ako tieto dve krajiny balansujú, resp. balansovali medzi disciplinárnou zodpovednosťou a nezávislosťou sudcov na podklade kreácie a zloženia disciplinárnych senátov. Príspevok zároveň poukazuje na poľský komparatívny poznatok v súvislosti s nedávnou novelou v Slovenskej republike v oblasti disciplinárnej zodpovednosti sudcov.

Kľúčové slová: disciplinárna zodpovednosť, súdnictvo, nezávislosť, Poľsko, komparácia, Disciplinárna komora

Abstract: Since 2015, following the advent of a new government, Poland has undertaken reforms in the judiciary that have negatively affected judicial independence. These reforms have also manifested in the sphere of judicial disciplinary liability, symbolically represented by the Disciplinary Chamber, through which judicial compliance was to be ensured. By contrast, since 2021

¹ Tento príspevok vznikol v rámci projektu č. UK/1280/2025 Komparatívna analýza niektorých aspektov disciplinárnej zodpovednosti sudcov Slovenskej a Poľskej republiky.

² Katedra teórie práva a filozofie práva, Univerzita Komenského v Bratislave, Právnická fakulta.

Slovakia has experienced an institutional reform whereby the competence to adjudicate disciplinary matters concerning judges was transferred from disciplinary panels established by the Judicial Council to the Supreme Administrative Court of the Slovak Republic. The paper therefore focuses on a comparative analysis of the composition and establishment of disciplinary panels in Poland and Slovakia. The period under review in Poland relates to the turbulent developments after 2015, whereas in Slovakia the analysis covers the situation from 2021, in order to ensure the contemporary relevance of the comparative findings. The objective of the paper is to examine how these two countries have balanced in the past, and how they currently balance, judicial disciplinary liability with judicial independence through the lens of the creation and composition of disciplinary panels. The paper also highlights the Polish comparative insight in connection with the recent legal amendments in Slovakia concerning judicial disciplinary liability.

Key words: disciplinary liability, judiciary, independence, Poland, comparative analysis, Disciplinary Chamber

Úvod

V rámci rozšírenia Európskej Únie v roku 2004 sa medzi členské štáty pridali aj Poľsko a Slovensko. Pred prístupom obe krajiny absolvovali prístupové rokovania, súčasťou ktorých bola, prirodzene, aj požiadavka zosúladiť stav právneho štátu so štandardmi stanovenými EÚ.³ Od nadobudnutia členstva v EÚ však obe tieto krajiny stredoeurópskeho priestoru prešli rôzne cesty. Poľsko od roku 2015 s novou vládou započalo aj neslávne známe zmeny v rámci súdnictva, ktoré ovplyvnili stav nezávislosti sudcov prakticky dodnes. Tieto zmeny sa prejavili aj v rámci disciplinárnej zodpovednosti sudcov, vďaka ktorým sa mala dosiahnuť poslušnosť sudcov v novej klíme v rámci súdnictva.⁴ Na druhú stranu, Slovensko od roku 2021 zaznamenalo inštitucionálnu zmenu z disciplinárnych senátov zabezpečovaných Súdnou radou na Najvyšší správny súd Slovenskej republiky (ďalej aj len „NSS SR“), ako aj s tým súvisiace zmeny v kreácii a zložení senátov. Od vzniku Najvyššieho správneho súdu sa zásadnejšie zmeny v disciplinovaní sudcov neudiali, no to sa zmenilo v septembri 2025, kedy v parlamente bola schválená novela meniaci podrobnosti zloženia a kreácie disciplinárneho senátu.

³ KNEŽEVIĆ BOJOVIĆ, Ana – ĆORIĆ, VESNA: Challenges of Rule of Law Conditionality in EU Accession. In: Bratislava Law Review, roč. 7, č. 1, 2023, s. 41-42.

⁴ KUSTRA-ROGATKA, Aleksandra: The Hypocrisy of Authoritarian Populism in Poland: Between the Facade Rhetoric of Political Constitutionalism and the Actual Abuse of Apex Courts. In: European Constitutional Law Review, roč. 19, č. 1, 2023, s. 55.

So zreteľom na tieto zmeny sme sa rozhodli položiť si otázku, ktorá je neustále v pozadí tohto príspevku, a to: *„Ako balansovali, resp. balansujú Poľsko a Slovensko medzi disciplinárnou zodpovednosťou a nezávislosťou sudcov?“* Keďže balansovanie medzi týmito „hodnotami“ je ovplyvnené mnohými faktormi, podujali sme sa na skúmanie faktorov, ktoré zásadne vplyvajú na túto krehkú rovnováhu, a to je zloženie a kreácia disciplinárneho senátu. Dôvodom pre skúmanie tak parciálnych súvislostí, ako je spôsob kreácie a zloženia senátu v disciplinárnych veciach je na jednu stranu to, že v zložení senátu sa prejavuje, kto má legitimitu „súdiť“ sudcov.⁵ Zároveň však pri hľadaní ideálneho modelu vyvodzovania ich zodpovednosti je neustále prítomný akýsi „boj“ medzi viacerými hodnotami. Nie je sporným, že sa snažíme udržať sudcov disciplinárne zodpovedných, no zároveň je potrebné systém nastaviť tak, aby nenarážal na limity kladené požiadavkou nezávislosti súdnictva, ako tomu bolo aj v poľskom prípade.

Príspevok sa preto zameriava na komparáciu zloženia a kreácie poľského a slovenského senátu, ktorý rozhodoval a v súčasnosti rozhoduje v disciplinárnych veciach sudcov. Skúmané obdobie v Poľsku je vybrané zámerne na „turbulentné“ obdobie započaté v roku 2015. Súčasný legislatívny stav v Poľsku navyše nie je príliš odlišný, preto nám umožňuje poukázať na negatívne javy súvisiace s novelami prebiehajúcimi od roku 2015, a zároveň predstaviť zmeny, ktorými odvtedy prešiel. Tento stav síce neporovnávame s rovnakým časovým obdobím na Slovensku, ale pre aktuálnosť komparatívnych záverov so stavom účinným v čase písania príspevku, konkrétne od roku 2021, a zároveň analyzujeme aj navrhované zmeny právnej úpravy relevantné v kontexte právneho poriadku Slovenskej republiky. Pre vyhodnotenie a analýzu jednotlivých skutočností (ako súčasných, tak aj potenciálne budúcich) nám preto slúži komparatívny poznatok z Poľska ako dôležitý zdroj poznania.

Disciplinovanie sudcov v Poľsku od roku 2015 a jeho zmeny v čase

Spolu s novou vládou reprezentovanou predovšetkým stranou Prawo i Sprawiedliwość (PiS) sa v roku 2015 započali širšie zmeny v justícii a jej organizácii.⁶ „Režim“, ktorý je predmetom skúmania tohto príspevku, bol účinný od roku 2017,

⁵ GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť sudcov – interpretácia v pripravovaných legislatívnych zmenách alebo úvahy o tom, kto má disciplinárne súdiť sudcov. In: BĀRĀNY, Eduard (ed.): Interpretácia v práve: zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava : Ústav štátu a práva SAV, 2025, s. 259.

⁶ Podstatnou zmenou v roku 2015 bola najmä novela spôsobu obsadenia poľského Ústavného tribunálu. Tento aspekt nebudeme v príspevku bližšie rozoberať, ale je potrebné poznamenať, že zhoršenie stavu justície v Poľsku bolo spôsobené simultánnym pôsobením viacerých noviel a nemožno ich vnímať izolovane. Viac na: BRZozowski, Wojciech: Can the Constitutional Court Accelerate Democratic Backsliding? Lessons from the Polish Experience. In: BELOV, Martin (ed.): The Role of Courts in Contemporary Legal Orders. The Hague : Eleven International Publishing, 2019, s. 372.

kedy na Najvyššom súde vznikla Disciplinárna komora.⁷ Práve Disciplinárna komora bola jedným z najvypuklejších problémov pre stav právneho štátu v Poľsku a stala sa aj predmetom viacerých konaní pred SDEÚ a ESLP, ktoré spochybnilí jej nezávislosť.⁸ Disciplinárna komora spolu s tzv. „Náhubkovým zákonom“⁹ vznikla ako prostriedok na potrestanie neposlušných sudcov, ktorí neboli ochotní sa podvoliť novým pomerom. Konania so sudcami pred touto komorou zároveň plnili odstrašujúcu funkciu voči ostatným sudcom, ktorí by sa chceli vzoprieť novému *statusu quo*.¹⁰ Dôvodom, prečo považujeme Disciplinárnu komoru za problematickú, je, že jej členmi sa stali úplne noví sudcovia, ktorých zvolila Národná rada súdnictva (poľský ekvivalent Súdnej rady Slovenskej republiky). Kontroverzným je, že z hľadiska zloženia a kreácie tiež neostala nedotknutá zo strany vládnej moci. Národnú radu súdnictva „reštrukturalizovali“ tak, že jej pôvodným členom predčasne ukončili funkčné obdobie a po novele zákona už sudcovských členov na ich miesto volil Sejm.¹¹ Z 25 členov Národnej rady súdnictva tvorí 15 sudcov, ktorí mali byť pôvodne volení sudcovskou samosprávou,¹² ale v dôsledku legislatívnej zmeny presadenej vládnucimi stranami bolo týchto 15 sudcov volených dolnou komorou parlamentu.¹³ Navyše, zvyšných 10 členov Národnej rady súdnictva sú menovaní buď parlamentom, vládou, prezidentom, alebo sú sami aktívnymi politikmi – napr. členom Národnej

⁷ Pozri napr. PECH, Laurent: *Protecting Polish Judges from the Ruling Party's "Star Chamber": The Court of Justice's interim relief order in Commission v Poland (Case C-791/19 R)*. In: *Verfassungsblog*, zverejnené dňa 9. apríla 2020. Dostupné na: <https://verfassungsblog.de/protecting-polish-judges-from-the-ruling-partys-star-chamber/> (cit.22.09.2025).

⁸ Príkladom ich uvádzame nižšie.

⁹ Tzv. „Muzzle law“ zavádzal nové skutkové podstaty disciplinárnych previnení tak, aby zabránil sudcom implementovať závery rozhodnutia SDEÚ v spojených veciach C-585/18, C-643/18 a C-625/18 - A.K. (Nezávislosť disciplinárneho senátu Najvyššieho súdu). Sudcovia v dôsledku tejto právnej úpravy nemohli spochybňovať nezávislosť iných sudcov, či ich vymenovanie do funkcie. Viac na SPIEKER, Luke Dimitrios: *The conflict over the Polish disciplinary regime for judges – an acid test for judicial independence, Union values and the primacy of EU law: Commission v. Poland*. In: *Common Market Law Review*, roč. 59, č. 3, 2022, s. 780.

¹⁰ KUSTRA-ROGATKA, Aleksandra: *The Hypocrisy of Authoritarian Populism in Poland: Between the Facade Rhetoric of Political Constitutionalism and the Actual Abuse of Apex Courts*. In: *European Constitutional Law Review*, roč. 19, č. 1, 2023, s. 55.

¹¹ GAJDA-ROSZCZYŃSKA, Katarzyna - MARKIEWICZ, Krystian: *Disciplinary Proceedings as an Instrument for Breaking the Rule of Law in Poland*. In: *Hague Journal on the Rule of Law*, roč. 12, 2020, s. 458, 459.

¹² MIKULI, Piotr - PACH, Maciej: *Disciplinary liability of judges. The Polish case*. In: MIKULI, Piotr - KUČA, Grzegorz (eds.): *Accountability and the Law. Rights, Authority and Transparency of Public Power*. Abingdon: Routledge, 2022, s. 67.

¹³ SPIEKER, Luke Dimitrios: *The conflict over the Polish disciplinary regime for judges – an acid test for judicial independence, Union values and the primacy of EU law: Commission v. Poland*. In: *Common Market Law Review*, roč. 59, č. 3, 2022, s. 784.

radu súdnictva je podľa ešte stále účinných predpisov aj minister spravodlivosti.¹⁴ Po tomto kontroverznom kroku zo strany poľského parlamentu, teda faktickom ovládnutí orgánu, ktorý má zabezpečovať nezávislosť sudcov parlamentom, bolo z dôvodu nedostatku nezávislosti poľskej Národnej rade súdnictva pozastavené členstvo v Európskej sieti súdnych rád.¹⁵ Vo výsledku teda tieto zmeny znamenali, že na personálne obsadenie novovytvoreného disciplinárneho orgánu sudcov, teda na Disciplinárnu komoru, mal výlučný vplyv orgán, ktorý si už nemohol riadne plniť svoju pôvodne zamýšľanú úlohu, nakoľko ho z veľkej časti ovládal parlament a vládna moc. Pre zistenie zloženia disciplinárneho senátu, ktorý rozhodoval v sudcovských veciach, je potrebné nazrieť na to, ako sa líši v závislosti od zaradenia sudcu na typ súdu, na ktorom pôsobí. Právna úprava tak predpokladá disciplinovanie sudcov všeobecných súdov, sudcov vojenských súdov, sudcov správnych súdov a sudcov Najvyššieho súdu.¹⁶ Považujeme za potrebné podotknúť, že rozhodovanie Disciplinárnej komory sa najviac dotýkalo predovšetkým sudcov všeobecných súdov a sudcov Najvyššieho súdu. Zaujímavým však je, že aj napriek novej vláde sa nastavenie zloženia týchto disciplinárnych senátov od sledovaného obdobia (teda počas existencie Disciplinárnej komory) doteraz nezmenilo.¹⁷ V skúmanom období zákon o organizácii **všeobecných súdov** ustanovuje zloženie disciplinárneho senátu tak, že v prvom stupni sa senát skladal z troch sudcov

¹⁴ Články 7 – 9a zákona o Národnej rade súdnictva z 12. mája 2011 v znení neskorších predpisov (Ustawa z dnia 12 maja 2011 r. o Krajowej Radzie Sądownictwa). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20111260714/U/D20110714Lj.pdf> (cit.27.09.2025).

¹⁵ TILLES, Daniel: Poland becomes first country to be expelled from European judicial network. In: Notes from Poland, zverejnené dňa 29. októbra 2021. Dostupné na: <https://notesfrompoland.com/2021/10/29/poland-becomes-first-country-to-be-expelled-from-european-judicial-network/> (cit.25.09.2025).

¹⁶ V príspevku síce hovoríme o období v minulosti, no v poznámkach pod čiarou citujeme URL prepojenia z účinného znenia jednotlivých zákonov. Je tomu tak preto, že predmetné zákony sa vo veciach zloženia disciplinárneho senátu jednotlivých sudcov od sledovaného obdobia doposiaľ nezmenili a ich znenie sa zhoduje. Porovnaj MIKULI, Piotr - PACH, Maciej: Disciplinary liability of judges. The Polish case. In: MIKULI, Piotr - KUČA, Grzegorz (eds.): Accountability and the Law. Rights, Authority and Transparency of Public Power. Abingdon: Routledge, 2022, s. 71-77.

¹⁷ Keďže od sledovaného obdobia sa znenie zákonov v zložení disciplinárnych senátov nezmenilo (okrem toho, že došlo k nahradeniu Disciplinárnej komory Komorou pre profesnú zodpovednosť), v poznámkach pod čiarou pripájame URL prepojenia na účinné znenie jednotlivých zákonov. Porovnaj MIKULI, Piotr - PACH, Maciej: Disciplinary liability of judges. The Polish case. In: MIKULI, Piotr - KUČA, Grzegorz (eds.): Accountability and the Law. Rights, Authority and Transparency of Public Power. Abingdon: Routledge, 2022, s. 71-77.

disciplinárneho súdu, ktorý organizačne pôsobí pri odvolacom súde.¹⁸ Dejisko odvolacieho konania sa presúva na Najvyšší súd, pričom senát pozostával z dvoch sudcov Disciplinárnej komory a jedného prísediaceho z Najvyššieho súdu.¹⁹ Vo výnimočných prípadoch predpokladaných zákonom mohol rovnaký senát rozhodovať aj v prvoinštančnom konaní.²⁰

Sudcovia **vojenských súdov** sú disciplinovaní analogicky k spôsobu disciplinovania sudcov všeobecných súdov. V prvej inštancii je to opäť trojčlenný senát zložený zo sudcov na vojenskom súde v konkrétnom regióne. Zloženie odvolacieho senátu je rovnaké ako pri sudcoch všeobecných súdov a rovnako platí jurisdikcia druhoinštančného zloženia senátu vo výnimočných prípadoch v prvej inštancii.²¹

Menej spomínanými sú v tomto kontexte **sudcovia správneho súdnictva**,²² no ich disciplinovanie je zaujímavé práve pre výlučnú kompetenciu poľského Najvyššieho správneho súdu, a to v oboch inštanciách – v prvej ide o senát v počte traja sudcovia Najvyššieho správneho súdu, v druhej inštancii rozhodujú siedmi sudcovia.²³

Disciplinárne konanie voči **sudcom Najvyššieho súdu** je koncentrované na Najvyššom súde. V prvej inštancii rozhodoval senát zložený z dvoch sudcov Disciplinárnej komory a z jedného prísediaceho z Najvyššieho súdu.²⁴ V druhej

¹⁸ Čl. 110, § 1 ods. 1 písm. a) zákona o organizácii všeobecných súdov z 27. júla 2001 v znení neskorších predpisov (Ustawa z dnia 27 lipca 2001 r., Prawo o ustroju sądów powszechnych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20010981070/U/D20011070Lj.pdf> (cit.25.09.2025).

¹⁹ Tamže, čl. 110 § 1 ods. 2. Prísediaci podľa poľskej právnej úpravy však predstavujú nie právnický, ale skutočne laický prvok, keďže prísediacim nemôže byť napr. advokát, notár, či osoba zamestnaná na súde. Pozri aj tamže, čl. 159 § 1.

²⁰ Tamže, čl. 110 § 1 ods. 1 písm. b).

²¹ § 39a zákona o organizácii vojenského súdnictva z 21. augusta 1997 v znení neskorších predpisov (Ustawa z dnia 21 sierpnia 1997 r., Prawo o ustroju sądów wojskowych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20020002250/U/D20022250Lj.pdf> (cit.24.09.2025).

²² Pravdepodobne práve pre špecifickú právnu úpravu je disciplinovanie sudcov správneho súdnictva odolnejšie voči politickým tlakom. Pozri MIKULI, Piotr - PACH, Maciej: Disciplinary liability of judges. The Polish case. In: MIKULI, Piotr - KUČA, Grzegorz (eds.): Accountability and the Law. Rights, Authority and Transparency of Public Power. Abingdon: Routledge, 2022, s. 76-77.

²³ Článok 48 § 1 zákona o organizácii správnych súdov z 25. júla 2002 (Ustawa z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021531269/U/D20021269Lj.pdf> (cit.24.09.2025).

²⁴ Článok 73 § 1 ods. 1 zákona o Najvyššom súde z 8. decembra 2017 v znení neskorších predpisov (Ustawa z dnia 8 grudnia 2017 r., o Sądzie Najwyższym). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000005/U/D20180005Lj.pdf> (cit.25.09.2025)

inštancii už ide o päťčlenný senát, opäť s väčšinou sudcov z Disciplinárnej komory (traja členovia) a dvaja prísediaci z Najvyššieho súdu.²⁵

V týchto zloženiach rozhodovali disciplinárne senáty kreované zo sudcov Disciplinárnej komory aj napriek viacerým rozhodnutiam, ktoré konštatovali nedostatok nezávislosti Disciplinárnej komory ako orgánu, ktorý má na starosti disciplinárne súdnictvo.²⁶ Medzi tieto rozhodnutia patrí najmä rozhodnutie o prejudiciálnych otázkach v spojených veciach C-585/18, C-643/18 a C-625/18 - A.K. (*Nezávislosť disciplinárneho senátu Najvyššieho súdu*), v ktorom SDEÚ vytvoril kritériá na posúdenie nezávislosti sudcov a zároveň vyslovil aj svoje pochybnosti o nezávislosti Národnej rady súdnictva, čím spochybnil aj nezávislosť samotnej Disciplinárnej komory.²⁷ V nadväznosti na to rozhodoval poľský Najvyšší súd, ktorý konštatoval, že: „...NRS [Národná rada súdnictva] nie je nezávislá od zákonodarnej a výkonnej moci a tak ani DS NSP [Disciplinárna komora], ktorý NRS kreovala, nespĺňa požiadavky nezávislého a nestranného súdu.“²⁸

Zlom prišiel po súhrnnom pôsobení viacerých sankčných mechanizmov,²⁹ po ktorých PiS prehodnotila svoj doterajší postoj a napokon Disciplinárnu komoru rozpustila. Na prvý pohľad by sa to mohlo, vzhľadom na jej kontroverznosť, javiť ako adekvátne riešenie, problém však bol, že negatívny stav justície bol spôsobený spoločným pôsobením viacerých reforiem, pričom Disciplinárna komora bola len jedným

²⁵ Tamže, čl. 73 § 1 ods. 2.

²⁶ Okrem spomenutého rozhodnutia v texte ide napr. aj o rozhodnutie ESĽP vo veci Reczkowicz proti Poľsku zo dňa 22. júla 2021, č. sťažnosti 43444/19 a rozhodnutie SDEÚ vo veci C-791/19 Komisia proti Poľsku. Viac na KUSTRA-ROGATKA, Aleksandra: The Hypocrisy of Authoritarian Populism in Poland: Between the Facade Rhetoric of Political Constitutionalism and the Actual Abuse of Apex Courts. In: European Constitutional Law Review, roč. 19, č. 1, 2023, s. 47.

²⁷ SPIEKER, Luke Dimitrios: The conflict over the Polish disciplinary regime for judges – an acid test for judicial independence, Union values and the primacy of EU law: Commission v. Poland. In: Common Market Law Review, roč. 59, č. 3, 2022, s. 779.

²⁸ SVÁK, Ján: Medzinárodná ochrana disciplinárne stíhaných sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): Právne a etické aspekty disciplinárnej zodpovednosti sudcov. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 57.

²⁹ Domnievame sa, že zapôsobili práve finančné sankcie – jednak išlo o sankciu 1 000 000 Eur za každý deň, ktorý Poľsko neuposlúchne predbežné opatrenie vydané zo strany SDEÚ, ktorým sa nariaďovalo zastaviť činnosť Disciplinárnej komory (pozri bod 64 uznesenia podpredsedu Súdneho dvora z 27. októbra 2021 vo veci C-205/21 R Komisia proti Poľsku); a zároveň hrozba neuvolnenia finančných prostriedkov z Eurofondov, pozri CEELI Institute: Guidelines on Alternatives to Extraordinary Judicial Vetting. Compendium of CEE Experiences, 2025, s. 64. Dostupné na: <https://ceeliinstitute.org/assets/resources/compendium-of-cee-experiences.pdf> (cit. 24.09.2025). Zaujímavým je, že sankcia 1 000 000 Eur nakoniec uložená nebola, pretože SDEÚ akceptovalo vysvetlenia poľskej vlády. Viac na: SADURSKI, Wojciech: Poland's Constitutional Breakdown. Oxford : Oxford University Press, 2019, s. 209.

článkom reťazca „prehnitého“ systému.³⁰ Na nápravu tohto stavu sa preto vyžadovala komplexná zmena pozostávajúca z viacerých legislatívnych zásahov a nebolo možné očakávať, že postačuje len odstránenie toho najpálčivejšieho problému.

Namiesto Disciplinárnej komory bola (pre ako-také zachovanie kontinuity) vytvorená Komora pre profesnú zodpovednosť. Senáty v sudcovských disciplinárnych veciach boli ponechané v rovnakom zložení, teda legislatíva týkajúca sa pomeru jednotlivých členov senátu sa nezmenila, len namiesto sudcov z Disciplinárnej komory sú vyberaní sudcovia z Komory pre profesnú zodpovednosť. Táto „nová“ komora bola však opäť spochybnená pre jej zloženie, nakoľko jej obsadenie bolo čiastočne vytvorené s participáciou Národnej rady pre súdnictvo, ktorá zmenami v tom čase stále neprešla a jej zloženie bolo aj naďalej pod veľkým vplyvom vlády a parlamentu.³¹ Národnú radu pre súdnictvo sa nová vláda (od konca roku 2023) snažila zreformovať tak, aby prinavrátili stav, kedy jej sudcovských členov volia členovia sudcovskej samosprávy, no pre viaceré politické súvislosti takáto zmena doposiaľ nie je účinná.³²

Súčasný stav disciplinovania sudcov na Slovensku a komparácia s Poľskom

Zásadný posun sa v Slovenskej republike udial v dôsledku legislatívnych zmien vyvodzovania disciplinárnej zodpovednosti sudcov. Zmeny boli viaceré, ale v kontexte tohto príspevku sa javí za podstatné spomenúť jednak zmenu právomoci rozhodovať v disciplinárnych veciach sudcov z disciplinárnych senátov organizačne a technicky zabezpečovaných Súdnou radou na disciplinárne senáty Najvyššieho správneho súdu SR.³³ Spolu s touto zmenou došlo aj k vytvoreniu nového „modelu“

³⁰ Výraz „prehnitý systém“ bol použitý v blogu od Wojciecha Sadurskiego. Pozri SADURSKI, Wojciech: The Disciplinary Chamber May Go – But the Rotten System Will Stay. In: Verfassungsblog, zverejnené dňa 11. augusta 2021. Dostupné na: <https://doi.org/10.17176/20210811-232813-0> (cit. 26.09.2025).

³¹ KUSTRA-ROGATKA, Aleksandra: The Hypocrisy of Authoritarian Populism in Poland: Between the Facade Rhetoric of Political Constitutionalism and the Actual Abuse of Apex Courts. In: European Constitutional Law Review, roč. 19, č. 1, 2023, s. 47-48.

³² Prezydent Duda sa v októbri 2024 pred podpisom týchto zákonov obrátil na Ústavný tribunál na posúdenie ich súladnosti s Ústavou. Viac na TILLES, Daniel: President Duda refers government's constitutional court overhaul to constitutional court. In: Notes from Poland, zverejnené dňa 8. októbra 2024. Dostupné na: <https://notesfrompoland.com/2024/10/08/president-duda-refers-governments-constitutional-court-overhaul-to-constitutional-court/> (cit. 26.09.2025).

³³ GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť ako inštrument nezávislosti profesie. In: METEŇKANYČ, Olexij Mychajlovyč – MAJEROVÁ, Sára – ŤAŽKÁ, Veronika (zost.): Bratislavské právnické fórum 2023 : právna zodpovednosť a autonómia. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023, s. 93; a GAJDOŠOVÁ, Martina: Aktuálne otázky právnych a etických aspektov disciplinárnej zodpovednosti sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): Právne a etické aspekty disciplinárnej zodpovednosti sudcov. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 14.

vyvodzovania disciplinárnej zodpovednosti – tentokrát ide o päťčlenný senát zložený z troch sudcov NSS SR (predseda senátu a sudcovia) a dvoch prísediacich.³⁴ Väčšinu v senáte má teda sudcovský prvok. Prísediaci však nie sú laici, ale právnicki, ktorí nemôžu byť notármi, prokurátormi, súdnymi exekútormi, ani členmi Súdnej rady.³⁵ Musia však spĺňať podmienku aspoň 10-ročnej právnej praxe, čím sa má zabezpečiť profesionalizácia prísediacich v disciplinárnom senáte.³⁶ Sudcovia sú do senátu pridelení podľa rozvrhu práce určenom predsedom NSS, no veci sú jednotlivým senátom pridelené náhodne.³⁷ Prísediaci sú do databázy prísediacich volení Súdnou radou a do senátov sú, opäť, pridelení náhodne.³⁸

Zohľadňujúc doposiaľ uvedené skutočnosti môžeme konštatovať, že súčasný slovenský model vyvodzovania disciplinárnej zodpovednosti je z hľadiska nastavenia zloženia a kreácie disciplinárneho senátu v mnohých aspektoch ekvivalentný tomu poľskému, no nemožno opomenúť poukázanie na podstatné rozdiely.

Pri pohľade akoby z „vtácej perspektívy“ je v oboch právnych poriadkoch v súčasnosti vyvodzovanie disciplinárnej zodpovednosti pevne zasadené do súdnej moci. Potenciálne by to mohlo znamenať aj zvýšenú ochranu pred nenáležitým politickým vplyvom zo strany vládnej a zákonodarnej moci, to bude však vždy záležať od konkrétneho nastavenia vzájomných vzťahov medzi jednotlivými zložkami štátnej moci, čo nemožno badať výlučne len na základe toho, kam zaraďujeme orgán vyvodzujúci disciplinárnu zodpovednosť. V Poľsku je presah politiky do disciplinárnych konaní sudcov väčší práve pre zloženie Národnej rady súdnictva, ktorá kreovala celú Disciplinárnu komoru (neskôr väčšinu Komory pre profesnú zodpovednosť), pretože samotná Národná rada súdnictva bola volená zástupcami zákonodarnej či vládnej moci. Aj u nás je prítomná ingerencia Súdnej rady,³⁹ ale len pri voľbe prísediacich do databázy prísediacich disciplinárneho senátu. Čím sa však odlišuje je, že na Slovensku polovica členov Súdnej rady je tvorená sudcami zvolenými spomedzi seba, vďaka čomu, na rozdiel od Poľska, spĺňa medzinárodné

³⁴ § 5 ods. 1 a 2 zákona č. 432/2021 Z. z. o disciplinárnom poriadku Najvyššieho správneho súdu Slovenskej republiky a o zmene a doplnení niektorých zákonov (disciplinárny súdny poriadok) (ďalej aj len „DSP“).

³⁵ § 10 ods. 4 písm. a) a j) DSP.

³⁶ § 10 ods. 4 písm. g) DSP.

³⁷ § 6 ods. 1 a § 12 ods. 1 DSP.

³⁸ § 6 ods. 4 písm. a) v spojení s § 9 ods. 1 písm. d) DSP.

³⁹ Podľa Európskej siete súdnych rád je jednou z úloh súdnych rád mať istú mieru právomocí vo veciach sudcovskej disciplíny. Pozri ENCJ: Distillation of ECNJ Principles, Recommendations and Guidelines 2004-2017, s. 5. Dostupné na: https://pgwrk-websitemedia.s3.eu-west-1.amazonaws.com/production/pwk-web-encj2017-1/Reports/ENCJ_Distillation_Report_2004_2017.pdf (cit.26.09.2025).

štandardy zloženia súdnych rád.⁴⁰ Nemožno tak konštatovať, že by z pohľadu zloženia na Slovensku existoval funkčný ekvivalent Disciplinárnej komory ako sme ju opisovali v tomto príspevku.

Umiestnenie disciplinárneho konania na najvyššie súdy v rámci súdnej sústavy v oboch krajinách možno interpretovať aj ako snahu o vyjadrenie dôležitosti tohto procesu pre súdnictvo ako také. V Poľsku sa toto však netýka prvostupňového konania pri sudcoch všeobecných a vojenských súdov, pretože v ich veciach rozhodujú disciplinárne súdy pri odvolacích súdoch. Azda možno v tom badať akýsi prvok decentralizácie, ktorý nie je na Slovensku v disciplinárnych konaniach voči sudcom prítomný, nakoľko právomoc rozhodovať má len jediný orgán – Najvyšší správny súd SR. Uvedené neplatí pre predsedu a podpredsedu Najvyššieho súdu SR a predsedu Najvyššieho správneho súdu SR, pre ktorých je v disciplinárnom konaní príslušný Ústavný súd SR.⁴¹

Zloženie disciplinárnych senátov je v Poľsku diferencované jednak podľa zaradenia sudcu na súde, na ktorom pôsobí, ale aj podľa toho, či ide o prvostupňové, alebo odvolacie konanie. U nás takáto diferenciácia senátov podľa zaradenia sudcov v zásade prítomná nie je, okrem už spomenutých výnimiek predsedu a podpredsedu Najvyššieho súdu SR, a predsedu Najvyššieho správneho súdu SR. Vďaka tomuto odlíšeniu môžeme vidieť, že zmeny vo vyvodzovaní disciplinárnej zodpovednosti v Poľsku sa týkali predovšetkým sudcov Najvyššieho súdu, teda vláda sa snažila novelami ovplyvniť najmä vysoko postavených sudcov a zároveň si poistiť priaznivý výsledok odvolacieho konania v prípade sudcov všeobecných súdov a Najvyššieho súdu (keďže tie prebiehali na Najvyššom súde za účasti sudcov Disciplinárnej komory).

Podobnosti z hľadiska zloženia disciplinárneho senátu je pomerne náročné nájsť, no v oboch krajinách je v senáte zachované väčšinové postavenie sudcovského prvku, čo spĺňa štandard judikovaný ESLP o počte sudcov sediacich v disciplinárnom senáte.⁴² Na rozdiel od Poľska u nás doposiaľ nie je odlišné zloženie senátu v prvostupňovom

⁴⁰ Pozri napr. bod IV. Conclusions and recommendations, odporúčanie č. 14 CCJE Opinion No. 24 (2021): Evolution of the Councils for the Judiciary and their role in independent and impartial judicial systems. Dostupné na: <https://rm.coe.int/opinion-no-24-2021-of-the-cjje/1680a47604> (cit.26.09.2025).

⁴¹ Čl. 136 ods. 3 Ústavy Slovenskej republiky č. 460/1992 Zb.

⁴² Pozri najmä bod 109 rozhodnutia ESLP vo veci Volkov proti Ukrajine zo dňa 27. mája 2013, č. sťažnosti 21722/11, ktorý hovorí o aspoň polovičnom zastúpení sudcovského prvku v rámci disciplinárneho senátu. K miere zastúpenia sudcovského prvku v disciplinárnom senáte v slovenských podmienkach pozri MIKULOVÁ, Ema: Oslabenie sudcovského prvku pri vyvodzovaní disciplinárnej zodpovednosti sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): Právne a etické aspekty disciplinárnej zodpovednosti sudcov. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 145-160.

a odvolacom konaní, no schválená novela nám naznačuje, že v prípade jej podpisu prezidentom sa tento rozdiel odstráni a priblížime sa poľskému modelu.

Novela disciplinárnej zodpovednosti sudcov a záverečné úvahy

V slovenskom parlamente bol len pred pár dňami schválený balík noviel zákonov, ktorý môže do budúcnosti zmeniť viaceré aspekty týkajúce sa disciplinárnej zodpovednosti.⁴³ Pre nás je azda najvýraznejšou zmenou zavedenie dvojstupňovosti disciplinárneho konania a s ňou súvisiace zmeny v zložení a kreácii disciplinárnych senátov.

Podľa schváleného zákona má prvostupňový senát byť trojčlenný, pričom pôjde o sudcu NSS SR (predseda senátu), sudcu mimo NSS SR a prísediaceho. Posledných dvoch zmienených členov má podľa novely voliť Súdna rada. Ďalej sa schválilo, aby v odvolacom senáte sedeli dvaja sudcovia NSS SR (predseda a člen senátu), dvaja sudcovia pochádzajúci z prostredia mimo NSS SR a jeden prísediaci, pričom sudcovia mimo NSS SR a prísediaci majú byť opäť volení Súdnu radou SR.⁴⁴

Pri pohľade na nové zloženie disciplinárneho senátu a jeho kreáciu vidíme istý posun – jednak sa „uberá“ z vplyvu sudcov NSS SR, ale dochádza zároveň k posilneniu sudcovského samosprávneho prvku, nakoľko nadobudnú určité zastúpenie aj iní sudcovia, ako sudcovia NSS SR. Oproti momentálne účinnému stavu sa zároveň zvyšuje vplyv Súdnej rady na personálne zloženie disciplinárneho senátu. V súčasnosti má Súdna rada slovo v dvoch pätinách disciplinárneho senátu, po novele by išlo o dve tretiny v prvostupňovom a o tri pätiny v odvolacom senáte. Tento posun znamená, že zo súčasného menšinového slova Súdnej rady na zloženie senátu sa stane väčšinové.

Komparatívny pohľad z Poľska ukazuje, že nastavenie ingerencie súdnych rád do procesu disciplinárneho stíhania sudcov sa v jednotlivých európskych krajinách výrazne líši. Príklad Poľska po roku 2015 zároveň ukazuje, že zmena v kreovaní orgánov vyvodzujúcich disciplinárnu zodpovednosť môže zásadne ovplyvniť nezávislosť justície, ak sa otvorí dvere politickému vplyvu na disciplinárne mechanizmy. Z tohto poznatku vyplýva, že pri akejkoľvek zmene slovenského modelu je potrebné obzvlášť citlivo zvažovať mieru ingerencie iných orgánov, vrátane Súdnej rady, aby nedošlo k narušeniu krehkej rovnováhy medzi

⁴³ Vládný návrh zákona, ktorým sa mení a dopĺňa zákon č. 385/2000 Z. z. o sudcoch a prísediacich a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (IX. volebné obdobie, parlamentná tlač č. 816).

⁴⁴ Prehľad najdôležitejších navrhovaných zmien bol poskytnutý v príspevku GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť sudcov – interpretácia v pripravovaných legislatívnych zmenách alebo úvahy o tom, kto má disciplinárne súdiť sudcov. In: BÁRÁNY, Eduard (ed.): Interpretácia v práve: zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava : Ústav štátu a práva SAV, 2025, s. 249-254.

zodpovednosťou sudcov a ochranou nezávislosti súdnej moci. Na každé takéto opatrenie je nevyhnutné nazerať z hľadiska materiálneho, nie len formálneho, keďže prítomnosť externého prvku v disciplinárnom senáte môže napokon zvýšiť nezávislosť tohto orgánu.⁴⁵

Nastavenie „ideálneho“ zloženia disciplinárneho senátu a jeho kreácie je náročná úloha. Podľa Martiny Gajdošovej *„Odpovedať na otázku – KTO má / môže disciplinovať sudcov? – je vec vyvažovania a zohľadňovania predovšetkým účelu, ktorému má slúžiť, a to k zabezpečeniu spravodlivosti vo vnútri spoločenstva sudcov a k zabezpečeniu nezávislosti sudcu a súdnej moci.“*⁴⁶ Navyše, každá krajina bude mať svoje vlastné ideálne riešenie v závislosti od konkrétnych politických pomerov. Zároveň však vzhľadom na to, že prostredníctvom určitého nastavenia disciplinárnej zodpovednosti možno ľahko dosiahnuť narušenie práv sudcov aj celkovo „zmrazenie“ súdnictva, musíme ku každej novelizácii a zmene pomeru síl pristupovať citlivo. Máme za to, že poľská skúsenosť a aj nadväzujúce rozhodnutia ESLP a SDEÚ nám ukazujú potrebu istej zdržanlivosti. Ak však disciplinárna zodpovednosť prestane slúžiť cieľu znovunastoliť homeostázu v rámci určitej skupiny a stane sa nástrojom tlaku, hrozí nielen oslabenie nezávislosti sudcov, ale aj celkovo stavu právneho štátu.

Zoznam použitej literatúry

1. BRZOZOWSKI, Wojciech: Can the Constitutional Court Accelerate Democratic Backsliding? Lessons from the Polish Experience. In: BELOV, Martin (ed.): The Role of Courts in Contemporary Legal Orders. The Hague : Eleven International Publishing, 2019, s. 371-382. ISBN 978-94-6236-920-7
2. CCJE Opinion No. 24 (2021): Evolution of the Councils for the Judiciary and their role in independent and impartial judicial systems. Dostupné na: <https://rm.coe.int/opinion-no-24-2021-of-the-ccje/1680a47604> (cit.26.09.2025)
3. CEELI Institute: Guidelines on Alternatives to Extraordinary Judicial Vetting. Compendium of CEE Experiences, 2025, s. 64. Dostupné na: <https://ceeliinstitute.org/assets/resources/compendium-of-cee-experiences.pdf> (cit.24.09.2025)
4. ENCJ: Distillation of ECNJ Principles, Recommendations and Guidelines 2004-2017, 26 s. Dostupné na: <https://pgwrk-websitemedia.s3.eu-west->

⁴⁵ MIKULI, Piotr: Judicial Disciplinary Accountability. In: FLINDERS, Matthew – DIMOVA, Gergana – MONAGHAN, Chris (eds.): Understanding Accountability: New Perspectives on a Fractured World. London : Routledge, 2025, s. 224.

⁴⁶ GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť sudcov – interpretácia v pripravovaných legislatívnych zmenách alebo úvahy o tom, kto má disciplinárne súdiť sudcov. In: BÁRÁNY, Eduard (ed.): Interpretácia v práve: zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava : Ústav štátu a práva SAV, 2025, s. 269.

1.amazonaws.com/production/pwk-web-encj2017-p/Reports/ENCJ_Distillation_Report_2004_2017.pdf (cit.26.09.2025)

5. GAJDA-ROSZCZYNIŁSKA, Katarzyna - MARKIEWICZ, Krystian: Disciplinary Proceedings as an Instrument for Breaking the Rule of Law in Poland. In: Hague Journal on the Rule of Law, roč. 12, 2020, s. 451 - 483
6. GAJDOŠOVÁ, Martina: Aktuálne otázky právnych a etických aspektov disciplinárnej zodpovednosti sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): Právne a etické aspekty disciplinárnej zodpovednosti sudcov. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 8-23. ISBN 978-80-7160-739-7
7. GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť ako inštrument nezávislosti profesie. In: METEŇKANYČ, Olexij Mychajlovyč – MAJEROVÁ, Sára – ŤAŽKÁ, Veronika (zost.): Bratislavské právnické fórum 2023 : právna zodpovednosť a autonómia. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023, s. 70-112. ISBN 978-80-7160-704-5
8. GAJDOŠOVÁ, Martina: Disciplinárna zodpovednosť sudcov – interpretácia v pripravovaných legislatívnych zmenách alebo Úvahy o tom, kto má disciplinárne súdiť sudcov. In: BÁRÁNY, Eduard (ed.): Interpretácia v práve: zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava : Ústav štátu a práva SAV, 2025, s. 246-271. ISBN 978-80-9744-875-2
9. KNEŽEVIĆ BOJOVIĆ, Ana – ĆORIĆ, VESNA: Challenges of Rule of Law Conditionality in EU Accession. In: Bratislava Law Review, roč. 7, č. 1, 2023, s. 41-62
10. KUSTRA-ROGATKA, Aleksandra: The Hypocrisy of Authoritarian Populism in Poland: Between the Facade Rhetoric of Political Constitutionalism and the Actual Abuse of Apex Courts. In: European Constitutional Law Review, roč. 19, č. 1, 2023, s. 25-58
11. MIKULI, Piotr - PACH, Maciej: Disciplinary liability of judges. The Polish case. In: MIKULI, Piotr - KUČA, Grzegorz (eds.): Accountability and the Law. Rights, Authority and Transparency of Public Power. Abingdon: Routledge, 2022, s. 63-79. ISBN 9780367767358
12. MIKULI, Piotr: Judicial Disciplinary Accountability. In: FLINDERS, Matthew – DIMOVA, Gergana – MONAGHAN, Chris (eds.): Understanding Accountability: New Perspectives on a Fractured World. London : Routledge, 2025, s. 211-228. ISBN 9781032588483
13. MIKULOVÁ, Ema: Oslabenie sudcovského prvku pri vyvodzovaní disciplinárnej zodpovednosti sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): Právne a etické aspekty disciplinárnej zodpovednosti sudcov. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 145-160. ISBN 978-80-7160-739-7

14. PECH, Laurent: Protecting Polish Judges from the Ruling Party's "Star Chamber": The Court of Justice's interim relief order in *Commission v Poland* (Case C-791/19 R). In: *Verfassungsblog*, zverejnené dňa 9. apríla 2020. Dostupné na: <https://verfassungsblog.de/protecting-polish-judges-from-the-ruling-partys-star-chamber/> (cit.22.09.2025)
15. Rozhodnutie ESLP vo veci *Reczkowicz* proti Poľsku zo dňa 22. júla 2021, č. sťažnosti 434447/19
16. Rozhodnutie ESLP vo veci *Volkov* proti Ukrajine zo dňa 27. mája 2013, č. sťažnosti 21722/11
17. Rozhodnutie SDEÚ v spojených veciach C-585/18, C-643/18 a C-625/18 - A.K. (Nezávislosť disciplinárneho senátu Najvyššieho súdu)
18. Rozhodnutie SDEÚ vo veci C-791/19 Komisia proti Poľsku
19. SADURSKI, Wojciech: *Poland's Constitutional Breakdown*. Oxford : Oxford University Press, 2019, 289 s. ISBN 978- 0- 19- 884050- 3
20. SADURSKI, Wojciech: The Disciplinary Chamber May Go – But the Rotten System Will Stay. In: *Verfassungsblog*, zverejnené dňa 11.8.2021. Dostupné na: <https://doi.org/10.17176/20210811-232813-0> (cit.26.09.2025)
21. SPIEKER, Luke Dimitrios: The conflict over the Polish disciplinary regime for judges – an acid test for judicial independence, Union values and the primacy of EU law: *Commission v. Poland*. In: *Common Market Law Review*, roč. 59, č. 3, 2022, s. 777-812
22. SVÁK, Ján: Medzinárodná ochrana disciplinárne stíhaných sudcov. In: GAJDOŠOVÁ, Martina - KASINEC, Rudolf (zost.): *Právne a etické aspekty disciplinárnej zodpovednosti sudcov*. Bratislava : Právnická fakulta, Univerzita Komenského v Bratislave, 2024, s. 51-77. ISBN 978-80-7160-739-7
23. TILLES, Daniel: Poland becomes first country to be expelled from European judicial network. In: *Notes from Poland*, zverejnené dňa 29. októbra 2021. Dostupné na: <https://notesfrompoland.com/2021/10/29/poland-becomes-first-country-to-be-expelled-from-european-judicial-network/> (cit.25.09.2025)
24. TILLES, Daniel: President Duda refers government's constitutional court overhaul to constitutional court. In: *Notes from Poland*, zverejnené dňa 8. októbra 2024. Dostupné na: <https://notesfrompoland.com/2024/10/08/president-duda-refers-governments-constitutional-court-overhaul-to-constitutional-court/> (cit.26.09.2025)
25. Ústava Slovenskej republiky č. 460/1992 Zb.
26. Uznesenie podpredsedu Súdneho dvora z 27. októbra 2021 vo veci C-205/21 R Komisia proti Poľsku
27. Vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 385/2000 Z. z. o sudcoch a prísediach a o zmene a doplnení niektorých zákonov v znení neskorších

predpisov a ktorým sa menia a dopĺňajú niektoré zákony (IX. Volebné obdobie, parlamentná tlač č. 816)

28. Zákon č. 432/2021 Z. z. o disciplinárnom poriadku Najvyššieho správneho súdu Slovenskej republiky a o zmene a doplnení niektorých zákonov (disciplinárny súdny poriadok)
29. Zákon o Najvyššom súde z 8. decembra 2017 v znení neskorších predpisov (Ustawa z dnia 8 grudnia 2017 r., o Sądzie Najwyższym). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000005/U/D20180005Lj.pdf> (cit.25.09.2025)
30. Zákon o Národnej rade súdnictva z 12. mája 2011 v znení neskorších predpisov (Ustawa z dnia 12 maja 2011 r. o Krajowej Radzie Sądownictwa). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20111260714/U/D20110714Lj.pdf> (cit.27.09.2025)
31. Zákon o organizácii správnych súdov z 25. júla 2002 (Ustawa z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021531269/U/D20021269Lj.pdf> (cit.24.09.2025)
32. Zákon o organizácii vojenského súdnictva z 21. augusta 1997 v znení neskorších predpisov (Ustawa z dnia 21 sierpnia 1997 r., Prawo o ustroju sądów wojskowych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20220002250/U/D20222250Lj.pdf> (cit.24.09.2025)
33. Zákon o organizácii všeobecných súdov z 27. júla 2001 v znení neskorších predpisov (Ustawa z dnia 27 lipca 2001 r., Prawo o ustroju sądów powszechnych). Dostupné na: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20010981070/U/D20011070Lj.pdf> (cit.25.09.2025)

Kontaktné údaje

Mgr. Ema Mikulová

ema.mikulova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Katedra teórie práva a filozofie práva

ORCID 0009-0009-1155-3122

DIGITÁLNE AKTÍVA V MEDZINÁRODNOM PRÁVE SÚKROMNOM

DIGITAL ASSETS IN PRIVATE INTERNATIONAL LAW

Dominika Juck¹

Abstrakt: Existencia a využívanie digitálnych aktív so sebou prináša aj celý rad nových výziev naprieč medzinárodným právom súkromným, na ktoré musí zákonodarca primerane reflektovať. Pre určenie rozhodného práva pre transakcie, ktorých predmetom sú digitálne aktíva, je nevyhnutné zohľadniť aj možnú väzbu na viacero právnych poriadkov a špecifiká technológie, ktorá ich vytvára a spravuje. Táto komplexnosť si vyžaduje precíznu analýzu platných hmotnoprávnych aj kolíznych noriem, s cieľom posúdiť, do akej miery sú schopné reagovať na technologický vývoj a digitálne aktíva, ktoré sú predmetom transakcií. Príspevok je preto venovaný analýze súčasnej právnej úpravy obsiahnutej v Dohovore OSN o zmluvách o medzinárodnej kúpe tovaru (CISG), ktorý predstavuje hmotnoprávnú úpravu pre medzinárodné kúpne zmluvy, a úpravy nachádzajúcej sa v Nariadení Rím I, ako kľúčovej kolíznej normy určujúcej rozhodné právo pre zmluvné záväzky. Cieľom je identifikovať, do akej miery tieto pramene reflektujú osobitosti digitálnych aktív. Osobitná pozornosť je sústredená na vybrané digitálne aktívum – NFT, tzv. nezameniteľný token.

Kľúčové slová: digitálne aktíva, NFT, medzinárodné právo súkromné, kolízne normy.

Abstract: The existence and use of digital assets bring a wide range of new challenges across private international law, which legislators must adequately address. When determining the applicable law for transactions involving digital assets, it is essential to consider their potential connection to multiple legal systems as well as the specific features of the technology that creates and manages them. This complexity requires a precise analysis of existing substantive and conflict-of-law rules in order to assess the extent to which they are capable of responding to technological developments and to the digital assets that form the subject of transactions. The paper is therefore devoted to

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra medzinárodného práva a medzinárodných vzťahov

an analysis of the current legal framework contained in the United Nations Convention on Contracts for the International Sale of Goods (CISG), which provides the substantive regulation for international sales contracts, and in the Rome I Regulation, which serves as a key conflict-of-law instrument determining the applicable law for contractual obligations. The aim is to identify the extent to which these sources reflect the specific characteristics of digital assets. Special attention is given to a selected type of digital asset—NFTs, so-called non-fungible tokens.

Key words: digital assets, NFT, private international law, conflict of law rules

Úvod

Ak by sme mali stručne opísať najvýraznejšie zmeny, ktoré nastali v 21. storočí, tak je to rozhodne technologický rozvoj. V predkladanom príspevku sa zameriame na jednu konkrétnu oblasť technického rozvoja, ktorou sú digitálne aktíva, t. j. rôzne kryptomeny, digitálne tokeny či non-fungible token (NFT), ktorý by sme do slovenčiny mohli doslovne preložiť ako „*nezameniteľný token*." Nie len hodnota týchto aktív, ale aj frekvencia ich používania sa značne zvýšila v uplynulých rokoch. Cieľom tohto príspevku je preto analyzovať súčasnú právnu úpravu za účelom identifikácie, do akej miery táto reflektuje digitálne aktíva, menovite NFT s väzbou na viacero právnych poriadkov. Za účelom dosiahnutia stanoveného cieľa je potrebné zodpovedať si otázku, čo je možné považovať za digitálne aktívum. Nakoľko predmetom príspevku nie je poskytnúť vyčerpávajúcu analýzu toho, čo je možné považovať za digitálne aktíva, pojmu sa venujeme iba do miery nevyhnutnej pre vykonanie ďalšej analýzy. V ďalšej časti príspevku sa zameriavame na vybrané normy medzinárodného práva súkromného a spôsob akým regulujú existenciu NFT. Sústredíme sa pritom na zmluvy s väzbou na viacero právnych poriadkov, predmetom ktorých je nadobúdanie NFT.

Pojem digitálne aktíva a NFT

V odbornej literatúre ako aj v legislatívnych prameňoch sa stretávame s rôznou definíciou toho, čo je možné považovať za digitálne aktívum. Princípy Unidroit o digitálnych aktívach a súkromnom práve definujú digitálne aktíva ako *elektronický záznam, ktorý môže byť predmetom kontroly*,² pričom možnosť byť predmetom kontroly je potrebné na účely tejto definície chápať ako kontrolu zo strany osoby ako jej schopnosť zabrániť iným osobám aby získali úžitok z tohto aktíva, zároveň schopnosť získať úžitky z predmetného aktíva a môcť previesť obe vyššie uvedené na

² Článok 2 ods. 2 Princípov Unidroit o digitálnych aktívach v súkromnom práve

tretiu osobu.³ Consultation paper vydaný britskou Law Commission považuje digitálne aktíva za tzv. tretiu kategóriu majetku, ktorá môže byť predmetom vlastníckych práv, aj keď nie je v držbe a zároveň nie je nehmotným majetkom,⁴ (pozn. autora: aspoň nie v tradičnom význame). Pre zjednodušenie, medzi digitálne aktíva zaradíme kryptomeny, NFT (non-fungible token), tokeny, avšak zaradíme sem aj tradičnejšie druhy digitálnych aktív ako fotky, videá či ilustrácie. Pre účely predmetného príspevku sa nezameriavame na celú množinu digitálnych aktív, ale rozhodli sme sa našu pozornosť upriamiť iba na jednu kategóriu, a to práve NFT. Napriek tomu, že NFT sa tradične zaradzujú medzi digitálne aktíva, je potrebné podotknúť, že tieto sú skôr predmetom vlastníckeho práva, než platidlom, čo ich odlišuje napr. od kryptomien.⁵

Rozhodné právo

Spoločnosť A, zriadená podľa slovenského práva so sídlom na Slovensku nákup NFT cez digitálnu umeleckú platformu, ktorá je registrovaná v USA. Nákup je zaplatený v kryptomene, pričom NFT je uložené na nezávislej blockchain sieti. Pri určovaní rozhodného práva pre predmetnú transakciu je potrebné rozlišovať rozhodné právo pre samotnú zmluvu, t. j. záväzkovo právny vzťah a podmienky, za ktorých je možné nadobudnúť vlastníckej právo k „veci“, samotnému NFT, teda vecnoprávny vzťah. V rámci tohto príspevku sa zameriavame práve na záväzkovo právne aspekty. Pre záväzkovo právne aspekty je z pohľadu slovenského medzinárodného práva súkromného nevyhnutné analyzovať dva pramene práva a to Dohovor OSN o zmluvách o medzinárodnej kúpe tovaru („CISG“) a Nariadenie Európskeho parlamentu a Rady (ES) č. 593/2008 zo 17. júna 2008 o rozhodnom práve pre zmluvné záväzky („Nariadenie Rím I“).

CISG

V zmysle článku 1 sa CISG aplikuje na zmluvy o kúpe tovaru medzi stranami, ktoré majú miesta podnikania v rôznych štátoch ak sú tieto štáty zmluvnými stranami alebo ak podľa ustanovení medzinárodného práva súkromného sa má použiť právny poriadok niektorého zmluvného štátu.⁶ Smerodajným je pre nás pritom pojem *tovar*

³ Článok 6 ods. 1 Princípov Unidroit o digitálnych aktívach v súkromnom práve

⁴ Law Commission. *Digital assets and (electronic) trade documents in private international law. Consultation paper.* č. 273. 2025. s. 112, 149 a 156. Dostupné na: <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/54/2025/06/Digital-assets-conflicts-CP-2025.pdf.pdf> (cit. 15.09.2025)

⁵ SEMPERE, C., P.: *Governance and Control of Data and Digital Economy in the European Single Market Legal Framework for New Digital Assets, Identities and Data Spaces.* Springer Cham. 2025. s. 8.

⁶ Článok 1 ods. 1 Dohovoru OSN o zmluvách o medzinárodnej kúpe tovaru

a otázka, či je možné NFT považovať za tovar na účely CISG. CISG samotnú definíciu pojmu tovar neobsahuje, preto je potrebné ho vykladať na základe celého textu dohovoru. Právna teória definuje pojem tovar ako pojem zahŕňajúci hnutelné hmotné veci,⁷ pričom to úzko súvisí aj s obdobím, kedy bol dohovor pripravovaný. Už z vyššie uvedeného vyplýva, že NFT nie je možné subsumovať pod predmetnú definíciu, nakoľko nejde o hmotnú vec. V súčasnosti sa však CISG aplikuje na elektronické softwarové transakcie,⁸ ale aj na kúpu rôznych iných digitálnych aktív, ktoré nie sú softvérom: vrátane mediálnych súborov, aplikácií a surových dát.^{9 10} Pri aplikácii CISG s ohľadom na povahu veci v zmysle hmotná / nehmotná je rozhodne potrebné brať do úvahy aj článok 7 CISG vyžaduje široký a autonómny výklad CISG. Hlavným cieľom CISG ako jednotného právneho predpisu je podporovať medzinárodný obchod. Berúc do úvahy potencionálny rozsah transakcií, predmetom ktorých bude nie len NFT, ale aj iný nehmotný tovar, je potrebné dbať na to, aby tieto transakcie pre zmluvné strany prebiehali čo najbezproblémovšie. Jednoznačná uplatniteľnosť CISG na tieto kúpy by rozhodne zvýšila právnu istotu na medzinárodnej úrovni.

Čiastočné negatívne vymedzenie je badateľné v rámci článku 2, negatívne vymedzujúceho tovar z pohľadu jeho účelu (písm. a)), spôsobu nadobudnutia (písm. b) a c)) a povahy veci (písm. d), e) a f)). Za osobitnú zmienku stojí písm. a) predmetného článku, ktoré vylučuje kúpu na osobnú spotrebu. V tomto bode tak môžeme konštatovať, že pokiaľ bude jednou zo strán zmluvy spotrebiteľ, CISG sa na daný záväzkovo právny vzťah aplikovať nebude.

V rámci predmetného článku stojí rozhodne za zmienku aj písm. d), v zmysle ktorého sa CISG nebude aplikovať na kúpy cenných papierov alebo peňazí. Účelom predmetného článku je zabezpečiť aby sa CISG vzťahovalo práve na kúpy tovaru a nie na kúpy práv. Na tomto mieste je rozhodne vhodné zamyslieť sa nad otázkou, či NFT spadá pod výnimku určenú v čl. 2 písm. d) CISG. Cenné papiere je možné podľa CISG vymedziť ako všetky obchodovateľné a speňažiteľné pohľadávky, podiely alebo práva, ktoré môžu byť predmetom kúpnych zmlúv.¹¹ Do tejto kategórie samotné NFT nie je možné zaradiť. Otázkou však ostáva, či je možné na účely článku 2 písm. d)

⁷ Tichý, L. *CISG (Úmluva OSN o smlouvách o mezinárodní koupi zboží)*. C. H. Beck. 1. vydanie 2017. s. 17 - 28

⁸ HAYWARD, B.: *To boldly go, part II: Data as the CISG's next (but probably not final) frontier*. In. *University of New South Wales Law Journal*. Vol 44 (4). 2021. s. 1484

⁹ Tamtiež

¹⁰ K tomuto pozri aj FAUSING KYLKJÆR, K.: *The applicability of the CISG on transactions of software*. s. 13. Dostupné na: https://law.au.dk/fileadmin/Jura/dokumenter/forskning/Rettid/Afh_2019/afh6-2019.pdf (cit. 12.09.2025).

¹¹ Tichý, L. *CISG (Úmluva OSN o smlouvách o mezinárodní koupi zboží)*. C. H. Beck. 1. vydanie 2017. s. 17 - 28

CISG vylúčiť jeho aplikáciu aj na kryptomenu ako peniaze. Ak odpovieme, že CISG nie je možné aplikovať na kúpy, predmetom ktorých sú kryptomeny, nakoľko nejde o peniaze, ktoré sú vylúčené z aplikácie podľa článku 2 písm. d), potom je na mieste si položiť ďalšiu otázku, a teda či kryptomeny môžu byť platidlom za tovar v zmysle článku 53 CISG alebo pôjde o tzv. barterový obchod, na ktorý sa už samotné CISG nevzťahuje? Jedným z ďalších definičných znakov tovaru je totiž v zmysle CISG zaplatenie kúpnej ceny zo strany kupujúceho.

V prvom rade sa teda pozrime na otázku, či je možné kryptomenu považovať za platidlo v zmysle CISG. Pre účely výkladu predmetného článku je rozhodne nevyhnutné, aby pojem peniaze bol vykladaný ako autonómne tak aj čo najužším spôsobom, a to za účelom zabezpečenia právnej istoty.¹² Peniazmi, resp. platobnými prostriedkami sa na účely CISG rozumejú všetky tuzemské a zahraničné platobné prostriedky platné v mene.¹³ Predmetnú definíciu potvrdzuje aj princíp čo najužšieho výkladu pojmu peniaze na účely CISG. Pokiaľ sú tak vylúčené štátom vydané peniaze, kryptomeny (pokiaľ nie sú vydávané zo strany napríklad centrálnych bánk), by vylúčené byť nemali.¹⁴ Ak teda kryptomeny ako také nepovažujeme za peniaze v zmysle CISG, nemôžu byť ani platidlom na účely zaplatenia kúpnej ceny v rámci CISG, nakoľko by v takomto prípade mohlo ísť o barterový obchod, ktorý nie je predmetom CISG. Rovnako si na tomto mieste dovoľíme poukázať na skutočnosť, že všeobecné obchodné podmienky niektorých platforiem poskytujúcich predaj NFT vylučuje aplikáciu CISG.¹⁵

Na základe vyššie uvedených argumentov si dovoľíme skonštatovať nasledovné. Je nepochybné, že zmluvy, predmetom ktorých je NFT sú záväzkovo právnymi kontraktmi a pri ich uzatváraní je potrebné vziať do úvahy existenciu CISG. Názory teoretikov, či je CISG aplikovateľné alebo neaplikovateľné na medzinárodné kúpy tovaru, ktorým je NFT sa v súčasnosti rozlišujú. Rozhodne valídny je názor, že NFT nie je hmotnou vecou a z tohto dôvodu by sa na neho CISG nemal vzťahovať, na druhej strane je však potrebné zamyslieť sa, či by nebolo vhodné upustiť od prílišného formalizmu výkladu pojmu tovar (znova akcentujeme na skutočnosť, že tento pojem samotný CISG priamo nevykladá) a nepozrieť sa na účel transakcie ako celok.

¹² HAYWARD, B.: *To boldly go, part II: Data as the CISG's next (but probably not final) frontier*. In. University of New South Wales Law Journal. Vol 44 (4).2021. s. 1517

¹³ Tichý, Ľ. *CISG (Úmluva OSN o smlouvách o mezinárodní koupi zboží)*. C. H. Beck. 1. vydanie 2017. s. 28 – 34

¹⁴ K tomuto pozri aj T HAYWARD, B.: *To boldly go, part II: Data as the CISG's next (but probably not final) frontier*. In. University of New South Wales Law Journal. Vol 44 (4).2021. s. 1518 a JANSSEN A.: *The United Nations Convention on contracts for the international sale of goods (CISG) and the emergence of smart contracts and cryptocurrencies: should we try to teach an old dog some new tricks?* In. Tsinghua China Law Review.2021. Vol 14. s. 10.

¹⁵ Pozri napríklad všeobecné obchodné podmienky Open Sea dostupné na: <https://opensea.io/tosw> bod 19.

Nariadenie Rím I

Nariadenie Rím I sa aplikuje na zmluvné záväzkové vzťahy v občianskych a obchodných veciach. Z pôsobnosti Negatívny rozsah pôsobnosti v rámci nariadenia Rím I nájdeme v článku 1 ods. 2, pričom rovnako ako pri analýze aplikácie CISG, aj tu sa stretávame s vylúčením záväzkov vyplývajúcich zo zmieniek, šekov a dlžobných úpisov a iných prevoditeľných cenných papierov v rozsahu, v ktorom záväzky z takýchto iných prevoditeľných cenných papierov vyplývajú z ich prevoditeľnej povahy.¹⁶ Už v rámci prípravy Rímskeho dohovoru sa prípravná skupina zhodla na tom, že tieto nástroje nie sú vhodné byť predmetom v záväzkovo právnych vzťahov spadajúcich pod Rímsky dohovor.¹⁷ Predmetný článok vylučuje aj iné obchodovateľné cenné papiere v rozsahu, v akom záväzky vyplývajúce z týchto iných prevoditeľných cenných papierov vyplývajú z ich prevoditeľného charakteru. Ak dokument, hoci je záväzok z neho prenosný, nie je považovaný za obchodovateľný cenný papier, nespadá pod výnimku. To má za následok, že dokumenty ako nákladné listy, podobné dokumenty vydané v súvislosti s prepravnými zmluvami a dlhopisy, záložné listy, záruky, ručiteľské listy, certifikáty o vklade, záručné listy a skladové listy sú vylúčené podľa písm. c) len vtedy, ak ich možno považovať za prevoditeľné cenné papiere, a aj vtedy sa vylúčenie vzťahuje len na záväzky vyplývajúce z ich prevoditeľného charakteru.¹⁸ Sme toho názoru, že NFT nespadá do tejto kategórie a teda dôjde k aplikácii Nariadenia Rím I.

Pri určovaní rozhodného práva na základe Nariadenia Rím I je nevyhnutné určiť, či došlo k voľbe rozhodného právneho poriadku alebo k voľbe rozhodného právneho poriadku nedošlo. V prípade ak si strany zmluvy zvolili rozhodný právny poriadok, je nevyhnutné, aby postupovali v súlade s článkom 3 Nariadenia Rím I, pričom je nevyhnutné brať do úvahy aj ods. 3 a 4 tohto článku podmieňujúce aplikáciu noriem od ktorých sa nie je možné odchyliť dohodou.

V prípade absencie voľby rozhodného právneho poriadku je nevyhnutné aplikovať článok 4 Nariadenia Rím I, pričom pokiaľ sa zmluvný typ nenachádza medzi zmluvnými typmi v rámci článku 4 ods. 1 písm. a) – d) je možné aplikovať ods. 2. V zmysle ods. 1 je možné zvažovať subsumovanie zmluvy, predmetom ktorej je NFT pod písm. a) *zmluva o predaji tovaru sa spravuje právnym poriadkom krajiny obvyklého pobytu predajcu*. Rovnako ako pri analýze CISG, sa aj pri Nariadení Rím I dostávame k otázke, ako je možné definovať pojem tovar. Staršia judikatúra ESD definuje tovar

¹⁶ Čl. 1 ods. 2 písm. d) Nariadenia Európskeho parlamentu a Rady (ES) č. 593/2008 zo 17. júna 2008 o rozhodnom práve pre zmluvné záväzky (Rím I)

¹⁷ Report on the Convention on the law applicable to contractual obligations by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris I. Official Journal C 282, 31/10/1980. bod 11.

¹⁸ Tamtiež.

ako výrobok, ktorého hodnota je vyjadriteľná v peniazoch a ktorý môže byť predmetom obchodnej transakcie.¹⁹

Ak je však záverom, že NFT nespadá pod pojem tovar podľa článku 4 ods. 1 písm. a), neznamená to, že nie je možné Nariadenie Rím I aplikovať. V zmysle ods. 2 rovnakého článku totiž platí, že sa predmetná zmluva bude spravovať právnym poriadkom krajiny obvyklého pobytu zmluvnej strany, ktorá má uskutočniť plnenie charakteristické pre zmluvu.

V rámci predmetnej kapitoly nie je rozhodne možné opomenúť ani spotrebiteľské zmluvy. Nariadenie Rím I obsahuje osobitnú právnu úpravu, ktorá sa na nich vzťahuje v článku 6. Aj v rámci spotrebiteľských zmlúv je možné vykonať voľbu rozhodného právneho poriadku, avšak takáto voľba rozhodného práva však nesmie zbaviť spotrebiteľa ochrany, ktorú mu poskytujú také ustanovenia, od ktorých sa nemožno odchýliť dohodou podľa inak rozhodného právneho poriadku. V prípade absencie voľby práva, sa zmluva bude spravovať právnym poriadkom krajiny obvyklého pobytu spotrebiteľa, za predpokladu, že sú splnené ďalšie požiadavky podľa článku 6 Nariadenia Rím I.

Záver

Z vykonanej analýzy jednoznačne vyplýva, že problematika NFT predstavuje oblasť, ktorá sa vyvíja rýchlejšie, než sa vyvíja či už právna úprava v tejto otázke, ako aj samotná judikatúra a aplikačná prax. V rámci príspevku sme si stanovili cieľ, a to analyzovať súčasnú právnu úpravu a to, do akej miery reflektuje digitálne aktíva, konkrétne NFT s väzbou na viacero právnych poriadkov. Za týmto účelom sme sa zamerali na pramene, CISG ako priamu normu, Nariadenie Rím I ako kolíznu normu pre určovanie rozhodného práva v záväzkovo právnych veciach. Je nepopierateľné, že súčasná právna úprava nedostatočne nereflektuje existenciu skúmaného NFT, a to najmä ak sa pozrieme na CISG. V tomto kontexte sa pritom prikláňame k názoru prezentovaného v príspevku a teda, že v rámci aplikácie CISG by sa malo ustúpiť od uplatňovania prílišného formalizmu pojmu tovar.

Zoznam použitej literatúry

1. FAUSING KYLKJÆR, K.: The applicability of the CISG on transactions of software. Dostupné na: https://law.au.dk/fileadmin/Jura/dokumenter/forskning/Rettid/Afh_2019/afh6-2019.pdf (cit. 12.09.2025).

¹⁹ Rozsudok súdneho dvora z 10. decembra 1968 vo veci 7/68 Komisia Európskych spoločenstiev proti Talianskej republike. ECLI:EU:C:1968:51, s. 428.

2. HAYWARD, B.: To boldly go, part II: Data as the CISG's next (but probably not final) frontier. In. University of New South Wales Law Journal. Vol 44 (4).2021. s. 1482 – 1523.
3. JANSSEN A.: The United Nations Convention on contracts for the international sale of goods (CISG) and the emergence of smart contracts and cryptocurrencies: should we try to teach an old dog some new tricks? In. Tsinghua China Law Review.2021. Vol 14.
4. SEMPERE, C., P.: Governance and Control of Data and Digital Economy in the European Single Market Legal Framework for New Digital Assets, Identities and Data Spaces. Springer Cham. 2025. 978-3-031-74889-9. 515 s.
5. Tichý, Ľ. CISG (Úmluva OSN o smlouvách o mezinárodní koupi zboží). C.H. Beck. 1. vydanie 2017 ISBN: 978-8-07400649-4. s. 440.
6. Rozsudok súdneho dvora z 10. decembra 1968 vo veci 7/68 Komisia Európskych spoločenstiev proti Talianskej republike. ECLI:EU:C:1968:51.
7. Dohovor OSN o zmluvách o medzinárodnej kúpe tovaru
8. Law Commission. Digital assets and (electronic) trade documents in private international Law. Consultation paper. č. 273. 2025. s Dostupné na: <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/54/2025/06/Digital-assets-conflicts-CP-2025.pdf.pdf> (cit. 15.09.2025)
9. Nariadenie Európskeho parlamentu a Rady (ES) č. 593/2008 zo 17. júna 2008 o rozhodnom práve pre zmluvné záväzky
10. Princípy Unidroit o digitálnych aktívach v súkromnom práve

Kontaktné údaje

JUDr. Dominika Juck, PhD.

dominika.juck@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

KOLÍZNE DILEMY V DIGITÁLNEJ REALITE ALEBO URČOVANIE ROZHODNÉHO PRÁVA PRE CEZHRANIČNÉ SPORY TÝKAJÚCE SA DOMÉNOVÝCH MIEN V METAVERZE ¹

CONFLICTING DILEMMAS IN DIGITAL REALITY OR DETERMINING THE APPLICABLE LAW FOR CROSS-BORDER DISPUTES CONCERNING DOMAIN NAMES IN THE METAVERSE

Ema Krkošková²

Abstrakt: Súčasný rozmach digitálneho prostredia a Metaverza, chápaného ako počítačom vytvoreného virtuálneho sveta, v ktorom ľudia môžu pracovať, študovať či nakupovať virtuálne nehnuteľnosti, predstavuje jednu z najvýraznejších inovácií v digitálnej sfére. Exponenciálna hospodárska činnosť v tomto prostredí so sebou prináša aj potrebu riešiť cezhraničné spory o virtuálne doménové mená, ktoré slúžia ako adresy pre virtuálny majetok. Vzhľadom na decentralizovanú povahu a absenciu geografického umiestnenia takýchto virtuálnych doménových mien, predstavujú bežné metódy určovania rozhodného práva neaplikovateľný a neúčinný systém, ktorý nedokáže pružne reagovať na absenciu fyzického sídla, decentralizovanú povahu aktív či na skutočnosť, že v prípade sporu škoda vzniká výhrade vo virtuálnom priestore. Hlavným cieľom článku je preto špecifikácia tohto priestoru z pohľadu medzinárodného práva súkromného a navrhnutie nového modelu kolíznej úpravy v podobe návrhov *de lege ferenda*, ktoré by dokázali efektívne riešiť otázky určenia rozhodného práva v cezhraničných sporoch týkajúcich sa práve doménových mien v Metaverze. Príspevok teda navrhuje novú právnu úpravu, ktorá netkvie v geograficky stanovených kritériách, ale poskytuje väzbu viažucu sa na ekonomické a funkčné faktory Metaverza.

Kľúčové slová: doménové meno, duševné vlastníctvo, Metaverzum, rozhodné právo, virtuálne domény.

¹ Tento príspevok je výstupom z projektu č. UK/1250/2025 s názvom „Ochrana duševného vlastníctva v digitálnom veku: Medzinárodnoprávne výzvy“.

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra medzinárodného práva a medzinárodných vzťahov.

Abstract: The current boom in the digital environment and the Metaverse, understood as a computer-generated virtual world in which people can work, study, or purchase virtual real estate, represents one of the most significant innovations in the digital sphere. The exponential economic activity in this environment also brings with it the need to resolve cross-border disputes over virtual domain names, which serve as addresses for virtual property. Given the decentralized nature and absence of geographical location of such virtual domain names, the usual methods of determining the applicable law represent an inapplicable and ineffective system that cannot respond flexibly to the absence of a physical location, the decentralized nature of the assets, or the fact that in the event of a dispute, the damage occurs exclusively in virtual space. The main objective of this article is therefore to specify this space from the perspective of international private law and to propose a new model of conflict of laws in the form of *de lege ferenda* proposals that would effectively address the issues of determining the applicable law in cross-border disputes concerning domain names in the Metaverse. The paper therefore proposes new legislation that is not based on geographically defined criteria, but provides a link to the economic and functional factors of the Metaverse.

Key words: domain name, intellectual property, Metaverse, applicable law, virtual domains.

Úvod

Súčasne prebiehajúca digitálna transformácia prekročila hranice tradičného online internetového prostredia a do popredia nastupuje tzv. *Metaverzum*,³ ktoré značí úplne ekonomicky sebestačný virtuálny priestor vznikajúci spojením fyzickej reality s digitálnou virtualitou.⁴ Tento fenomén digitálneho priestoru so sebou prináša nové príležitosti pretavené v možnosti vytvárania a vlastníctva aktív, obchodovania či nakupovania, socializovania sa prostredníctvom svojich avatarov alebo navštevovania virtuálnych udalostí.⁵

³ K fenoménu Metaverza pozri napríklad: CHENG, Shenghui: Metaverse. In: Metaverse: Concept, Content and Context. Springer, Cham, 2023. S. 1-23 alebo ZHANG, Jiale - QUOQUAB, Farzana - MOHAMMAD, Jihad: Embracing the new reality: Gen Y's intention to use metaverse apps and devices. In: Curr Psychol, vydanie 44, 2025. S. 398-417. DOI: <https://doi.org/10.1007/s12144-024-07160-5>.

⁴ MYSTAKIDIS, Stylianos: Metaverse. In: Encyclopedia 2, číslo 1, 2022. S. 486. DOI: <https://doi.org/10.3390/encyclopedia2010031>.

⁵ V roku 2021 spoločnosť Nike oznámila, že v rámci spolupráce s hernou platformou s názvom Roblox spustila fungovanie tzv. „*Nikeland*“ – virtuálneho športového parku v Metaverze, v ktorom používatelia môžu napríklad hrať virtuálne hry či kupovať tenisky značky Nike pre svojich avatarov.

Tieto domény, spravované prostredníctvom decentralizovaných sietí⁶ nie sú len akýmsi technickým rozhraním, ale nadobúdajú aj značnú ekonomickú hodnotu, čo má za následok práve nárast cezhraničných sporov týkajúcich sa doménových mien v Metaverze. Z pohľadu medzinárodného práva súkromného táto evolúcia predstavuje aktuálnu výzvu, v ktorej tradičné kolízne normy zodpovedajúce otázky určenia rozhodného práva, sú historicky a koncepcne zakotvené v geografických princípoch, čo v prípade bezhraničného Metaverza stráca význam.

Aj napriek faktu, že Nariadenie Európskeho parlamentu a Rady (ES) č. 864/2007 z 11. júla 2007 o rozhodnom práve pre mimozmluvné záväzky (ďalej len ako „nariadenie Rím II“),⁷ predstavuje pomerne moderný unifikačný nástroj, využíva hraničné kritériá ako *lex loci damni infecti*⁸ či *lex loci protectionis*.⁹ Ako teda určiť miesto vzniku škody, ak je virtuálna doména prístupná globálne, a teda škoda mohla vzniknúť v rovnakej miere kdekoľvek na svete, pričom absentuje reálne fyzické sídlo takejto domény? Ďalej, ako máme správne určiť rozhodné právo pomocou kolíznej normy, ak je doménové meno prakticky chránené vo virtuálnom svete neobmedzene?

Na základe uvedeného si preto tento príspevok kladie za cieľ identifikovať a následne analyzovať systémové nedostatky existujúcich kolíznych noriem obsiahnutých v nariadení Rím II, a to konkrétne v kontexte cezhraničných sporov týkajúcich sa virtuálnych doménových mien v prostredí Metaverza. Sprihliadnutím na technologické atribúty tohto virtuálneho prostredia, a najmä na jeho decentralizovanú a perzistentnú povahu, si preto kladieme za cieľ zistiť, či je potrebné prijať novú právnu úpravu v prístupe k určovaniu rozhodného práva, ktorá by dokázala adekvátne a predvídateľne regulovať právne vzťahy v takomto imateriálnom prostredí. V prípade, že zistíme, že je nutné prijať takúto novú právnu úpravu týkajúcu sa Metaverza, pretavíme túto myšlienku do konkrétneho návrhu *de lege ferenda*, ktorý bude zohľadňovať špecifiká virtuálneho prostredia s cieľom zabezpečiť právnu istotu pre subjekty cezhraničných sporov týkajúcich sa doménových mien v Metaverze, ktorá je v takýchto právnych vzťahoch plynúcich pri porušeníach doménového mena ako jedného z práv duševného vlastníctva, priam

Hlavnou stratégiou v Metaverze bol v tomto prípade zisk výnosov v reálnom svete, ktorý mal byť docielený preferenciami používateľov v digitálnom svete pretavenými v tom reálnom. LEE, Jyh-An - YANG, Liang - PAN, Hui: Legal Implications of Self-presence in the Metaverse. The Chinese University of Hong Kong Faculty of Law: Media & Arts Law Review, vydanie 25, číslo 4. S. 279-280. SSRN: <https://ssrn.com/abstract=4665569>.

⁶ Napríklad spravované prostredníctvom decentralizovanej databázy blockchain, ktorá slúži na uchovávanie záznamov.

⁷ Nariadenie Európskeho parlamentu a Rady (ES) č. 864/2007 z 11. júla 2007 o rozhodnom práve pre mimozmluvné záväzky (Rím II), Ú. v. EÚ L 199, s. 40 – 49.

⁸ Právo miesta, kde vznikla škoda.

⁹ Právo miesta, v ktorom je poskytovaná ochrana právu duševného vlastníctva.

nutnosťou, a to aj vzhľadom na čoraz viac sa rozmáhajúce digitálne prostredie tohto fenoménu.

Stav *de lege lata* pri porušení doménového mena

Pri posúdení otázky rozhodného práva v prípade porušenia práva duševného vlastníctva, do ktorého spadá aj doménové meno ako jedna z jeho mnohých podkategórií,¹⁰ bude potrebné túto otázku zodpovedať v intenciách nariadenia Rím II, ktoré je uplatňované iba na mimozmluvné záväzkové vzťahy v občianskych a obchodných veciach, v ktorých dochádza ku kolízii právnych poriadkov.¹¹

Pri určovaní rozhodného práva v prípadoch porušenia práv duševného vlastníctva, je už dlhodobo uznávanou zásadou *lex loci protectionis*, ktorá je pretavená i v samotnom čl. 8 ods. 1 nariadenia Rím II, ktorý znie: „*Mimozmluvný záväzok vyplývajúci z porušenia práva duševného vlastníctva sa spravuje právnym poriadkom krajiny, na území ktorej je toto právo chránené.*“ V prípade, že teda existuje mimozmluvný záväzkový vzťah a pôjde pritom o občiansku či obchodnú vec, pri ktorej nastáva kolízia právnych poriadkov rozličných štátov, pričom zároveň bolo porušené právo na doménové meno v Metaverze, je nutné skúmať v ktorom štáte poživalo predmetné doménové meno svoju ochranu. V prípade porušenia doménového mena v Metaverze, ktoré by bolo zároveň klasifikované ako jednotný nástroj Európskej únie, rozhodné právo by sa posudzovalo podľa práva štátu, na území ktorého došlo k porušeniu takéhoto práva duševného vlastníctva (jednotné právo Európskej únie viažuce sa na porušenie práv duševného vlastníctva Európskej únie).^{12,13} Pri jednotlivých porušeníach doménového mena je voľba rozhodného práva subjektami, v intenciách skúmaného článku 8 vylúčená, a teda subjekty mimozmluvného vzťahu si nemôžu zvoliť právny poriadok, ktorým by sa spravoval takýto mimozmluvný záväzok.¹⁴ Určenie rozhodného práva sa tak bude posudzovať

¹⁰ DAWOOD, Aya Muhammad - KHALIL, Israa Khader: The domain name and other intellectual property rights. In: International Journal of Environmental Sciences, vydanie 11, číslo 12, 2025. S. 863-876.

¹¹ KRAMER, Xandra E.: The Rome II Regulation on the Law Applicable to Non-Contractual Obligations: The European private international law tradition continued – Introductory observations, scope, system, and general rules. In: Netherlands Internationaal Privaatrecht (NIPR), vydanie 4, 2008. S. 415.

¹² Čl. 8 ods. 2 nariadenia Rím II: „*Mimozmluvný záväzok vyplývajúci z porušenia jednotného práva duševného vlastníctva Spoločenstva sa spravuje právnym poriadkom krajiny, na území ktorej došlo k porušeniu, pokiaľ ide o otázky, na ktoré sa nevzťahuje príslušný právny nástroj Spoločenstva.*“

¹³ Na účely tohto príspevku sa tejto oblasti práv duševného vlastníctva nebudeme ďalej venovať, nakoľko jednotné nástroje práva Európskej únie v podobe práv duševného vlastníctva tvoria osobitnú kategóriu.

¹⁴ Pre viac informácií týkajúcich sa voľby práva subjektami v intenciách nariadenia Rím II pozri: KUR, Annette - MAUNSBACH, Ulf: Choice of Law and Intellectual Property Rights. In: Oslo Law Review, vydanie 6, číslo 1, 2019. S. 43-61.

podľa klasifikácie, či bolo porušené právo duševného vlastníctva Európskej únie v prípadoch, kedy je doména chránená unifikovaná úniovým hmotným právom alebo naopak, bolo porušené právo duševného vlastníctva v podobe doménového mena národného či medzinárodného charakteru.¹⁵

V prípade, ak by doménové meno v Metaverze bolo registrované napríklad ako ochranná známka, aplikovateľné ustanovenia by boli tie, ktoré sa týkajú nekalosúťažného konania a konania obmedzujúceho slobodnú súťaž subjektov mimozmluvného záväzkového vzťahu obsahujúceho cudzí prvok. V situácii, kedy bude možné hovoriť o takomto vzťahu ako o doménovom spore nekalosúťažného charakteru, rozhodné právo budeme určovať podľa právneho poriadku štátu, v ktorom došlo alebo môže dôjsť k poškodeniu konkurenčných vzťahov alebo kolektívnych záujmov spotrebiteľov.¹⁶ V prípade, ak by mimozmluvný záväzok subjektov vyplýval z obmedzenia hospodárskej súťaže, rozhodným právom by bol právny poriadok štátu, na ktorého trhu by malo alebo mohlo mať takéto obmedzenie účinok.¹⁷ Praktickou otázkou, na ktorú odpoveď ponúka aj samotné nariadenie Rím II je – ako sa posúdi otázka rozhodného práva v prípade, ak by obmedzenie slobodnej súťaže malo účinky na trhu vo viacerých štátoch kumulatívne? V takejto situácii je možné, aby si subjekt požadujúci náhradu škody vybral, či vec bude riešená a rozhodovaná na súde v mieste bydliska štátu odporcu, a teda podľa právneho poriadku takéhoto štátu, alebo si svoj nárok môže založiť na práve konajúceho súdu členského štátu, a to v prípade, že: *„trh v tomto členskom štáte je jedným z trhov, na ktorý má obmedzenie hospodárskej súťaže, z ktorého vyplýva mimozmluvný záväzok, na ktorom sa zakladá nárok, priamy a značný účinok“*.¹⁸

Ak nemožno uplatniť predošlé spomínané ustanovenia týkajúce sa priamo duševného vlastníctva, nekalosúťažného konania alebo konania obmedzujúceho slobodnú súťaž, je možné využitie poslednej možnosti, akou je uplatnenie všeobecného pravidla nariadenia Rím II. V takomto prípade sa bude mimozmluvný záväzok spravovať právnym poriadkom štátu, na území ktorého vznikla škoda.¹⁹

¹⁵ LYSINÁ, Peter, HAŤAPKA, Miloš, BURDOVÁ, Katarína a kol.: Medzinárodné právo súkromné. 3. vydanie. Bratislava: C. H. Beck, 2023. S. 268.

¹⁶ Čl. 6 ods. 1 nariadenia Rím II.

¹⁷ Čl. 6 ods. 3 písm. a) nariadenia Rím II.

¹⁸ Čl. 6 ods. 3 písm. b) nariadenia Rím II, ktorý ďalej vytvára priestor pre situáciu, kedy by bolo na žalovanej strane viac než jeden odporca: *„Ak sa osoba žiadajúca náhradu škody v súlade s uplatniteľnými pravidlami o súdnej právomoci súdi s viac ako jedným odporcom na uvedenom súde, svoj nárok môže založiť len na právnom poriadku krajiny tohto súdu, ak má obmedzenie hospodárskej súťaže, na ktorom sa zakladá nárok proti každému z týchto odporcov, priamy a značný účinok aj na trh členského štátu tohto súdu.“*

¹⁹ Čl. 4 ods. 1 nariadenia Rím II, ktorý okrem iného dodáva, že sa v takomto prípade neprihliada na územie štátu, v ktorom došlo k skutočnosti, ktorá spôsobila škodu, a ani na územie štátu, kde nastali nepriame následky tejto skutočnosti.

V prípade, že oba subjekty právneho vzťahu v podobe zodpovednej osoby a osoby poškodenej majú svoj obvyklý pobyt v tom istom štáte,²⁰ je možné, aby sa civilný delikt spravoval právnym poriadkom takéhoto štátu, v ktorom majú oba subjekty svoj obvyklý pobyt.²¹ V prípade, ak by civilný delikt mal zjavne užšiu väzbu s iným štátom, než so štátom na území ktorého vznikla škoda a so štátom, v ktorom majú subjekty spoločný obvyklý pobyt, rozhodným právnym poriadkom by bol práve takýto štát vykazujúci zjavne užšiu väzbu.²²

Nová realita neprísôbiaca sa starým zákonom?

Súčasne aktuálne a účinné nariadenie Rím II, ktoré bolo v podstate vytvorené na svete viazanom na fyzickú geografiu a na princípe teritoriality, čelí súčasne už v značne digitalizovanom svete podstatnej kríze. Fenomén v podobe Metaverza, ktoré je definované najmä svojou perzistentnou a zdieľanou povahou,²³ takmer úplne "odstrihol" ekonomické a sociálne interakcie od tradičných štátnych hraníc tak ako sme ich kedysi poznali. Súčasná bilancia cezhraničných digitálnych sporov nielen v priestore Metaverza má exponenciálny nárast,²⁴ pričom k najčastejším sporom možno zaradiť práve spory o porušenie práv duševného vlastníctva a nekalosúťažné konanie, ktoré prebieha typicky vo forme tzv. cybersquattingu²⁵. Konkrétne pri sporoch o virtuálne doménové mená, ktoré nachádzame v podobe unikátnych digitálnych adries, sa jednotlivé nedostatky súčasného a aktuálneho práva prejavujú vo viacerých rozličných aspektoch. Práve, už spomínané nariadenie Rím II, ktoré by sa dalo označiť za akúsi vlajkovú loď medzinárodného práva súkromného v priestore Európskej únie v oblasti určovania rozhodného práva pre mimozmluvné záväzky, vykazuje znaky nefunkčného nástroja pri riešení týchto digitálnych konfliktov

²⁰ Je nutné skúmať obvyklý pobyt v čase vzniku škody.

²¹ Čl. 4 ods. 2 nariadenia Rím II.

²² Čl. 4 ods. 3 nariadenia Rím II, ktorý vytyčuje spojenie „zjavne užšej väzby“ ako väzby zakladajúcej sa najmä na už existujúcom vzťahu medzi subjektami, akým môže byť napríklad už existujúca zmluva, pričom takáto zmluva je úzko prepojená práve s riešeným civilným deliktom. K termínu „zjavne užšia väzba“ pozri: KONKOL, Anton: Porušenie prá duševného vlastníctva a otázka určenia rozhodného práva v Európskej únii. In: Právní rozpravy 2014, vydanie 4, 2014. S. 12.

²³ SADEGHI-NIARAKI, Abolghasem, et al.: Groundbreaking taxonomy of metaverse characteristics. In: Artificial Intelligence Review, vydanie 58, číslo 244, 2025. S. 19.

²⁴ KUMAR BAL GOVIND, Singh: Online Dispute Resolution in Cross-Border Disputes: A Comprehensive Analysis, 2023. S. 3.

²⁵ Cybersquattingom označuje neoprávnenú registráciu a využívanie doménových mien v prostredí internetu, ktoré môžu byť podobné či identické napríklad s ochrannými známkami. Subjekt používa doménové meno so zlým úmyslom s cieľom profitácie z dobrej povesti skutočného vlastníka pôvodnej ochrannej známky. Pre viac informácií k činnosti cybersquattingu pozri: GLONINA, Vera: Back to the Future with Blockchain Domain Names: Toward a Global Policy to Fight Cybersquatting in Web 3.0. In: Trademark Reporter, vydanie 114, číslo 4, 2024. S. 591-597.

týkajúcich sa porušenia doménového mena v Metaverze, na ktoré poukážeme bližšie v nasledujúcich častiach príspevku.

Po prvé, zásada *lex loci protectionis*, ktorá je pretavená práve v ochrane doménového mena podľa práva určitého štátu, a teda je postavená na teritorialite ochrany tohto práva duševného vlastníctva, ktoré sú *ex lege* teritoriálne, je v prípade virtuálnych domén a ich mien prakticky neuplatniteľná. Virtuálne domény s konkrétnymi doménovými menami a v neposlednom rade aj s virtuálnymi aktívami nachádzajúcimi sa na takýchto doménach, sú globálnymi v technickom a aj v ich funkčnom ponímaní.²⁶ Prístup na takéto domény, ich zobrazenie či potenciálne škody, ktoré na doméne môžu vzniknúť, sú realizované simultánne na celom svete, a to bez ohľadu na akékoľvek rozvrstvenie štátnych hraníc. Ak by sme teda požadovali ochranu doménového mena len pre jeden štát v kontexte univerzálne prístupného priestoru v podobe Metaverza, tento postup by viedol buď k nutnosti aplikovať právne poriadky všetkých štátov kumulatívne (čo je prakticky absolútne nemožné pri kolízii viacerých právnych poriadkov) alebo by bolo potrebné aplikovať ako rozhodné právo ako výber z jedného z právnych poriadkov štátov sveta, ktorý by nemal s podstatou sporu relevantnú väzbu, a teda tento výber by nebol opodstatnený zásadou rozumného a spravodlivého usporiadania právneho vzťahu. Navyše, tradičné domény sú primárne viazané na centrálného registrátora, pričom virtuálne domény, vrátane domén v Metaverze, sú spravované prostredníctvom decentralizovaných sietí.²⁷ Takáto situácia absencie centrálného registrátora v prípade domény eliminuje základné kolízne kritériá, ktoré by mohli byť uplatniteľné podľa nariadenia Rím II, keďže je sídlo registrátora alebo miesto registrácie takejto domény nemožné zistiť. Zásada *lex loci protectionis* s princípom teritoriality stráca pri určení rozhodného práva v prípade porušenia doménového mena v priestore Metaverza svoju oporu v akomkoľvek geografickom faktore, ktorý by inak slúžil ako spájajúci prvok v predmetnom vzťahu. Decentralizácia a absencia registračného miesta doménových mien teda vylučuje aplikovateľnosť článku 8 ods. 1 nariadenia Rím II, ktoré stanovuje určenie rozhodného práva v podobe právneho poriadku štátu, v ktorom sa pre právo duševného vlastníctva poskytuje jeho ochrana.²⁸

Po druhé, ak by bolo porušenie doménového mena v Metaverze klasifikované ako nekalosúťažný akt, nie je v takomto prípade možné určiť dotknutý trh, na ktorom boli ovplyvnené porušením doménového mena vzťahy hospodárskej súťaže alebo spoločné záujmy spotrebiteľov. Trh v prostredí Metaverza nie je viazaný na jeden

²⁶ FEIFEI, Shi, et al.: A new technology perspective of the Metaverse: Its essence, framework and challenges. In: Digital Communications and Networks, vydanie 10, číslo 6, 2024. S 1653.

²⁷ Pozri poznámku pod čiarou č. 6.

²⁸ Pre viac informácií o rozhodnom práve v prostredí Metaverza pozri: PELLEGRINI, Cécile: Applicable law in the metaverse: A European International Private Law perspective. In: Research Handbook on the Metaverse and Law, 2024. S. 375-397.

konkrétny štát,²⁹ a teda v prípade hospodárskej súťaže medzi virtuálnymi entitami pôjde o hospodársku súťaž v akomsi "nadmárodnom priestore", ktorý nie je vytýčený akýmkoľvek štátnymi hranicami. Presné určenie, ktoré by definovalo kde (v akom štáte či štátoch) boli vzťahy ovplyvnené, by vyžadovalo napríklad sledovanie IP adries³⁰ a geolokalizácie všetkých účastníkov transakcií, čo je jednak technicky náročný proces, a jednak by sa takýmto postupom obchádzala esenciálna povaha podstaty Metaverza tkvejúca práve v jeho bezhraničnej povahe. Navyše, ak pozornosť upriamime práve na článok 6 ods. 1 nariadenia Rím II a na jeho špecifické kolízne kritérium postavené na ovplyvnení vzťahov hospodárskej súťaže, zistíme, že v rozhraní súdnej praxe je interpretované prostredníctvom vymedzenia cieľového publika.³¹ Takáto interpretácia tohto kolízneho kritéria je opäť naviazaná na geografické vymedzenie trhu jednotlivých štátov, čo je pri virtuálnych doménach nevyužiteľné. A teda, predmetné ustanovenie nariadenia Rím II, ktoré favorizuje právny poriadok štátu, na trhu ktorého sú ovplyvnené vzťahy hospodárskej súťaže alebo spoločné záujmy spotrebiteľov, tak taktiež ako aj článok 8 tohto sekundárneho právneho aktu Európskej únie, nenachádza svoje uplatnenie v oblasti určenia rozhodného práva pri porušení doménového mena v Metaverze.

A na záver po tretie, v prípade, keby spor o virtuálne doménové meno jestvujúce v Metaverze nebolo možné subsumovať pod špecifické režimy *a)* ako režim pre právo duševného vlastníctva, ktorého rozhodné právo by sa určilo podľa ustanovenia článku 8 nariadenia Rím II, a ani podľa *b)* ako režim pre nekalosúťažné konanie, ktorého rozhodné právo by sa určilo podľa ustanovenia článku 6 nariadenia Rím II, malo by sa pristúpiť k uplatneniu všeobecného kolízneho pravidla obsiahnutého v článku 4 predmetného nariadenia. Pri nutnosti aplikovania prvého kolízneho kritéria, ktoré stavia na právnom poriadku krajiny, v ktorej škoda vznikla, a teda *lex loci damni infecti*, je v kontexte Metaverza rovnako neúčinné a logicky nerealizovateľné. Aj napriek tomu, že vo virtuálnom svete Metaverza pri porušení

²⁹ SPAIS, George, et al.: A new Walk in the Future of the Metaverse: Marketing Implications for Consumer Behavior. In: Journal of Consumer Behaviour, vydanie 24, číslo 2, 2025. S. 860.

³⁰ V prípade problematiky IP adries a Metaverza pozri: GAETANO, Dimita, et al.: IP and Metaverse (S)-an Externally Commissioned Research Report. Queen Mary Law Research Paper no. 427/2024, 2024. S. 19.

³¹ Cieľové publikum alebo cieľový trh slúži práve na identifikáciu skutočnosti, na ktorom trhu jednotlivého štátu došlo k ovplyvneniu, respektíve k poškodeniu konkurenčných vzťahov alebo kolektívnych záujmov spotrebiteľov. Vo fyzickom svete je relatívne ľahké určiť takýto štát, avšak v online prostredí s globálnym dosahom potrebujú súdy určiť niekoľko kritérií, ktoré by napomohli upresniť takýto trh a konkrétny štát, na ktorý malo porušenie doménového mena dosah. Cieľové publikum alebo cieľový trh sa vyvodzuje preto z rozličných faktorov, ktoré indikujú, na ktorú geografickú oblasť bolo porušenie domény zamerané. Týmito faktormi môže byť napríklad jazyk webovej stránky, zobrazovanie cien v konkrétnej mene na predmetnej doméne, identifikácia využitia národných reklamných kampaní a iné.

doménového mena nastane reálna peňažná ujma nositeľovi práva duševného vlastníctva, samotný akt vzniku škody je síce možné vo väčšine prípadov lokalizovať, avšak je nutné apelovať práve na jednoduchší postup, ktorý by súdom uľahčil „zistovanie“ takéhoto miesta.³² Škoda vzniká v rámci virtuálneho priestoru, kde sú servery a blockchainové uzly rozmiestnené prakticky po celom svete, čo v niektorých prípadoch znemožňuje geografickú lokalizáciu miesta vzniku škody, dokonca v takýchto prípadoch nie je možné určiť, kde nastala skutočnosť, ktorá zakladá nárok na náhradu škody.³³ Ak by sme aj pristúpili k aplikácii určenia *lex loci damni infecti*, pokus o jeho určenie by opäť viedol k nutnosti výberu jedného z kolidujúcich právnych poriadkov štátov.³⁴

Návrh *de lege ferenda* v podobe Lex Metaversi

Po predošlej analýze kolíznych noriem nariadenia Rím II sme zistili, že v ňom obsiahnuté teritoriálne princípy sú zásadne neúčinné a neaplikovateľné na spory o virtuálne doménové mená, ktoré vznikli v bezhraničnom priestore Metaverza. Zásady *lex loci damni infecti* a *lex loci protectionis* nemajú žiadny oporný bod v decentralizovanej digitálnej realite, čo vedie k právnemu vákuu ohrozujúcemu právnú istotu, predvídateľnosť či ochranu subjektov v takomto imateriálnom prostredí. V súčasnej dobe už nepostačuje len interpretovať alebo extenzívne vykladať už existujúce ustanovenia,³⁵ namiesto toho je nevyhnutné navrhnúť inovatívny prístup, ktorý bude pretavený v konkrétnom návrhu *de lege ferenda*, s cieľom predstaviť a vedecky odôvodniť zavedenie novej a komplexnej zásady *lex metaversi*.

*Lex metaversi*³⁶ by slúžilo v medzinárodnom práve súkromnom ako primárne kolízne kritérium pre mimozmluvné záväzky, ktoré vznikli výlučne v bezhraničnom online prostredí. Navrhovaná zásada by sa uplatnila prednostne pred článkom 4, 6 a 8

³² Riešenu otázku týkajúcu sa vzniknutej škody v prostredí Metaverza v spojení s určením medzinárodnej právomoci pri riešení cezhraničných sporov pozri: COLEMAN, Ben: Jurisdiction and torts in the metaverse. 2022. Príspevok dostupný online na nasledovnom webovom sídle: <https://www.bristows.com/news/jurisdiction-and-torts-in-the-metaverse/>.

³³ K riešeniu kolíznoprávnej problematiky pozri aj: LYSINA, Peter: Kolízne normy v digitálnom veku: výzvy pre medzinárodné právo súkromné. In: Acta Facultatis Iuridicae Universitatis Comenianae, diel 44, číslo 1, 2025. S. 69-94.

³⁴ Napokon, ani úniková klauzula v článku 4 ods. 3 nariadenia Rím II neposkytuje dostatočnú záruku, nakoľko koncept „zjavne užšej väzby“ je primárne interpretovaný v intenciách geografických faktorov.

³⁵ Prakticky sudcovia ani nemajú na výber, keďže musia zodpovedať otázku rozhodného práva, pričom prednostne musia sudcovia súdov členských štátov aplikovať nariadenie Rím II. Buď teda sudca aplikuje konkrétne ustanovenie nariadenia tak, že musí využiť jeho extenzívny výklad na prostredie Metaverza v prípade, že chce určiť rozhodné právo alebo ho musí interpretovať odlišne.

³⁶ RODRÍGUEZ, Ana Mercedes López: Towards a Lex Metaversi? The law applicable to virtual real estate in the metaverse. In: Interactive Entertainment Law Review, vydanie 2, číslo 2, 2024. S. 110.

nariadenia Rím II, pričom by vychádzala konkrétne z predpokladu, že najužšia väzba s doménovým sporom sa nachádza v štáte, v ktorom je riadená technická či ekonomická činnosť takejto virtuálnej platformy. Navrhujeme preto, aby bolo do nariadenia Rím II doplnený nový článok 8a s názvom: „*Mimozmluvné záväzky súvisiace s decentralizovanými virtuálnymi aktívami*“. Presné znenie ustanovenia by bolo: „*Mimozmluvný záväzok vyplývajúci z porušenia či ohrozenia doménového mena alebo iného decentralizovaného aktíva vo virtuálnom prostredí, sa spravuje právnym poriadkom krajiny, s ktorým má takéto doménové meno alebo iné decentralizované aktívum vo virtuálnom prostredí najužšiu funkčnú alebo ekonomickú väzbu.*“ Takéto navrhované ustanovenie by teda vychádzalo z predpokladu, že najužšie spojenie s potenciálnym doménovým sporom by sa nachádzalo v právnom poriadku štátu, v ktorom je riadená technická a ekonomická činnosť samotnej virtuálnej domény. Implementáciou tohto navrhovaného ustanovenia by medzinárodné právo súkromné vytvorilo nové kolízne kritérium pretavené v *lex metaversi*, ktoré by transformovalo doteraz zaužívaný koncept „najužšej väzby“ tkvejúci v geografickom aspekte a v princípe teritoriality, na rovinu funkčnosti a technickosti. Takýto posun by definitívne zabezpečil aplikovateľnosť právneho poriadku štátu na doménový spor, s ktorým bude mať predvídateľnú väzbu na bezhraničné prostredie, a to vrátane priestoru decentralizovaného Metaverza.³⁷

Hoci by nami navrhované riešenie v podobe ustanovenia vyžadovalo novelizáciu nariadenia Rím II, pričom by tak bol prelomený princíp viažuci sa na teritorialitu práv duševného vlastníctva, alebo prijatie medzinárodného aktu v podobe nového dohovoru, ktorý by sa vo svojom obsahu podrobnejšie venoval oblasti doménových sporov a virtuálnemu priestoru, je tento krok jedinou cestou, ktorou sa môže docieľiť efektívnosť a spravodlivosť v dnešnej pohlcujúcej ére digitalizácie.³⁸

³⁷ Metaverzum z technického pohľadu sleduje: „a) komplexný virtualizovaný alebo virtuálne-fyzický fúzovaný imerzný zážitok, b) online alebo cloud-to-device 3D interaktívny svet s ľudským a zariadeným rozhraním s tímovou spolupracou, c) živú aplikáciu na demonštrovanie dizajnu, aplikácií a služieb, d) ekosystém s obchodnými trhmi, finančnými službami, ekonomickými aktivitami a sociálnymi službami, a e) súbor podporných technológií pre infraštruktúru, rozhrania, interakciu, dizajn a vývojové stroje.“ CAO, Longbing: Decentralized ai: Edge intelligence and smart blockchain, metaverse, web 3, and desc. In: IEEE Intelligent Systems, vydanie 37, číslo 3, 2022. S. 8. Na základe takto vymedzeného technického pohľadu Metaverza je teda zrejmý jeho široký záber, a preto by bolo najvhodnejšie určovať otázky rozhodného práva v prípade mimozmluvného záväzku pri porušeniach doménového mena v Metaverze primárne podľa jeho funkčných a ekonomických väzieb s takýmto mimozmluvným záväzkom.

³⁸ Pozri aj: SLAŠŤAN, Miroslav: Recent developments in European private international law under case law of the Court of Justice. In: Universal, regional, national. Ways of the development of private international law in 21st century. Brno: Masarykova univerzita, 2019. S. 315-335.

Záver

Systémové zdôvodnenie "krízy" kolíznych noriem medzinárodného práva súkromného obsahu v nariadení Rím II vytvára priestor pre novú právnu úpravu, ktorá by adekvátne reagovala na potreby súčasnej digitálnej doby. Jednotlivé články nariadenia, ktoré boli v príspevku predstavené a akými sú menovite: článok 4 zakotvujúci využitie všeobecného pravidla pri posúdení rozhodného práva, článok 6 zakotvujúci rozhodné právo pri nekalosúťažnom konaní a konaní obmedzujúceho slobodnú súťaž, a článok 8 zakotvujúci posúdenie rozhodného práva pri právach duševného vlastníctva, nie sú vo väčšine prípadov adekvátne využiteľné v situácii, kedy bolo porušené doménové meno v prostredí Metaverza. Týmto príspevkom sme preukázali, že odkaz na geograficky viazané kritériá v podobe *lex loci damni infecti* a v podobe *lex loci protectionis*, je v decentralizovanej realite virtuálneho sveta, kde škoda vzniká bez akejkoľvek fyzickej polohy miesta, prakticky ťažko uchopiteľná.

Prekonanie legislatívneho a interpretačného vákuu si vyžaduje najmä radikálny odklon od teritoriálnej paradigmy, ktorá bola doteraz využívaná súdmi členských štátov Európskej únie. Návrh *de lege ferenda* nového ustanovenia, ktoré obsahuje *lex metaversi* je v tomto smere priam nutnosťou, a to aj s prihliadnutím na fakt, že v budúcnosti sa takéto digitálne decentralizované platformy budú naďalej čoraz viac popularizovať a rozvíjať. *Lex metaversi* tak v novej ére digitalizácie nahrádza doterajšie geografické väzby viažuce sa na kolízne kritériá, a nahrádza ich za funkčné a technologické väzby. Takáto novelizácia časti medzinárodného práva súkromného môže byť zásadným krokom k adaptácii tohto odvetvia práva na aktuálnu virtuálnu dobu. Nami navrhované hraničné kritérium *lex metaversi* má potenciál legitimovať väčšinu ekonomických aktivít v priestore Metaverza tým, že poskytne subjektom jasne stanovené pravidlá určovania rozhodného práva pri riešení doménových sporov. Takýmto postupom by nastala žiadaná minimalizácia potreby výberu nevhodných súdov štátov, pri ktorých absenteje zjavne užšia väzba sporu s takýmto štátom, obchádzania práva či potreby extenzívneho výkladu zo strany súdov, či mylnej interpretácie ustanovení nariadenia Rím II.

Na základe nami predostretej analýzy je zrejmé, že bezprecedentná rýchlosť digitalizácie a exponenciálny nárast virtuálnych priestorov, akým je aj Metaverzum, spôsobili neudržateľnosť doteraz ustálených kolíznych kritérií, podľa ktorých sa posudzuje rozhodné právo v prípade mimozmluvného záväzku pri cezhraničných sporoch, ktoré vystali z porušenia doménového mena v Metaverze. Kým doterajšie doménové spory mali jasne stanovené geograficky vymedzené hraničné kolízne kritériá, v súčasnom digitálnom prostredí sa už nie je možné sa na ne spoliehať. Preto je nutné pristúpiť k zamysleniu či budeme aplikovať doteraz platné a účinné normy kolízneho práva obsiahnuté v nariadení Rím II aj na priestor Metaverza, pričom tým riskujeme napríklad prehĺbenie právnej neistoty, alebo vytvoríme nový koncept

v podobe právnej normy či právneho nástroja obsahujúceho *lex metaversi*, ktorý by odzrkadľoval špecifiká úplne ekonomicky sebestačného virtuálneho priestoru.

V súvislosti s nami navrhovaným ustanovením a rýchlo rastúcim digitálnym prostredím a technologickým vývojom, sa však vynára zaujímavá otázka: Ak budeme akceptovať, že *lex metaversi* sa stane účinným a aplikovateľným kolíznym kritériom v medzinárodnom práve súkromnom, nemalo by byť nasledujúcim logickým krokom vytvorenie akéhosi nadnárodného *lex digitalis*, ktorý by úplne eliminoval závislosť na akejkoľvek národnej jurisdikcii štátov?

Zoznam použitej literatúry

1. CAO, Longbing: Decentralized ai: Edge intelligence and smart blockchain, metaverse, web 3, and desc. In: IEEE Intelligent Systems, vydanie 37, číslo 3, 2022. S. 8. ISSN 1541-1672.
2. COLEMAN, Ben: Jurisdiction and torts in the metaverse. 2022. Prípsevok dostupný online na webovom sídle: <https://www.bristows.com/news/jurisdiction-and-torts-in-the-metaverse/>.
3. DAWOOD, Aya Muhammad - KHALIL, Israa Khader: The domain name and other intellectual property rights. In: International Journal of Environmental Sciences, vydanie 11, číslo 12S, 2025. S. 863-876. ISSN: 2229-7359.
4. FEIFEI, Shi, et al.: A new technology perspective of the Metaverse: Its essence, framework and challenges. In: Digital Communications and Networks, vydanie 10, číslo 6, 2024. S. 1653. ISSN 2352-8648.
5. GAETANO, DIMITA, et al.: IP and Metaverse (S)-an Externally Commissioned Research Report. Queen Mary Law Research Paper no. 427/2024, 2024. S. 19. ISBN 978-1-915090-53-9.
6. GLONINA, Vera: Back to the Future with Blockchain Domain Names: Toward a Global Policy to Fight Cybersquatting in Web 3.0. In: Trademark Reporter, vydanie 114, číslo 4, 2024. S. 591-597. ISSN 0041-056X.
7. CHENG, Shenghui: Metaverse. In: Metaverse: Concept, Content and Context. Springer, Cham, 2023. S. 1-23. ISBN 978-3-031-24358-5.
8. KONKOL, Anton: Porušenie prá duševného vlastníctva a otázka určenia rozhodného práva v Európskej únii. In: Právní rozpravy 2014, vydanie 4, 2014. S. 12. ISBN 978-80-87952-02-3.
9. KRAMER, Xandra E.: The Rome II Regulation on the Law Applicable to Non-Contractual Obligations: The European private international law tradition continued – Introductory observations, scope, system, and general rules. In: Netherlands Internationaal Privaatrecht (NIPR), vydanie 4, 2008. S. 415.

10. KUMAR BAL GOVIND, Singh: Online Dispute Resolution in Cross-Border Disputes: A Comprehensive Analysis, 2023. S. 3. DOI: <http://dx.doi.org/10.2139/ssrn.4643682>.
11. KUR, Annette - MAUNSBACH, Ulf: Choice of Law and Intellectual Property Rights. In: Oslo Law Review, vydanie 6, číslo 1, 2019. S. 43-61.
12. LEE, Jyh-An - YANG, Liang - PAN, Hui: Legal Implications of Self-presence in the Metaverse. The Chinese University of Hong Kong Faculty of Law: Media & Arts Law Review, vydanie 25, číslo 4. S. 279-280. SSRN: <https://ssrn.com/abstract=4665569>.
13. LYSINA, Peter, HAŤAPKA, Miloš, BURDOVÁ, Katarína a kol.: Medzinárodné právo súkromné. 3. vydanie. Bratislava: C. H. Beck, 2023. S. 268. ISBN 978-80-8232-031-5.
14. LYSINA, Peter: Kolízne normy v digitálnom veku: výzvy pre medzinárodné právo súkromné. In: Acta Facultatis Iuridicae Universitatis Comenianae, diel 44, číslo 1, 2025. S. 69-94. DOI: <https://doi.org/10.62874/afi.2025.1>.
15. MYSTAKIDIS, Stylianos: Metaverse. In: Encyclopedia 2, číslo 1, 2022. S. 486. DOI: <https://doi.org/10.3390/encyclopedia2010031>.
16. Nariadenie Európskeho parlamentu a Rady (ES) č. 864/2007 z 11. júla 2007 o rozhodnom práve pre mimozmluvné záväzky (Rím II), Ú. v. EÚ L 199, , s. 40 – 49.
17. PELLEGRINI, Cécile: Applicable law in the metaverse: A European International Private Law perspective. In: Research Handbook on the Metaverse and Law, 2024. S. 375-397. ISBN 9781035324859.
18. RODRÍGUEZ, Ana Mercedes López: Towards a Lex Metaversi? The law applicable to virtual real estate in the metaverse. In: Interactive Entertainment Law Review, vydanie 2, číslo 2, 2024. S. 110.
19. SADEGHI-NIARAKI, Abolghasem, et al.: Groundbreaking taxonomy of metaverse characteristics. In: Artificial Intelligence Review, vydanie 58, číslo 244, 2025. S. 19.
20. SLAŠŤAN, Miroslav: Recent developments in European private international law under case law of the Court of Justice. In: Universal, regional, national. Ways of the development of private international law in 21st century. Brno: Masarykova univerzita, 2019. S. 315-335. ISBN 978-80-210-9496-3.
21. SPAIS, George, et al.: A new Walk in the Future of the Metaverse: Marketing Implications for Consumer Behavior. In: Journal of Consumer Behaviour, vydanie 24, číslo 2, 2025. S. 860. ISBN 1479-1838.
22. ZHANG, Jiale - QUOQUAB, Farzana - MOHAMMAD, Jihad: Embracing the new reality: Gen Y's intention to use metaverse apps and devices. In: Curr Psychol, vydanie 44, 2025. S. 398-417. DOI: <https://doi.org/10.1007/s12144-024-07160-5>.

Kontaktné údaje

JUDr. Ema Krkošková

ema.krkoskova@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

Katedra medzinárodného práva a medzinárodných vzťahov

MEDZI FORMÁLNYMI POŽIADAVKAMI A SKUTOČNOU VYKONATEĽNOSŤOU: ANALÝZA NEDOSTATKOV NARIADENIA O DIGITÁLNYCH SLUŽBÁCH V SLOVENSKOM PRÁVNOM PROSTREDÍ¹

BETWEEN FORMAL REQUIREMENTS AND REAL ENFORCEABILITY: ANALYSIS OF THE SHORTCOMINGS OF THE DIGITAL SERVICES ACT IN THE SLOVAK LEGAL ENVIRONMENT

Marián Ruňanin², Igor Sloboda³

Abstrakt: Nariadenie o digitálnych službách (DSA) predstavuje ambiciózny pokus Európskej únie o vytvorenie bezpečnejšieho, transparentnejšieho a zodpovednejšieho online prostredia. Jeho ciele zahŕňajú nielen boj proti nezákonnému obsahu, ale aj posilnenie základných práv používateľov, vrátane práva na účinné opravné prostriedky. Tento článok kriticky analyzuje rozdiel medzi regulačnými cieľmi DSA a jeho praktickou implementáciou, a tvrdí, že súčasná situácia vedie k fenoménu „prázdnej regulácie“. Analýza sa zameriava na dva kľúčové nedostatky. Prvým je nefunkčnosť mechanizmov transparentnosti; hoci platformy formálne sprístupňujú údaje prostredníctvom databáz a správ, ich štrukturálne a metodické obmedzenia bránia zmysluplnej vedeckej, regulačnej a verejnej kontrole. Druhým nedostatkom, ktorý je kľúčový pre vynútiteľnosť práva, je absencia certifikovaných mimosúdnych orgánov na riešenie sporov na Slovensku. To vytvára právne vákuum, v ktorom sú práva používateľov zaručené len na papieri, bez akejkoľvek reálnej možnosti vynútiteľnosti. Na základe týchto zistení článok skúma, do akej miery formálne dodržiavanie DSA platformami maskuje skutočnú absenciu zodpovednosti a prístupu k spravodlivosti, a analyzuje dôsledky tejto situácie na ochranu individuálnych práv v digitálnom veku.

Kľúčové slová: Nariadenie o digitálnych službách, zodpovednosť online platforiem, transparentnosť online platforiem, prístup k spravodlivosti, mimosúdne riešenie sporovo

¹ Tento príspevok je výstupom z grantu GUK 2025 č. UK/1182/2025 s názvom: „*Moderácia obsahu na sociálnych sieťach a sloboda prejavu*“

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra teórie práva a filozofie práva

³ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav európskeho práva

Abstract: The Digital Services Act (DSA) represents an ambitious attempt by the European Union to create a safer, more transparent, and more accountable online environment. Its objectives include not only combating illegal content, but also strengthening the fundamental rights of users, including the right to effective remedies. This article critically analyzes the gap between the regulatory objectives of the DSA and its practical implementation, arguing that the current situation leads to the phenomenon of "empty regulation." The analysis focuses on two key shortcomings. The first is the dysfunctionality of transparency mechanisms; although platforms formally make data available through databases and reports, their structural and methodological limitations prevent meaningful scientific, regulatory, and public scrutiny. The second shortcoming, which is crucial for the enforceability of the law, is the absence of certified out-of-court dispute resolution bodies in Slovakia. This creates a legal vacuum in which users' rights are guaranteed only on paper, without any real possibility of enforcement. Based on these findings, the article examines the extent to which the formal compliance of platforms with the DSA masks a real absence of accountability and access to justice, and analyzes the implications of this situation for the protection of individual rights in the digital age.

Key words: Digital Services Act, Responsibility of Online Platforms, Transparency of Online Platforms, Access to Justice, Out-of-court Dispute Resolution

Úvod

Každá technologická revolúcia so sebou prináša moment spoločenského šoku. Príchod prvého automobilu bol presne takouto udalosťou, fascinujúcim príslubom pokroku, ktorého dôsledky si v plnej miere nedokázal predstaviť nikto. Spoločnosť spočiatku vnímala najmä bezprostredné výhody: schopnosť preklenúť vzdialenosti, zrýchliť cestovanie a otvoriť nové možnosti pre obchod a osobnú slobodu. S masovým rozšírením automobilov sa však začali prejavovať aj ich negatívne externality, teda nielen chaotické situácie na neregulovaných cestách, ale predovšetkým tragické ujmy na zdraví a stratách na životoch. Rýchlosť, s akou táto technológia prenikla do každodenného života, si nevyhnutne vyžiadala novú, komplexnú formu štátneho zásahu. Zavedenie dopravných predpisov, technických noriem a pravidiel zodpovednosti nebolo len administratívnym cvičením, ale fundamentálnou odpoveďou na potrebu ochrániť spoločnosť pred deštruktívnym potenciálom neregulovanej inovácie.

S istou mierou zjednodušenia môžeme v nástupe internetu a neskôr v dominantnom postavení veľkých online platforiem vidieť paralelu k tejto historickej skúsenosti.

Počiatočná fáza digitálnej éry bola charakteristická takmer úplnou absenciou špecifickej regulácie. Tento stav nebol náhodný; bol výsledkom vedomého politického rozhodnutia. Štáty po celom svete vytvorili pre platformy priaznivé podnikateľské prostredie s nízkymi nákladmi, a to najmä prostredníctvom zavedenia rozsiahlych výnimiek zo zodpovednosti za obsah tretích strán.⁴ Tento prístup, známy ako princíp „*bezpečného prístavu*“, mal podporiť inovácie a slobodný rozvoj internetu, no zároveň viedol k situácii, kde platformy mohli profitovať z obsahu bez toho, aby niesli plnú zodpovednosť za škody, ktoré tento obsah mohol spôsobiť.

Model "samoregulácie",⁵ postavený na minimálnych zásahoch a rozsiahlych imunitách, sa však postupom času ukázal ako dlhodobu neudržateľný, najmä v kontexte Európskej únie, kde sa čoraz intenzívnejšie vynárali otázky systémových rizík.⁶ Problémy ako šírenie dezinformácií, hybridné hrozby či manipulatívne využívanie algoritmov odhalili, že absencia zmysluplnej regulácie má vážne spoločenské dôsledky. Zároveň sa stávalo čoraz zrejmejším, že netransparentné a často nekonzistentné pravidlá moderovania obsahu, ktoré si platformy stanovovali samy, im zverili rolu faktických arbitrov verejnej diskusie bez akejkoľvek demokratickej kontroly. Internet sa zmenil z okrajovej technológie na infraštruktúru každodenného života,⁷ a tým sa služby dovtedy takmer neregulovaných platforiem stali centrálnym priestorom pre prácu, vzdelávanie aj spoločenskú interakciu. V tomto novom kontexte sa prístup samoregulácie, ktorý platformám ponechával takmer voľnú ruku, javil nielen ako nepostačujúci, ale priam nebezpečný. Európska únia preto dospela k záveru, že je nevyhnutné prejsť k novej, asertívnejšej forme regulácie. Výsledkom tohto úsilia je práve Nariadenie o digitálnych službách, ktoré predstavuje komplexný pokus o zavedenie poriadku, zodpovednosti a ochrany

⁴ V Spojených štátoch amerických táto „imunita“ vychádza priamo z § 230 zákona „Communications Act of 1934“. Dodnes jeho existencia je predmetom viacerých akademických sporov, najmä či je táto výnimka v súčasnom digitálnom prostredí udržateľná.

⁵ K analýze modelov regulácie online prostredia odporúčame článok: MARSDEN, Chris - MEYER, Trisha – BROWN, Ian: Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation? In: Computer Law & Security Review Volume 36, April 2020. ISSN: 2212-473X [online]. Dostupné na: <https://doi.org/10.1016/j.clsr.2019.105373> (cit. 25.09.2025)

⁶ Pozri dôvodovú správu k návrhu nariadenia o digitálnych službách, kde sa uvádza, že samoregulačné iniciatívy mali síce priaznivé výsledky, no neboli právne presadzovateľné a nevzťahovali sa na všetkých účastníkov digitálneho hospodárstva, čo spolu s právnou roztrieštenosťou znížovalo efektívnosť rámca smernice o elektronickom obchode.

⁷ Len sociálne siete využíva viackrát denne viac než 60 % Slovákov, čo je ohromný nárast voči roku 2001, kde internet ako taký používalo len 18 % Slovákov. Pre viac informácií pozri: HRNČÁROVÁ, Katarína: Koľko Slovákov je na sociálnych sieťach? Prekvapujú seniori, poukazujú na nový trend In: Trend. 20. Októbra 2024. [online]. Dostupné na: <https://medialne.trend.sk/internet/kolko-slovakov-je-socialnych-sietach-prekvapuju-seniori-ich-pouzivanie-ukazuje-novy-trend> (cit. 25.09.2025).

základných práv do digitálneho ekosystému. Práve toto nariadenie a jeho praktické dopady na postavenie používateľov budú predmetom analýzy tohto článku.

DSA ako nástroj ochrany slobody prejavu

O Nariadení o digitálnych službách (v článku ďalej len ako „DSA“) sa viedli v neakademickom a najmä politicko-mediálnom priestore kritické diskusie, ktoré označovali DSA ako nástroj „cenzúry“ či obmedzovania slobody prejavu.⁸ My sa však na DSA pozeráme aj z iného uhla pohľadu, ako na nástroj ochrany slobody prejavu, najmä užívateľov digitálnych služieb. Tento pohľad vieme zdôvodniť dvoma aspektami DSA, ktoré sú: pravidlá o transparentnosti moderácie obsahu na digitálnych platformách a mimosúdne riešenie sporov v tomto vecnom rozsahu.

Pilier transparentnosti je základom, na ktorom stojí celá architektúra zodpovednosti. Platformy sú po novom povinné nielen formulovať svoje zmluvné podmienky jasne a predvídateľne, ale musia aj detailne odôvodniť každé jednotlivé rozhodnutie o obmedzení obsahu voči konkrétnemu používateľovi. Cieľom tejto povinnosti je napraviť informačnú asymetriu a umožniť používateľom „pochopiť, prečo bolo prijaté konkrétne rozhodnutie a posúdiť, či ho chcú napadnúť“. Tým, že platforma musí svoje konanie vysvetliť, sa výrazne znižuje priestor pre svojvoľné či politicky motivované zásahy do obsahu, ktorý je síce kontroverzný, ale legálny. Transparentnosť sa tak stáva prvou obrannou líniou slobody prejavu, pretože núti platformy konať na základe vopred stanovených pravidiel, a nie na základe momentálnych a nevyspytateľných pohnútok.⁹ Druhým, a pre vymožitelnosť práv rovnako dôležitým pilierom je vytvorenie systému nápravy. DSA ukladá platformám povinnosť zriadiť efektívny interný mechanizmus na vybavovanie sťažností.¹⁰ Skutočnou inováciou je však zavedenie práva používateľa obrátiť sa na certifikovaný orgán mimosúdneho riešenia sporov, ak so svojou internou sťažnosťou neuspeje. Tieto orgány majú slúžiť ako „nezávislí arbitri, ktorí poskytujú dostupnú a rýchlu alternatívu k súdnemu konaniu“. Ich úlohou je nestranne posúdiť, či rozhodnutie platformy bolo v súlade s jej vlastnými zmluvnými podmienkami a s právom. Tým sa do systému vnáša prvok externej kontroly, ktorý bol doteraz úplne neprítomný. Používateľ už nie je odkázaný len na interné postupy platformy, kde je v zjavne nerovnom postavení, ale získava možnosť nechať spor posúdiť treťou, nezávislou

⁸ Napr.: ONAČILLA, Jozef: Cenzúra nevidaných rozmerov? Európska únia chce krotiť online priestor nejasnými pravidlami. In: Štandard. 30. Decembra 2023. [online]. Dostupné na: <https://standard.sk/530407/cenzura-nevidanych-rozmerov-europska-unia-chce-krotit-online-priestor-nejasnymi-pravidlami> (cit. 25.09.2025).

⁹ FOLKERT, Wilman - KALÉDA, Saulius Lukas - LOEWENTHAL, Paul-John: The EU Digital Services Act A Commentary – 1st. ed. Oxford: Oxford University Press, 2024. s. 145.

¹⁰ Tamtiež, s. 164 – 171.

stranou. Práve táto kombinácia vynútenej transparentnosti a dostupných mechanizmov nápravy mení povahu vzťahu medzi používateľom a platformou a predstavuje reálny nástroj na ochranu slobody prejavu pred jej neodôvodneným obmedzovaním zo strany súkromných aktérov.¹¹

Mimosúdne orgány riešenia sporov podľa DSA

Právna úprava a reálna prax však môže byť niekedy diametrálne odlišná, a zamýšľané ciele nemuseli byť nevyhnutne dosiahnuté. V tejto časti článku sa budeme venovať certifikovaným orgánom mimosúdneho riešenia sporov (V článku ďalej len ako „certifikovaný orgán“), a teda jeho súčasnej praxi. Ako upozorňuje Husovec, cieľom článku 21 DSA je dvojitý: na jednej strane umožniť používateľovi nezávislé a rýchle preskúmanie rozhodnutia platformy, na druhej strane vytvoriť finančný stimul pre platformy, aby robili menej chýb už vo svojich interných procesoch. Tento mechanizmus však nie je koncipovaný ako záväzné rozhodovanie, ale skôr ako systém „druhého názoru“, ktorý síce poskytovatelia nemôžu ignorovať systematicky, no v jednotlivých prípadoch môžu odmietnuť jeho implementáciu. Účinnosť certifikovaných orgánov tak bude do veľkej miery závisieť od toho, či ich platformy budú rešpektovať v praxi a či národní digitálni koordinátori dokážu zabezpečiť férovú certifikáciu a dohľad nad ich fungovaním.¹² Na tento problém nadväzuje aj novšia literatúra, ktorá zdôrazňuje, že certifikované orgány majú priniesť nielen alternatívu k súdnemu konaniu, ale aj zvýšiť dôveryhodnosť celého systému riešenia sporov medzi používateľmi a platformami. Ide o pokus vybudovať sieť nezávislých arbitrov, ktorých činnosť má byť prístupná, rýchla a nákladovo efektívna. Zároveň však upozorňujú na viacero otvorených otázok, od zložitosti certifikačných kritérií, cez hrozbu nadmernej fragmentácie praxe medzi členskými štátmi, až po riziko, že najväčšie platformy si budú vyberať len tých poskytovateľov, ktorí im budú najviac vyhovovať. Tieto faktory môžu oslabiť očakávaný prínos mechanizmu a spôsobiť, že v niektorých prípadoch sa pôvodný cieľ vyrovnať nerovnováhu síl medzi používateľom a platformou, nepodarí dosiahnuť.¹³

¹¹ Tamtiež, s. 171 – 183.

¹² HUSOVEC, Martin: Certification of Out-of-Court Dispute Settlement Bodies under the Digital Services Act. In: London School of Economics, Londýn 2023. [online]. Dostupné na: <https://doi.org/10.2139/ssrn.4501726> (cit. 25.09.2025).

¹³ HARRISON, Ruairí - SHIPP, Jonny - CURTIS, Aebha: Settling DSA-Related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act. (May 15, 2024) [online]. Dostupné na: <https://doi.org/10.2139/ssrn.4787648> (cit. 25.09.2025).

Mimosúdne orgány riešenia sporov podľa DSA v podmienkach SR

Po našom výskume sme zistili, že v tejto časti DSA nedokázala naplniť očakávania používateľov a teda zvýšiť zodpovednosť platforiem. Nemusí to byť však nevyhnutne problém DSA ako takej. Na Slovensku ani v Česku neexistuje žiaden certifikovaný orgán. V Česku je situácia jasnejšia práve kvôli absencii právnej úpravy, keďže plánovaný zákon o digitálnej ekonomike nebol doteraz schválený, primárne z politických dôvodov.¹⁴ Na Slovensku však máme všetky potrebné právne predpisy na vytváranie týchto orgánov. K dnešnému dňu na Slovensku neexistuje ani jeden orgán, ktorý by bol koordinátorom digitálnych služieb¹⁵ certifikovaný na mimosúdne riešenie sporov podľa DSA. Pre používateľa na Slovensku, ktorého sťažnosť platforma zamietne, tak vzniká slepá ulička. Jeho právo na ďalší účinný opravný prostriedok, ktoré mu nariadenie garantuje, sa stáva iluzórnym. V praxi mu nezostáva nič iné, ako sa buď zmieriť s rozhodnutím globálnej technologickej firmy, alebo sa pustiť do náročného a neistého súdneho sporu, čo je pre väčšinu jednotlivcov neprekonateľná prekážka. Tým sa celý viac stupňový systém nápravy, ako ho DSA navrhlo, rúca a z práva na papier sa stáva právo nevyžiteľné. Problém teda nespočíva v absencii európskeho či národného legislatívneho rámca, ale v tom, že sa zatiaľ nenašiel žiadny subjekt, ktorý by sa tejto úlohy ujal a splnil náročné kritériá na certifikáciu. Pohľad na mapu Európskej únie tento deficit ešte viac prehľbuje. Zoznam, ktorý vedie Európska komisia, ukazuje, že v krajinách ako Nemecko, Francúzsko, Holandsko či Taliansko¹⁶ už takéto orgány fungujú a ponúkajú používateľom reálnu možnosť preskúmania rozhodnutí platforiem. Tento kontrast jasne demonštruje, že vízia DSA je síce uskutočniteľná, no jej naplnenie si vyžaduje existenciu a iniciatívu nezávislých a odborne zdatných entít v rámci jednotlivých štátov. Absencia certifikovaného orgánu na Slovensku tak nie je technickým detailom, ale zásadným praktickým nedostatkom, ktorý podkopáva samotný zmysel ochrany používateľa. Vytvára sa tak právne vákuum, v ktorom sa ambiciózny regulačný rámec mení na prázdnu kulisu a práva používateľov, vrátane ochrany ich slobody prejavu, zostávajú garantované len formálne, bez skutočnej možnosti ich reálneho uplatnenia.

Prečo je absencia takéhoto orgánu na Slovensku, je zaujímavá situácia. Na prvý pohľad by sa mohlo zdať, že pozícia certifikovaného orgánu mimosúdneho riešenia sporov je mimoriadne atraktívna. Akt o digitálnych službách totiž v článku 21 odsek

¹⁴ HRDLIČKA, Jan: Zákon ostal na „mŕtvom bode“. In: Echo24. 26. Augusta 2025. [online]. Dostupné na: <https://www.echo24.cz/a/HvNXx/zpravy-domov-snemovna-mrtvy-bod-bitcoiny-afery-obstrukce-poslanci-vysvetluji-nic-nestihnou> (cit. 25.09.2025).

¹⁵ Rada pre mediálne služby

¹⁶ Zoznam certifikovaných orgánov je dostupný online: <https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement>

5 stanovuje, že platformy sú povinné znášať primerané trovy konania, čím sa odstraňuje finančná bariéra nielen pre používateľov, ale aj pre samotné orgány. Tento model vytvára ideálne podmienky pre vznik nezávislých inštitúcií, ktoré by mohli fungovať ako dôležitý korektív voči moci veľkých technologických firiem bez toho, aby sa museli obávať o svoje financovanie. Prečo teda, napriek tejto zdanlivej príležitosti, zostáva na Slovensku táto pozícia neobsadená?

Odpoveď pravdepodobne nespočíva v jedinom zjavnom dôvode, ale v súhre viacerých komplexných bariér, teda finančných, právno-štrukturálnych a najmä kvalifikačných, ktoré výrazne sťažujú vstup do tejto novej a náročnej sféry regulácie. V prvom rade, hoci prevádzkové náklady konania znášajú platformy, samotné založenie a udržanie funkčnosti takéhoto orgánu si vyžaduje značný počiatočný kapitál a finančnú odolnosť. Potenciálny orgán, ktorý má najčastejšie formu neziskovej organizácie, musí ešte pred získaním certifikácie investovať do personálneho zabezpečenia, technickej infraštruktúry a vytvorenia komplexných procesných pravidiel. Získanie takéhoto kapitálu bez komerčných väzieb, ktoré by mohli ohroziť nezávislosť, je samo osebe výzvou. Navyše, orgán musí byť pripravený na riziko, že platformy nebudú jeho rozhodnutia rešpektovať alebo budú jeho kompetencie spochybňovať súdnou cestou. Prípadné súdne spory s globálnymi technologickými gigantmi predstavujú enormné finančné a právne riziko, ktoré si vyžaduje silné finančné zázemie. Bez neho sa môže aj ten najlepšie úmyselný projekt stať neudržateľným, čo odrádza potenciálnych zakladateľov, ktorí nemajú za sebou podporu silného mecenáša či inštitucionálneho partnera. Ďalšiu prekážku predstavuje právno-štrukturálna nejednotnosť v Európe. Akt o digitálnych službách síce vytvára jednotný funkčný rámec pre mimosúdne riešenie sporov, no právnu formu a štruktúru samotných orgánov ponecháva na vnútroštátne právo.

Právne prostredie pre fungovanie neziskových organizácií, nadácií či iných vhodných entít sa však v jednotlivých členských štátoch výrazne líši. Zatiaľ čo v niektorých krajinách môže byť založenie takejto organizácie relatívne flexibilné, v iných, ako napríklad na Slovensku, podlieha pomerne prísny a detailným pravidlám. Táto heterogenita môže vytvárať nerovnaké podmienky a komplikovať vznik cezhraničných alebo paneurópskych riešení. Vzniká tak paradox, kde harmonizovaná európska regulácia naráža na neharmonizované národné právne rámce, čo môže spomaľovať alebo úplne blokovать vznik potrebných inštitúcií. Azda najvýznamnejšou bariérou sú však mimoriadne prísne a komplexné podmienky na získanie certifikácie, ktoré sa týkajú nezávislosti, odbornosti a administratívnej pripravenosti.

Analýza oficiálnej žiadosti o udelenie štatútu orgánu mimosúdneho riešenia sporov odhaľuje, že ide o oveľa viac než len o administratívny proces. Žiadateľ musí preukázať, že spĺňa prísne kritériá, ktoré sú navrhnuté tak, aby zabezpečili jeho absolútnu bezúhonnosť a profesionalitu. Kľúčovou podmienkou je preukázaná nezávislosť. Nejde len o formálne vyhlásenie; žiadateľ musí detailne popísať svoju

organizačnú štruktúru, zdroje financovania a interné pravidlá, aby jednoznačne preukázal, že je chránený pred akýmkoľvek vonkajším vplyvom, či už zo strany platforiem, alebo iných záujmových skupín. Tento imperatív nestrannosti môže byť pre mnohé existujúce organizácie, ktoré majú väzby na komerčný sektor alebo sa venujú advokácii, neprekonateľnou prekážkou. Ešte náročnejšou požiadavkou sa však javí byť preukázanie odbornej spôsobilosti. Podľa žiadosti sa vyžadujú „preukázateľné odborné znalosti a skúsenosti“, ktoré idú ďaleko za rámec všeobecného právneho vzdelania. Potenciálny orgán musí disponovať expertízou v komplexnej a dynamicky sa vyvíjajúcej oblasti, ktorá zahŕňa nielen právo, ale aj hlboké porozumenie fungovaniu online platforiem, problematike moderovania obsahu a predovšetkým ochrane základných práv, s osobitným dôrazom na slobodu prejavu. Žiadosť vyžaduje predloženie životopisov osôb, ktoré budú spory rozhodovať, aby sa ich kvalifikácia dala overiť. V slovenskom prostredí môže byť však počet expertov, ktorí by spĺňali takúto multidisciplinárnu a špecifickú kvalifikáciu, veľmi obmedzený. Okrem toho musí žiadateľ už vopred vypracovať a predložiť podrobné a spravodlivé pravidlá postupu, ktoré budú v súlade s DSA. To predstavuje značnú administratívnu a právnu záťaž ešte predtým, ako orgán vôbec začne fungovať a riešiť prvý spor (na druhej strane tieto podmienky sú pochopiteľné). Kombinácia týchto faktorov, teda požiadavka na absolútnu nezávislosť, vysokošpecializovanú expertízu a pripravenosť niesť administratívnu záťaž, vytvára vysokú bariéru vstupu. Faktom ale ostáva, že podmienky sú formulované aj široko, teda je plne na Rade pre mediálne služby ako vyhodnotí splnenie týchto požiadaviek.¹⁷ Problém teda nemusí byť primárne v tom, že by neexistoval udržateľný finančný model prevádzky, ale v tom, že na Slovensku zrejme chýba inštitucionálna a personálna kapacita, teda "ľudský kapitál", schopná tieto náročné podmienky naplniť.

Práve táto medzera v odbornosti a kapacitách môže byť hlavným dôvodom, prečo kľúčový prvok systému nápravy podľa DSA na Slovensku zatiaľ existuje len ako teoretická možnosť. To len prehlbuje fenomén „prázdnej regulácie“, kde práva síce formálne existujú, no v praxi chýbajú inštitúcie schopné zabezpečiť ich reálnu vymožiteľnosť. A tým pádom nie je zodpovednosť platforiem riadne naplnená.

Využívanie orgánov mimosúdneho riešenia sporov

Ako bolo uvedené v predchádzajúcej kapitole, článok 21 ods. 1 nariadenia DSA priznáva príjemcom služieb právo iniciovať mimosúdne urovnanie sporov, pokiaľ sa jedná o rozhodnutia podľa článku 20 ods. 1 DSA. Certifikácia príslušného mimosúdneho orgánu je v tomto prípade platná v rámci celého územia EÚ, čo

¹⁷ Podmienky sú dostupné online: <https://rpms.sk/ziadost-o-statut-organu-mimosudneho-riesenia-sporov>

odstraňuje bariéry spojené s otázkou teritoriálnej pôsobnosti jednotlivých mimosúdnych orgánov a zároveň zvyšuje dostupnosť mechanizmov riešenia sporov medzi príjemcami a poskytovateľmi služieb.¹⁸

Poskytovatelia služieb sú zároveň povinní v rámci svojich pravidelných správ o transparentnosti zverejňovať nielen informácie podľa článku 15 DSA, ale aj údaje o prebiehajúcich mimosúdnych sporoch a o počte sporov, ktoré boli urovnané.¹⁹

V rámci realizovaného výskumu sme sa sústredili na dve platformy - XVideos a Stripchat. V oboch prípadoch ide o poskytovateľov služieb zameraných na obsah pre dospelých, pričom rozdiel medzi nimi spočíva v spôsobe poskytovania služieb. Kým platforma XVideos sa zameriava predovšetkým na sprístupňovanie nahratého obsahu vo forme videí a fotografií, platforma Stripchat sa zameriava na živé vysielanie obsahu pre dospelých. Tento rozdiel v spôsobe poskytovania služieb je z hľadiska uplatňovania požiadaviek DSA podstatný, keďže pri živom vysielaní je potrebná promptnejšia a flexibilnejšia reakcia poskytovateľa služieb v porovnaní s obsahom, ktorý je nahratý.

Analyzovaným obdobím bol jún 2024 až jún 2025. V prípade platformy Stripchat pokrývali uvedené obdobie dve správy o transparentnosti – z decembra 2024 a júna 2025. V rámci oboch správ platforma Stripchat informovala, že za dané obdobie nebol z jej strany zaznamenaný ani jeden prebiehajúci spor pred certifikovanými mimosúdnyimi orgánmi.²⁰

V prípade platformy XVideos pokrývajú skúmané obdobie opätovne dve správy o transparentnosti – z februára 2025 a z augusta 2025. Obdobný výsledok prinieslo aj skúmanie správ od platformy XVideos, ktorá rovnako ako v prípade platformy Stripchat, v oboch správach o transparentnosti uviedla, že za dané obdobie nebol z jej strany zaznamenaný ani jeden prebiehajúci spor pred certifikovanými mimosúdnyimi orgánmi.²¹

Príkazy vydané príslušnými vnútroštátnymi orgánmi

Jednou z povinností, ktoré poskytovateľom sprostredkovateľských služieb vyplývajú z nariadenia DSA, je povinnosť minimálne raz ročne zverejniť ľahko dostupnú správu o transparentnosti. V súlade s článkom 15 ods. 1 písm. a DSA musia tieto správy obsahovať informácie týkajúce sa akéhokoľvek moderovania obsahu, ktoré v období na ktoré sa príslušná správa vzťahuje, uskutočnili. Tieto správy majú okrem

¹⁸ FOLKERT, Wilman - KALÉDA, Saulius Lukas - LOEWENTHAL, Paul-John: The EU Digital Services Act A Commentary – 1st. ed. Oxford: Oxford University Press, 2024. s. 175.

¹⁹ Článok 24 ods. 1 písm. a DSA

²⁰ Stripchat DSA Transparency Report – December 2024 a June 2025.

²¹ WebGroup Czech Republic, a. s. (xvideos.com) Transparency Report – June / December 2024 p. 21 a January / June 2025 p. 22.

uvedených informácií obsahovať aj dáta o počte príkazov od príslušných orgánov členských štátov týkajúce sa konaní proti nezákonnému obsahu podľa článku 9 DSA a príkazov na poskytnutie informácií podľa článku 10 DSA. Tieto dáta majú byť v zmysle už zmieneného článku 15 ods. 1 písm. a v správe roztriedené podľa kategórie nezákonného obsahu, členského štátu, ktorého orgán príkaz vydal a informácie o mediáne času, ktorý bol potrebný na informovanie orgánu a o vykonaní príkazu. V rámci nasledujúceho textu sa podrobnejšie pozrieme na tieto dva druhy príkazov, ako sa s nimi v rámci svojich správ o transparentnosti vysporiadala stránka XVideos.com.²²

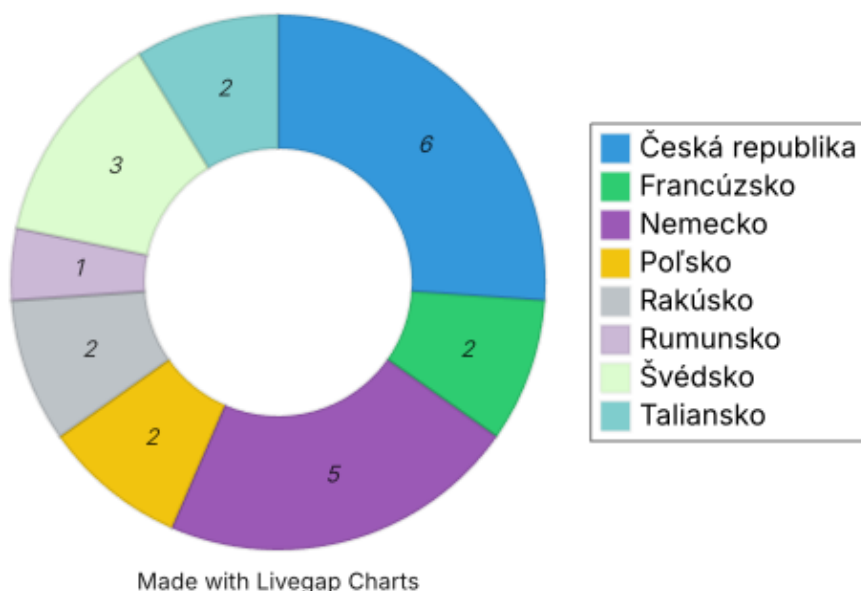
Zo zverejnenej správy o transparentnosti za obdobie jún až december 2024 vyplýva, že príslušné orgány žiadali konať zo strany XVideos proti nelegálnemu obsahu len v jednom prípade, pričom išlo o žiadosť orgánov Portugalska vo veci vydierania. V prípade príkazov na poskytnutie informácií, poslali príslušné orgány 8 členských štátov spolu 23 príkazov týkajúcich sa informácií o konkrétnych používateľoch služby. Išlo o príkazy od príslušných orgánov Českej Republiky, Francúzska, Nemecka, Poľska, Rakúska, Rumunska, Švédska a Talianska. Najviac príkazov pochádzalo v rámci zverejneného obdobia od českých orgánov - 6 nasledované nemeckými s 5 príkazmi. Švédske orgány adresovali 3 príkazy, Rakúsko, Francúzsko, Taliansko a Poľsko po 2 príkazy a Rumunsko 1. Príkazy slovenských orgánov, ktoré sú jedným z objektov nášho výskumu, neboli v rámci príslušnej správy uvedené. Zo zverejnených dát zároveň vyplýva, že časový medián na vyhovie príkazu bol 48 hodín. V prípade, ak sa zameriame len na Českú Republiku a Nemecko, tak je medián 168, respektíve 25 hodín.²³

²² Analýza sa zameriava na erotické platformy, a to z dôvodu, že akademická aj regulačná pozornosť sa v prevažnej miere koncentruje na veľké sociálne siete. Tým však zostáva v úzadí skutočnosť, že aj erotické platformy sú významným zdrojom nelegálneho obsahu, ktorý si vyžaduje osobitnú pozornosť.

²³ WebGroup Czech Republic, a. s. (xvideos.com) Transparency Report – June / December 2024 p. 5.

Počet príkazov na poskytnutie informácií

Jún 2024 - December 2024



Graf č.1 "Počet príkazov na poskytnutie informácií podľa článku 10 DSA"

Čo sa týka samotnej kategorizácie nelegálneho obsahu, v prípade príkazov od českých orgánov sa obsah týkal po jednom prípade "non-consensual" a tzv. "revenge porn". Zvyšné prípady spadali do kategórie tzv. iné, kde v rámci zverejnenej správy nemáme dotknutý obsah bližšie charakterizovaný ani zo strany žiadajúcich orgánov, ani zo strany platformy. V prípade príkazov od nemeckých orgánov, máme po jednom prípade v kategórii "non-consensual", znásilnenie, vek pod zákonom a dva prípady nám spadajú do kategórie iné, pričom v jednom prípade máme bližšie charakterizované, že v danom prípade išlo zo strany podozrivej osoby o vytvorenie používateľského účtu s menom žalobcu.²⁴

Zo správy za obdobie január až jún 2025 vyplýva, že v uvedenom čase prijal Xvideos od príslušných štátnych orgánov členských štátov rovnako len jeden príkaz týkajúci sa nelegálneho obsahu. Tento príkaz pochádzal od orgánu Portugalska, pričom zo správy vyplýva, že sa jednalo o falošný profil, ktorý mal byť podľa príkazu vymazaný. Vykonal príkaz trvalo v tomto prípade 192 hodín.²⁵

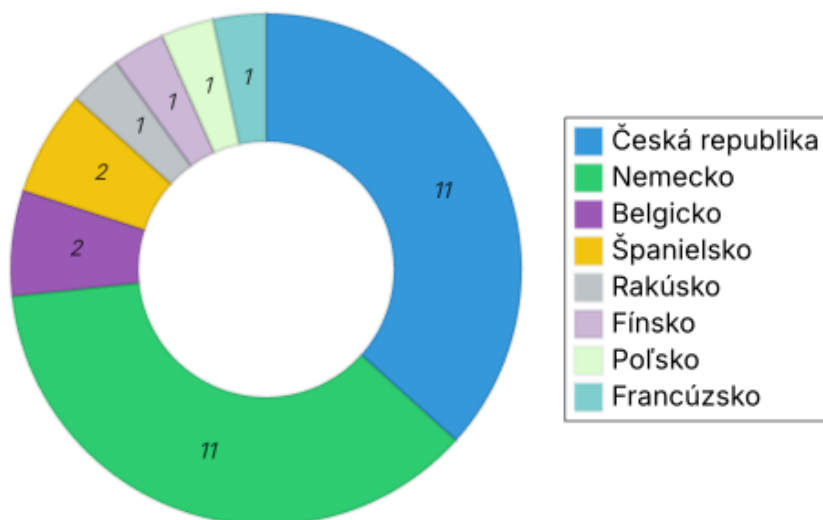
²⁴ Tamtiež s. 4 – 5.

²⁵ WebGroup Czech Republic, a. s. (xvideos.com) Transparency Report – January / June 2025 s. 4.

V prípade príkazov na poskytnutie informácií, poslali príslušné orgány 8 členských štátov spolu 30 príkazov týkajúcich sa používateľov služby. Tieto príkazy pochádzali od orgánov Belgicka, Českej Republiky, Fínska, Francúzska, Nemecka, Poľska, Rakúska a Španielska. Príkazy slovenských orgánov, ktoré sú jedným z objektov nášho výskumu, neboli v rámci príslušnej správy uvedené. Čo sa týka počtu príkazov, najviac ich prišlo od orgánov Českej Republiky (v ktorej má spoločnosť prevádzkujúca Xvideos.com svoje sídlo) a Nemecka – po 11, nasledované Belgickom a Španielskom s 2 príkazmi a zvyšné krajiny mali zhodne po 1 príkaze. Na základe zverejnených dát vyplýva, že časový medián na vyhovení príkazu bol 24 hodín. V prípade zamerania sa čisto len na Českú Republiku a Nemecko, je mediánom v prípade Českej Republiky 192 hodín a v prípade Nemecka medián 5 hodín.²⁶

Počet príkazov na poskytnutie informácií

Január 2025 – Jún 2025



Made with Livegap Charts

Graf č.2 "Počet príkazov na poskytnutie informácií podľa článku 10 DSA"

V prípade príkazov zaslaných od orgánov Českej republiky nám nie je známa konkretizácia nelegálneho obsahu, nakoľko ten je v rámci zverejnenej správy zaradený pod kategóriu iné, pričom ani v rámci opisu podkategórií, ktoré sa vyplňajú v prípade kategórie iné, nebola zo strany orgánov ani platformy v rámci správy žiadna konkretizácia. Je preto v našom prípade náročné vyhodnotiť, ako pristúpil Xvideos k riešeniu tohto obsahu, nakoľko nám zo správy nevyplývajú v tomto prípade žiadne bližšie informácie a konkrétnosti. Jediným smerodajným údajom je tak pre nás len

²⁶ Tamtiež s. 4 – 5.

časový rámec, v rámci ktorého bol príkaz vykonaný a príslušný orgán informovaný, ako aj medián vo vzťahu k českým orgánom.²⁷

Odišne sme na tom v prípade zverejnených dát vo vzťahu k príkazom pochádzajúcim od príslušných orgánov Nemecka. V tomto prípade príkazy nespádali výlučne do kategórie ostatné, ale do kategórií obchod s drogami (1), vydieranie (3), podvod (1), hate speech (1), detská pornografia (2), non consensual (2) a násilie (1).²⁸ Podrobnosti o jednotlivých príkazoch však zo správy nevyplývajú a opätovne je tak pre nás ďalším smerodajným údajom len časový aspekt vyhoveniu príkazu, informovania orgánu a medián. Ako sme uviedli v jednom z predchádzajúcich odsekov, ten je v porovnaní s Českou Republikou výrazne kratším, pričom z dát vyplýva, že aj v jednotlivých prípadoch bolo konanie vo vzťahu k Nemeckým orgánom kratšie.

Druhou skúmanou platformou bol portál Stripchat. Hneď môžeme pristúpiť k porovnaniu jednotlivých správ o transparentnosti oboch platforiem. Kým v prípade platformy XVideos, ide o podrobnejšie a obsiahlejšie správy, v prípade platformy Stripchat, ide už o na prvý pohľad stručnejšie správy, v rámci ktorých absentujú niektoré dáta, ktoré uvádza platforma XVideos. Zo zverejnenej správy za obdobie 1. jún až 30. November 2024 vyplýva, že platforma neobdržala od príslušných orgánov členských štátov žiaden príkaz týkajúci sa nelegálneho obsahu. V prípade príkazov na poskytnutie informácii sa na platformu obrátili 4 členské štáty - Španielsko, Nemecko, Švédsko a Cyprus. Zo zverejnenej správy však nie je možné zistiť presný počet príkazov, ktoré príslušné orgány platforme adresovali. Zo zverejnených dát je ďalej možné vyčítať počet prípadov týkajúcich sa podvodov a podvodného konania - Španielsko (4), Nemecko (5), Švédsko (0) a Cyprus (1) a ako aj počet nelegálneho obsahu - Španielsko (0), Nemecko (1), Švédsko (1), Cyprus (2). Tieto údaje sú tak jediné z ktorých môžeme dedukovať, že počet príkazov podľa článku 10 DSA bol pravdepodobne nasledovný - Nemecko (6), Španielsko (4), Cyprus (3), Švédsko (1). Zo strany platformy nám v tomto prípade absentujú akékoľvek ďalšie podrobnejšie informácie, ako aj charakteristiky jednotlivých prípadov. Zo správy tak nevieme zistiť, čoho konkrétne sa podvodné konanie malo týkať, prípadne v čom spočívalo nelegálne konanie. Rovnako tak absentuje aj časový údaj pri jednotlivých prípadoch, na základe čoho by sme vedeli vyhodnotiť, ako dlho trvá priemerné vyhovenie príkazu pre jednotlivé krajiny. Z časového hľadiska platforma zverejnila medián, ktorý bol v danom období 72 hodín, pričom však nemáme dostupné dáta z ktorých pri jeho výpočte platforma vychádzala.²⁹

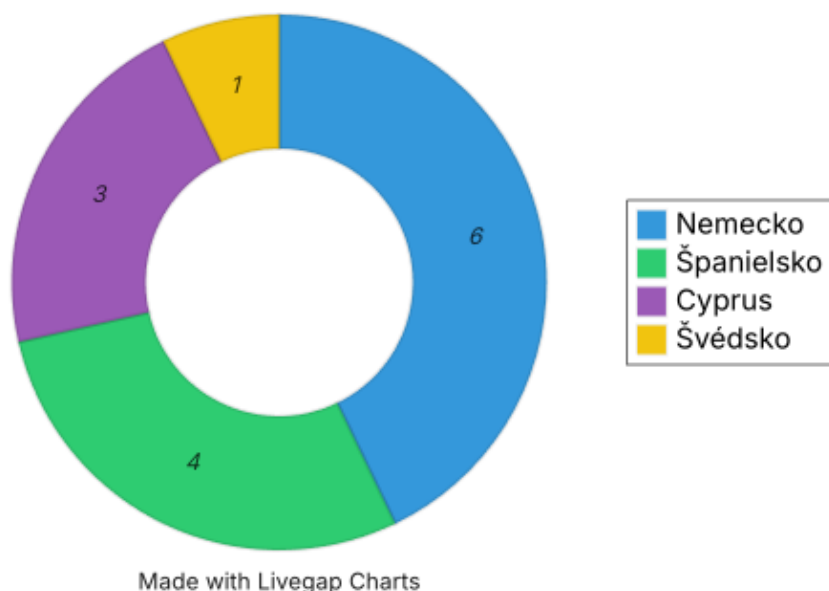
²⁷ Tamtiež s. 4 – 5.

²⁸ Tamtiež s. 4 – 5.

²⁹ Stripchat DSA Transparency Report – December 2024.

Počet príkazov na poskytnutie informácií

Jún 2024 - November 2024



Graf

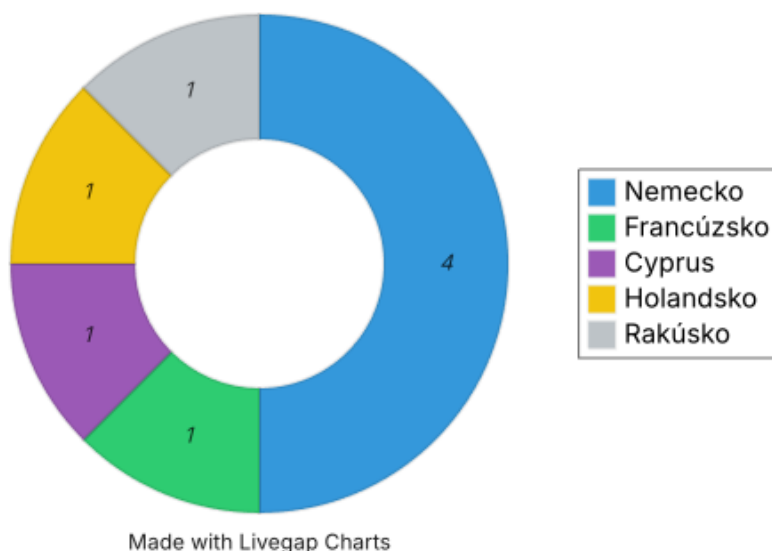
č.3"Počet príkazov na poskytnutie informácií podľa článku 10 DSA"

Obdobne je na tom po obsahovej stránke aj správa z tohto roku, pokrývajúca obdobie od 1. decembra 2024 až do 31. mája 2025. Zo zverejnených dát nám vyplýva, že sa na platformu obrátilo spolu 5 členských štátov - Nemecko, Francúzsko, Holandsko, Cyprus a Rakúsko. Tieto príkazy boli opätovne rozdelené na podvody a podvodné konania – Nemecko (3), Francúzsko (1), Holandsko (1), Cyprus (0), Rakúsko (0) ako aj počet nelegálneho obsahu – Nemecko (1), Cyprus (1), Rakúsko (1), Francúzsko a Holandsko (0). Z časového hľadiska platforma zverejnila medián, ktorý bol v danom rovnako na úrovni 72 hodín, pričom však opätovne nemáme dostupné dáta z ktorých pri jeho výpočte platforma vychádzala. Zo strany platformy nám okrem toho absentujú ďalšie dáta, z ktorých by vyplývala podrobnejšia charakteristika a popis jednotlivých prípadov podvodov a nelegálneho konania, čím sa pre nás sťažuje celkové vyhodnotenie. Celkový počet odoslaných príkazov podľa článku 10 DSA môžeme opätovne dedukovať, pričom bol pravdepodobne nasledovný - Nemecko (4), Francúzsko (1), Holandsko (1), Cyprus (1) a Rakúsko (1).³⁰

³⁰ Stripchat DSA Transparency Report – June 2025.

Počet príkazov na poskytnutie informácií

December 2024 - Máj 2025



Graf č.4 "Počet príkazov na poskytnutie informácií podľa článku 10 DSA"

Záver

Absencia certifikovaných orgánov v praxi devaluje tento kľúčový nástroj ochrany slobody prejavu na deklaratórnu rovinu a prehĺbuje fenomén „prázdnej regulácie“. Hoci DSA formálne priznáva používateľom právo na rýchlu a nezávislú nápravu, v podmienkach Slovenska (a časti EÚ) zostáva toto právo fakticky nevymožiteľné. Výsledkom je asymetria kde platformy preukazujú formálne súlad prostredníctvom správ a databáz, no chýba im protistrana externej kontroly, ktorá by ich rozhodnutia korigovala v individuálnych sporoch. Táto medzera oslabuje aj preventívnu funkciu DSA, nakoľko bez reálne dostupného mimosúdneho preskúmania sa znižuje motivácia platforiem minimalizovať pochybenia už v interných procesoch. To všetko vyvoláva akútnu potrebu regulačných zásahov, ktoré zabezpečia rovnakú dostupnosť, reálnu účinnosť a vymožiteľnosť mechanizmov nápravy naprieč členskými štátmi, a tým aj skutočnú zodpovednosť platforiem za obsah. Analýzou zverejnených správ oboch platforiem dospievame k názoru, že v podobe, v akej sú v súčasnosti zverejňované, nesledujú účel príslušných ustanovení nariadenia DSA vo vzťahu k transparentnosti. Tento záver opierame o skutočnosť, že z oboch správ nevieme bližšie zistiť, čoho konkrétne sa obsah voči ktorému bol príkaz adresovaný týkal. Hoci kategorizácia napovedá, v čom bol daný obsah závadný, absentuje jeho

bližšia charakteristika. V prípade, ak správy oboch skúmaných platforiem porovnáme, tak je na tom vzťahu k zverejneným dátam platforma XVideos lepšie ako platforma Stripchat. Ako sme uviedli aj v článku, zo zverejneného datasetu platformy Stripchat nie je možné zistiť, v čom konkrétne spočívali podvody, podvodné konania ako aj nelegálnosť obsahu, voči ktorému smerovali príkazy príslušných vnútroštátnych orgánov. Kým platforma XVideos v rámci správ o transparentnosti tieto dáta rozdeľuje do kategórií, ku ktorým je niekedy pridaný popis, v prípade platformy Stripchat tento popis respektíve podrobnejšia kategorizácia absentuje.

Zoznam použitej literatúry

1. ONAČILLA, Jozef: Cenzúra nevidaných rozmerov ? Európska únia chce krotiť online priestor nejasnými pravidlami In: Štandard. 30. Decembra 2023. [online]. Dostupné na: <https://standard.sk/530407/cenzura-nevidanych-rozmerov-europska-unia-chce-krotit-online-priestor-nejasnymi-pravidlami> (cit. 25.09.2025)
2. Communications Act of 1934
3. FOLKERT, Wilman - KALÉDA, Saulius Lukas - LOEWENTHAL, Paul-John: The EU Digital Services Act A Commentary – 1. ed. Oxford: Oxford University Press 2024, 625 p. ISBN 9780198892847
4. HARRISON, Ruairí - SHIPP, Jonny - CURTIS, Aebha: Settling DSA-Related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act. (May 15, 2024) [online]. Dostupné na: <https://doi.org/10.2139/ssrn.4787648> (cit. 25.09.2025)
5. HUSOVEC, Martin: Certification of Out-of-Court Dispute Settlement Bodies under the Digital Services Act. In: London School of Economics, Londýn 2023. Dostupné na: <https://doi.org/10.2139/ssrn.4501726> (cit. 25.09.2025)
6. HRNČÁROVÁ, Katarína: Kolko Slovákov je na sociálnych sieťach ? Prekvapujú seniори, poukazujú na nový trend In: Trend. 20. Októbra 2024. [online]. Dostupné na: <https://medialne.trend.sk/internet/kolko-slovakov-je-socialnych-sietach-prekvapuju-seniори-ich-pouzivanie-ukazuje-novy-trend> (cit. 25.09.2025)
7. MARSDEN, Chris - MEYER, Trisha - BROWN Ian: Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation? In: Computer Law & Security Review Volume 36, April 2020. ISSN: 2212-473X [online]. Dostupné na: <https://doi.org/10.1016/j.clsr.2019.105373> (cit. 25.09.2025)
8. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. Októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách), Ú. v. EÚ L 277, 27.10.2022, s. 1 – 102

9. Európska komisia: Návrh Nariadenia Európskeho parlamentu a Rady (EÚ) o jednotnom trhu s digitálnymi službami (akt o digitálnych službách) a o zmene smernice 2000/31/ES. Brusel 15.12.2020. COM/2020/825 final
10. Stripchat DSA Transparency Report – December 2024 [online] Dostupné na: <https://support.stripchat.com/hc/en-us/articles/31227854549137-DSA-TRANSPARENCY-REPORT-DECEMBER-2024> (cit.17.09.2025)
11. Stripchat DSA Transparency Report – June 2025 [online]. Dostupné na: <https://support.stripchat.com/hc/en-us/articles/36391881823249-DSA-TRANSPARENCY-REPORT-JUNE-2025> (cit.17.09.2025)
12. WebGroup Czech Republic, a. s. (xvideos.com) Transparency Report – June / December 2024 [online]. Dostupné na: https://cdn77-pic.xvideos-cdn.com/videos/transparency/XVideos_Transparency_Report_June-December_2024.pdf (cit.17.09.2025)
13. WebGroup Czech Republic, a. s. (xvideos.com) Transparency Report – January / June 2025 [online]. Dostupné na: https://cdn77-pic.xvideos-cdn.com/videos/transparency/XVideos_3rd_Transparency_Report_January_to_June_2025.pdf (cit.17.09.2025)
14. HRDLIČKA, Jan: Zákon ostal na „mŕtvom bode“. In: Echo24. 26. Augusta 2025. [online]. Dostupné na: <https://www.echo24.cz/a/HvNXx/zpravy-domov-snemovna-mrtvy-bod-bitcoiny-afery-obstrukce-poslanci-vysvetluji-nic-nestihnou> (cit. 25.09.2025)

Kontaktné údaje

Mgr. Marián Ruňanin
marian.runanin@flaw.uniba.sk
Katedra teórie práva a filozofie práva
Univerzita Komenského v Bratislave, Právnická fakulta
Slovenská republika

Mgr. Igor Sloboda
igor.sloboda@flaw.uniba.sk
ORCID: 0009-0005-9408-1618
Ústav európskeho práva
Univerzita Komenského v Bratislave, Právnická fakulta
Slovenská republika

OCHRANA ÚSTAVNOSTI VOLIEB V ÉRE KYBERNETICKÝCH HROZIEB

SAFEGUARDING THE CONSTITUTIONALITY OF ELECTIONS IN THE ERA OF CYBERSECURITY THREATS

Peter Matuška¹

Abstrakt: Aj napriek skutočnosti, že snaha o ovplyvňovanie volieb zo zahraničia nie je novým fenoménom tak silnejúca digitalizácia prináša nové aplikačné problémy. Cieľom predmetného príspevku je analyzovať na pozitívny záväzok štátu garantovať slobodné demokratické voľby a to v aj v kontexte kybernetických hrozieb. Tento pozitívny záväzok štátu nevyplýva iba z čl. 31 ústavy, ale aj z čl. 3 Dodatkového protokol č. 1. Európskeho dohovoru o ľudských právach. Obidve predmetné normy sú úzko prepojené s čl. 30 Ústavy, ktorý predstavuje základnú normu pre výkon volebného práva. V prvej časti sa článok zameriava na povinnosť štátu garantovať slobodné voľby ako súčasť právneho štátu. V ďalšej časti sa zameriame na otázku suverenity volieb z pohľadu medzinárodného a ústavného práva a to najmä v kontexte princípu suverenity štátu a princípu nezasahovania. V záverečnej časti článok analyzuje nedávne rozhodnutie Európskeho súdu pre ľudské práva vo veci *Bradshaw and Others v UK*, ktorý predstavuje významný míľnik v kontexte chrániť voľby pred zasahovaním zo zahraničia a to prostredníctvom kybernetických hrozieb. Napriek neúspechu sťažovateľov súd potvrdil narastajúcu hrozbu kybernetických útokov a operácií pre voľby v Európe a definoval povinnosť štátu aktívne predchádzať zasahovaniu do volieb zo zahraničia.

Kľúčové slová: sloboda volieb, zasahovanie a ovplyvňovanie volebného procesu, suverenita volieb, *Bradshaw and Others v UK*, článok 30 a 31 Ústavy

Abstract: Although attempts to influence elections from abroad are not a new phenomenon, increasing digitalization introduces novel challenges. The aim of the article under discussion is to analyse the state's obligation to guarantee free and democratic elections, including in the context of cyber threats. This positive obligation derives not only from Article 31 of the Constitution but also from Article 3 of Additional Protocol No. 1 to the European Convention on Human Rights. The norms under consideration maintain a substantive

¹ Katedra ústavného práva, Právnická fakulta Univerzity Komenského v Bratislave.

connection with Article 30 of the Constitution, which serves as the foundational normative source of the right to vote. The first part of the article examines the state's duty to ensure free elections as an fundamental element of the rule of law. The second part addresses the issue of electoral sovereignty from the perspective of international and constitutional law, with particular emphasis on the principles of state sovereignty and non-interference. The final part analyses the recent judgment of the European Court of Human Rights in *Bradshaw and Others v. the United Kingdom*, which constitutes an important contribution to the protection of electoral rights against foreign interference and cyber threats. Despite the applicants' failure in the case, the Court acknowledged the growing risks posed by cyberattacks and operations targeting elections in Europe and clarified the state's obligation to take active measures to prevent external interference.

Key words: freedom of elections, interference and influencing of electoral process, sovereignty of election, *Bradshaw and Others v UK*, Articles 30 and 31 of the Constitution

Úvod

Demokratická spoločnosť je charakteristická realizovaním volieb v pravidelných cykloch, ktorých cieľom je zistiť vôľu ľudu a premietnuť ju do zvolenia volených zástupcov. Cieľom predmetného článku je poukázať na nové hrozby pre volebný proces, ktorý je personifikovaný v kybernetických hrozbách. Nárast digitalizácie prinieslo nové výzvy pre organizáciu a realizáciu volieb. Otázka slobodných volieb je úzko spätá s výkonom suverenity štátu nakoľko ide o výkon štátnej moci na svojom území. V rámci Ústavy predstavuje čl. 30 pomyselný základný kameň pre výkon volebného práva nakoľko definuje jeho základné atribúty. V tomto kontexte predstavuje čl. 31 konkrétnejšie vyjadrenie, ktoré zakotvuje povinnosť ochraňovať slobodnú súťaž politických síl v demokratickej spoločnosti. V prvej časti príspevok poukazuje na skutočnosť, že existuje nielen pozitívny záväzok štátu organizovať voľby, ale tento termín je nutné vnímať extenzívne – ako pozitívny zväzok organizovať slobodné voľby. Druhá časť sa zameriava na právny režim zasahovania z pohľadu medzinárodného a ústavného práva a rozvíja tézu o potrebe rozšírenia atribútov volieb o prvok suverenity volieb ako takých. V tretej časti článok s prelomové rozhodnutie Európskeho súdu pre ľudské práva („ESLP“) vo veci *Bradshaw and Others* v ktorom sa ESLP prvýkrát zaoberal otázkou pozitívneho záväzku štátu zabrániť vonkajšiemu ovplyvňovaniu volieb.

Ovplyvňovanie volieb a kybernetické hrozby

„Dalo sa prirodzene očakávať, že títo najsmrteľnejší protivníci republikánskej vlády sa k nám priblížia z viacerých strán, ale najmä z túžby zahraničných mocností získať v našich radoch nepatričný vplyv.“²

Problematika ovplyvňovania volieb je prítomná prakticky od začiatku pravidelných volebných cyklov v 18. storočí, avšak s významným rozmachom digitalizácie vstúpila do novej éry.³ S rozširovaním skupiny demokratických krajín vo svete rástol aj počet snáh o ovplyvňovanie volieb.⁴ Cieľom volieb je vyjadrenie vôle ľudu a zabezpečenie legitimacy pre zvolených zástupcov tak aby sa mohli ujať výkonu kompetencií. Primárnym účelom právnej regulácie volebného procesu je zabezpečiť jeho základné atribúty t.j. aby boli voľby priame, rovné, všeobecné a tajné, avšak v súvislosti s narastajúcou digitalizáciou spoločnosti sa do popredia posúva aj otázka samotnej integrity volieb ako takých.⁵ Kybernetické hrozby môžu pôsobiť na voľby dvoma základnými spôsobmi z časového aspektu.

Prvým spôsobom je priame narušenie hlasovacieho procesu, resp. sčítavania hlasov. Táto hrozba je významná nielen pre krajiny v ktorých možné voliť cez internet ako

² HAMILTON, The Federalist Papers: No. 68 The Mode of Electing the President Friday, March 14, 1788.

³ Ako príklad je možné uviesť situáciu z roku 1796 kedy cestoval francúzsky špión Georges-Henri-Victor Collot údolím Mississippi, aby presvedčil západniarov, že je nevyhnutné v prezidentských voľbách v roku 1796 voliť Thomasa Jeffersona. Collota naverboval francúzsky minister vo Philadelphii Pierre-Auguste Adet. REEDER, Tyson: Jefferson's Election as President', *Serpent in Eden: Foreign Meddling and Partisan Politics in James Madison's America*, New York, 2024 ISBN 978-0197628591., s. 114-139.

⁴ K prehľadu niektorých operácií zameraných na ovplyvňovanie volieb pozri aj SCHMITT, Michael N: "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, In: *Chicago Journal of International Law*, Vol. 19: No. 1, (2018), s. 31- 39. K podrobnejšiemu prehľadu v 20 storočí pozri aj REIMANN, Nils: Foreign Electoral Interference: Normative Implications in Light of International Law, Human Rights, and Democratic Theory. *sui generis*, Zurich, Verlag, 2023, s. 15-20. Bubeck a Marinov analyzovali vzorku celkovo 262 volieb v 157 krajinách od konca druhej svetovej vojny. Celkovo definovali nejaký typ volebnej intervencie v 65 percentách volieb v náhodnej vzorke (170 z celkovo 262 volieb). Intervencie do volebného procesu našli v 52 percentách volieb a intervencie zamerané na konkrétnych kandidátov v 33 percentách volieb. BUBECK, Johannes. and MARINOV, Nikolay: *Rules and Allies: Foreign Election Interventions*. Cambridge: Cambridge University Press, 2019, s. 111-112.

⁵ Vo všeobecnosti je možné konštatovať, že najväčšiu pozornosť nielen zo strany štátnych orgánov, ale aj odbornej verejnosti priťahujú celoštátne voľby. Napriek tejto skutočnosti je však nutné podčiarknuť, že ani regionálne voľby, resp. voľby do územnej samosprávy nie sú imúnne voči kybernetickým hrozbám. Foreign interference in electoral processes at local and regional levels, Committee on the Monitoring of the implementation of the European Charter of Local Self-Government and on the respect of Human Rights and the Rule of Law at local and regional levels, CG (2025)48-10, 26 March 2025. s.3.

napr. Estónsko,⁶ ale aj prípade Slovenska nakoľko údaje s okrskových komisii sa posielajú elektronicky do centrálneho štatistického úradu.⁷ Predmetný článok sa na tento aspekt nebude bližšie zameriavať.

Druhý spôsob je podstatne komplikovanejší a zameriava sa situáciu pred uskutočnením samotného hlasovania, nakoľko jeho cieľom je ovplyvniť výsledok volieb a to najmä prostredníctvom vplyvu na voličov. Ako už bolo vyššie uvedené rozmach digitalizácie umožnil priamejší a adresnejší prístup k voličom čo v konečnom dôsledku umožňuje vytvorenie a riadenie informačných operácií, ktorých cieľom je zmeniť alebo posilniť postoje občanov.⁸

Vyššie uvedené delenie má význam aj z pohľadu dokazovania nakoľko v prípade prvého scenáru je možné definovať dopad na voľby, resp. hlasovanie. Benátska komisia zaraďuje medzi príklady nezrovnalostí, pri ktorých možno objektívne určiť pravdepodobný vplyv na výsledok volieb, patrí dvojité hlasovanie alebo sčítanie hlasov, stratené hlasovacie lístky alebo hlasy, nedostatok hlasovacích lístkov pre konkrétnu stranu alebo kandidáta, neplatné hlasovacie lístky a nesprávne zrušenie hlasov.^{9,10} Pri druhom spôsobe Benátska Komisia konštatuje, že môže byť objektívne stanoviť vplyv iných typov nezrovnalostí, ktoré zvyčajne súvisia s kampaňou nakoľko hrubé porušovanie týchto pravidiel môže ovplyvniť pravidlá hry v prospech konkrétnych kandidátov a/alebo mať významný vplyv na názory voličov.¹¹

Z pohľadu formy kybernetických hrozieb¹² smerom k volebnému procesu je možné identifikovať viaceré spôsoby ako napr. narušiť volebnú infraštruktúru pomocou distribuovaných útokov typu (DDoS) hacknutie webových verejných stránok politických strán, narušenie volebnej infraštruktúry, ukradnutie citlivých informácií,

⁶ Po prvýkrát v histórii bola väčšina hlasov v národných parlamentných voľbách odovzdaná online namiesto papierových hlasov keď Estónsko volilo svoj parlament v marci 2024. Viac ako 51 % hlasujúcich odovzdalo svoj hlas online.

⁷ Parlamentné voľby 2023 boli prvé kedy volebné komisie zápisnice s výsledkami vytvorili aj odoslali na sumarizáciu povinne elektronicky. Pozri §30 a nasledujúce zákona č. 180/2014. V tejto súvislosti treba uviesť, že sa zápisnice stále vedú aj v písomnej podobe, nakoľko sa musia vytlačiť.

⁸ Pozri napr. BENTHEM, V. Tsveletina., HOLLIS, Duncan. B., and DIAS, Talita: Information Operations under International Law, In: *Vanderbilt Journal of Transnational Law*, 55, (2022), s. 1217-21.

⁹ European Commission for Democracy through Law, Venice Commission, Issued on 27 January 2025, CDL-PI(2025)001-e, Urgent Report on the cancellation of election results by Constitutional Courts, s. 14.

¹⁰ V Rakúsku Ústavný súd (Verfassungsgerichtshof) zrušil druhé kolo prezidentských volieb v roku 2016 z dôvodu procesných nezrovnalostí (konkrétne nesprávneho spracovania hlasov zaslaných poštou). Hoci neexistovali žiadne dôkazy o podvode, ktoré by mohli ovplyvniť výsledok, súd rozhodol, že aj možnosť vplyvu postačuje na odôvodnenie zrušenia. Judgement of the Austrian Constitution Court, VfGH, AUT-2016-1-002, rozhodnutie zo dňa 2.7.2016.

¹¹ *Ibid.*

¹² Hrozba vonkajšieho zasahovania do volebného procesu je šíria ako iba kybernetické hrozby, nakoľko je tam možné zaradiť aj napr. skryté financovanie kandidátov.

útoky založené na ransomvéri na narušenie prístupu k volebným údajom a systémom, čo vedie k prerušeniu volebných služieb alebo adresovanie výhražných správ voličom, resp. šírenie cielených dezinformácií.¹³¹⁴ V princípe je možné uviesť, že vyššie uvedené scenáre sa nemusia vyhýbať ani slovenskej infraštruktúre čoho dôkazom je aj skúsenosť s hacknutím katastra nehnuteľností zo začiatku roka 2025.¹⁵ Významným prípadom, ktorý poukázal, že predmetná debata nie je iba akademického charakteru, ale má konkrétne konzekvencie v praxi sú prezidentské voľby v Rumunsku, ktoré sa odohrali v novembri, resp. decembri 2024. Pre účely tohto článku¹⁶ je kľúčové, že rozhodnutie zo strany rumunského ústavného súdu sa opieralo, okrem iného o cielenú dezinformačnú kampaň na sociálnej sieti tik tok.¹⁷

Suverenita volieb z pohľadu ústavného a medzinárodného práva

V tejto časti príspevku sa zameriame na analýzu právneho rámca pozitívneho záväzku zabezpečiť suverenitu volieb. Pod termínom suverenita volieb rozumieme situáciu kedy sú organizované a vykonané bez vonkajšieho vplyvu zo strany zahraničných aktérov.

¹³ Pozri napr. Kanadské centrum pre kybernetickú bezpečnosť. Dostupné na <<https://www.cyber.gc.ca/en/guidance/cyber-threats-elections>>.

¹⁴ Problematika riešenia dezinformácií prostredníctvom medzinárodného práva bola na stole už v medzivojnovom období. Vlády sa čoraz viac obávali potenciálnych dopadov zahraničného vysielania na vlastných občanov. V decembri 1933 československá vláda zakázala verejné počúvanie zahraničných staníc. V roku 1936 bol podpísaná International Convention Concerning the Use of Broadcasting in the Cause of Peace, ktorej cieľom bolo zakázať vysielanie cielených dezinformácií a ktoré by podnecovali obyvateľstvo k činom nezlučiteľným s vnútorným poriadkom alebo bezpečnosťou územia. Bližšie pozri POTTER, Simon. J: Broadcasting in the Cause of Peace: Regulating International Radio Propaganda in Europe, 1921–1939. In: *The International History Review*, 45(6) (2023), s. 855–859.

¹⁵ Začiatkom januára ochromil Slovensko masívny hackerský útok na Úrad geodézie a kartografie. Po troch mesiacoch sa kataster nehnuteľností postupne vrátil do prevádzky. Jedna z hlavných – systém pre geodetov na automatizované kontroly ich plánov – je už vyše sedem mesiacov ochromený. 22.7.2025 <<https://hnonline.sk/slovensko/96224732-po-kybernetickom-utoku-na-kataster-z-januara-2025-su-dalej-nefunkcne-casti-klucovych-sluzieb>>.

¹⁶ Pre podrobnejšiu analýzu pozri MATUŠKA, Peter: Rumunský precedens: ústavnoprávne aspekty anulovania výsledku volieb v Slovenskej republike a suverenita volieb, In: *Právnik*, roč. 164, č. 11. (2025), s. 1034–1054.

¹⁷ V tejto súvislosti treba uviesť, že internetová platforma, resp. aplikácia Tik Tok nevyhovela požiadavkám Rumunska na odstránenie jeho obsahu. CARROZZINI, Alina: Shooting Democracy in the Foot?: The Romanian Constitutional Court's Annulment of Presidential Elections, VerfBlog, 2024/12/13, Dostupné na <<https://verfassungsblog.de/shooting-democracy-in-the-foot/>>.

Medzinárodné právo

Z pohľadu medzinárodného práva sa povinnosť neovplyvňovať voľby v iných štátoch spája s princípom non-intervention,^{18,19} avšak niektorí autori sa opierajú aj o iné aspekty ako právo na participáciu na politickom procese alebo právo na demokratické sebaurčenie.²⁰ Medzi kľúčové dokumenty pre pravidlá kybernetickej suverenity je nutné uviesť Tallinn 2.0.,²¹ ktorý presadzuje zákaz všetkých foriem hackerského útoku na voľby „Štát nesmie vykonávať kybernetické operácie, ktoré porušujú suverenitu iného štátu.“²² Tallinský manuál má za cieľ reflektovať „customary international law“ t.j. medzinárodné obyčajové právo pre kybernetickú oblasť. Napriek tejto definícii je nutné uviesť, že záverečná správa Skupiny vládnych expertov OSN (UN Group of Governmental Experts) dospela k záveru, že pravidlo nezasahovania a ľudské práva sa vzťahujú na správanie štátov v kyberpriestore, ale nepotvrdila existenciu kybernetického pravidla suverenity.²³ Na druhej strane samotný tallinský manuál zdôrazňuje špecifické postavenie princípy suverenity nakoľko práve od tohto princípu sa vyvíjali ďalšie princípy a zásady medzinárodného práva.²⁴

¹⁸ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14, bod. 205.

¹⁹ Pre podrobný výpočet krajín a ich opinio juris v súvislosti s interpretáciou pravidla nezasahovania a jeho základných aspektov ako sú voľby pozri MILANOVIC Marko: 'Revisiting Coercion as an Element of Prohibited Intervention in International Law', In: *American Journal of International Law*, 117(4), (2023) s. 604-605. Ako príklad je možné uviesť pozíciu Fínska - International Law and Cyberspace: Finland's National Positions, (2020), s. 3-5. Dostupné na https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

²⁰ TSAGOURIAS, Nicholas: Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace, in BROEDERS, Dennis. and BERG, Van Den Berg: (eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy* (2020), s. 45. Navštívené cez WHEATLEY, Steven: Election hacking, the rule of sovereignty, and deductive reasoning in customary international law, In: *Leiden Journal of International Law*, 36(3), (2023) s. 676. Je možné taktiež argumentovať, že právo zúčastňovať sa na verejných záležitostiach, voliť vo voľbách a kandidovať vo voľbách sa považuje už za súčasť *customary international law*, keďže je zakotvené v mnohých dokumentoch vrátane Medzinárodný pakt o občianskych a politických právach, článok 19, 16. decembra 1966, 999 U.N.T.S. 171 alebo Všeobecná deklarácia ľudských práv Uznesenie V.A. 217 (III) A, článok 19, Všeobecná deklarácia ľudských práv (12. decembra 1948).

²¹ V súčasnosti sa pripravuje už Tallinn Manual 3.0, ktorý by mal reflektovať rozmach AI t.j. umelej inteligencie.

²² Rule 4. Pozri bližšie SCHMITT Michael. N: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press, 2017. s. 17-27.

²³ Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (2021).

²⁴ Rule 1, Explanatory bod. 3.

V tomto kontexte je však nevyhnutné zamerať sa konkrétne na otázku organizácie volieb. V prípade otázky či kybernetická aktivita cudzieho štátu, ktorá priamo znižuje schopnosť vlády viesť voľby, predstavuje priame porušenie zvrchovanosti tohto štátu je nutné poukázať na všeobecné princípy medzinárodného práva.²⁵ Schmitt medzi príklady takéhoto porušenia zaraďuje napríklad dočasné narušenie riadneho fungovania volebného hardvéru a softvéru, blokovanie prístupu k online vládnym informáciám o voľbách a zmena týchto informácií.²⁶ V tejto súvislosti je možné uviesť, že Wheatley z pohľadu narušenia suverenity rozlišuje medzi dvoma základnými situáciami. V prvom scenári prichádza k vykonaniu kybernetickej operácii, avšak bez spôsobenia škody a v druhom prípade je aj spôsobená škoda.²⁷ Konsenzus v tejto oblasti nie je ešte ustálený nakoľko každý z prístupov má svojich protagonistov.²⁸ Autor článku sa prikláňa k extenzívnejšiemu výkladu t.j. narušenie suverenity má byť posudzované z pohľadu procesu a konania a nie skúmané *ex post* z pohľadu následkov. Napriek extenzívnemu výkladu je však nevyhnutné sledovať kauzálny nexus t.j. v prípade hackerského útoku musí existovať vzťah medzi predmetným hackerským útokom a organizáciou volieb ako takých.²⁹ Vo všeobecnosti je však možné konštatovať, že skutočnosť, že cudzí subjekt ovplyvňuje voľby je porušením suverenity nakoľko obmedzuje suverenitu štátu.³⁰

²⁵ The Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means, <<https://elac.web.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through>>

²⁶ SCHMITT, Michael N.: Foreign Cyber Interference in Elections, Foreign Cyber Interference in Elections, In: *International Law Studies.*, Vol. 97, (2021), s. 753.

²⁷ WHEATLEY, Steven: *supra note* 20, s. 693-694.

²⁸ V prípade prvého scenáru t.j. akékoľvek narušenie je tma možné zaradiť Čínu alebo Francúzsko. Ako druhú skupiny pozri napr. BUCHAN, Russel: Cyber Espionage and International Law (2018) s. 51. *Ibid.* 694.

²⁹ Kybernetické aktivity, ktoré zasahujú do „inherentne vládnej funkcie“ cieľového štátu alebo si ju uzurpujú, môžu porušovať jeho zvrchovanosť. SCHMITT Michael. N.: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press; 2017, k Rule 4, s. 20-23.

³⁰ V tomto kontexte je nutné uviesť, že napr. Wheatley nesúhlasí so stanoviskom, že ide o porušenie princípu suverenity, ale poukazuje na princíp non-intervention. Podľa jeho názoru problém hackovania volieb spočíva v správnom pochopení uznávaného a akceptovaného pravidla non-intervention, nie v spornom a napadnuteľnom pravidle suverenity. WHEATLEY, Steven: *supra note* 20, s. 698. Obdobný názor vyjadrili Corn a Taylor. kedy uviedli, že zásada suverenity vrátane územnej suverenity by sa mala zohľadňovať pri vykonávaní každej kybernetickej operácie, avšak nestanovuje absolútnu prekážku individuálnym alebo kolektívnym štátnym kybernetickým operáciám, ktoré ovplyvňujú kybernetickú infraštruktúru v inom štáte, za predpokladu, že účinky nedosiahnu úroveň nezákonného použitia sily alebo nezákonného zásahu. CORN, Gary. P. and TAYLOR, Robert: Sovereignty in the Age of Cyber, In: *American Journal of International Law Unbound*, 111, (2017) s. 208-209.

V prípade volieb ide o obmedzenie fundamentálneho aspektu a to konkrétne vykonanie slobodných volieb.³¹

Princíp suverenity štátu v súvislosti s otázkou organizácie volieb je nutné vnímať nielen ako negatívne vymedzenie t.j. iné štáty majú povinnosť nezasahovať do volebného procesu, ale aj ako pozitívny záväzok štátu zabezpečiť organizáciu a priebeh volieb aby neprišlo k zásahom zo strany iných subjektov. Ako uviedol aj Medzinárodný súdny dvor v rozhodnutí *Island of Palmas* tak suverenita je vykonávanie funkcií štátu s vylúčením akékoľvek iného štátu.³²

Ústavné právo

Obdobne ako v prípade medzinárodného práva aj v prípade ústavného práva je kľúčový aspekt koncept suverenity štátu. Štát vykonáva suverénnu moc sa na svojom území a jeho imanentnou zložkou je aj organizácia moci a to prostredníctvom volebného procesu. V prípade Slovenskej republiky je táto kompetencia, resp. povinnosť zakotvená v čl. 1, ktorý definuje Slovenskú republiku ako zvrchovaný a právny štát. Ústavodarca zakotvil v prípade volieb aj špecifický pozitívny záväzok štátu v čl. 31 kde uviedol: *„Zákonná úprava všetkých politických práv a slobôd a jej výklad a používanie musia umožňovať a ochraňovať slobodnú súťaž politických síl v demokratickej spoločnosti.“* Slobodná súťaž politických strán, resp. ich predstaviteľov je garantovaná ústavou. Ide taktiež o pozitívny záväzok štátu zabezpečiť aby bola politická súťaž v ústavných medziach. Ústavný súd skonštatoval, že: *„Pre zákon, ktorý bližšie upravuje výkon politických práv, je základným interpretačným pravidlom čl. 31 ústavy. Podľa tohto ustanovenia zákonná úprava všetkých politických práv a slobôd a jej výklad a používanie musia umožňovať a ochraňovať slobodnú súťaž politických síl v demokratickej spoločnosti. Toto ustanovenie má priamu spojitosť so všetkými politickými právami vyjadrenými v ústave a svojou povahou ovplyvňuje formovanie politických síl v demokratickej spoločnosti. Slobodná súťaž politických síl nachádzajúca výraz predovšetkým vo voľbách je základným predpokladom fungovania demokratického štátu (PL. ÚS 19/98).“*³³

³¹ Medzi základné aspekty štátu ohrozených kybernetickými operáciami okrem volieb zaraďuje Pijpers aj vyberanie daní, obrana štátu, vedenie diplomacie, presadzovanie práva, riešenie kríz alebo vytvorenie systému sociálnej starostlivosti, úradnícka a verejná komunikácia. PIJPER, Peter B.M.J.: Careful What You Wish For

Tackling Legal Uncertainty in Cyberspace, In: *Nordic Journal of International Law*, 92 (2023), s. 409.

³² *Island of Palmas (Netherlands v. USA)*, Award of 4 April 1928, 2 RIAA 829 (1928), s. 838.

³³ PL. ÚS 82/07 rozhodnutie zo dňa 31. októbra 2007.

Ako príklad ústavnoprávnej úpravy, ktoré reflektuje narastajúce riziko kybernetických hrozieb pre uskutočnenie slobodných a suverénnych volieb³⁴ je možné uviesť nedávnu ústavnú zmenu v Nórsku z roku 2022. Po ústavnej zmene môže dvojtretinová väčšina v nórskom parlamente nariadiť nové voľby, ak mimoriadna udalosť, ktorá zahŕňa kybernetické útoky a dezinformačné kampane, zabránila významnej časti voličov voliť.³⁵ V súčasnosti slovenská legislatíva neprijala obdobné ustanovenie na úrovni ústavného predpisu.

Otázka pozitívneho záväzku štátu usporiadať voľby v zmysle ústavných princípov je nevyhnutné vnímať extenzívne a nie reštriktívne. Inými slovami, štát môže prijať aj opatrenia, ktoré môžu ísť na úkor iných slobôd v záujme. Ako uviedol už v predchádzajúcej judikatúre ESLP - aby sa zaručila stabilita a účinnosť demokratického systému, môže byť štát povinný prijať konkrétne opatrenia na svoju ochranu.³⁶ V nasledujúcej časti sa zameriame na analýzu nedávneho rozsudku vo veci *Bradshaw and Others v. United Kingdom* (ďalej ako „Bradshaw and Others“) v ktorom sa ESLP musel vysporiadať s otázkou pozitívneho záväzku štátu zabrániť zasahovaniu do volieb.

Prípád Bradshaw and Others v. United Kingdom

ESLP sa vo svojej judikatúre už viackrát zameriaval na možné porušenie čl. 3 Dodatkového Protokolu č. 1, označenom ako právo na slobodné voľby, ktorý zaväzuje zmluvné strany vykonať v primeraných intervaloch slobodné voľby s tajným hlasovaním za podmienok, ktoré zabezpečia slobodné vyjadrenie názorov ľudu pri voľbe zákonodarného zboru.³⁷

³⁴ Termín suverénne voľby používame pre označenie volieb, ktoré sú bez vonkajšieho zasahovania. Bližšie pozri MATUŠKA, Peter: Rumunský precedens: ústavnoprávne aspekty anulovania výsledku volieb v Slovenskej republike a suverenita volieb, *Právnik*, roč. 164, č. 11, (2025), s. 1034-1054.

³⁵ Článok 54 odsek 5 Ústavy Nórska: „Ak sa stane niečo mimoriadne, čo znemožní významnej časti voličov voliť, zasadajúci Storting môže s hlasmi dvoch tretín poslancov rozhodnúť o konaní nových volieb do Stortingu. Rozhodnutie o konaní nových volieb možno prijať len v rozsahu potrebnom na zabezpečenie toho, aby voliči mali možnosť voliť. Zvolení poslanci Stortingu zostanú vo funkcii až do konečného schválenia nových volieb.“

³⁶ *Vogt proti Nemecku* (26. september 1995, body 51 a 59, séria A č. 323)

³⁷ ESLP opakovane judikoval, že práva zaručené článkom 3 Protokolu č. 1 sa vzťahujú nielen na proces organizácie a riadenia volebného procesu, ale aj na spôsob preskúmania výsledku volieb a spory týkajúce sa sčítania hlasov a potvrdzovania výsledkov volieb (Kovach proti Ukrajine, 2008, bod 55, Namat Aliyev proti Azerbajdžanu, 2010, bod 81 alebo Mugemangango proti Belgicku [GC], 2020). Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights Right to free elections, Updated on 28 February 2025. s. 29.

Sťažovatelia v tomto prípade boli traja poslanci parlamentu zvolení v roku 2019.³⁸ Základom žaloby boli dve správy jednu zverejnenú House of Commons Digital, Culture, Media and Sport Committee (DCMS) a druhá výborom Intelligence and Security Committee of Parliament (ISC). Podľa názoru sťažovateľov poskytli predmetné správy dôveryhodné dôkazy o zasahovaní Ruska do referenda o nezávislosti Škótska v roku 2014, referenda o členstve v Európskej únii v roku 2016 a volieb v roku 2019. V tomto kontexte je zaujímavé, že konania na národných súdoch spojeného kráľovstva Veľkej Británie a Severného Írska (ďalej aj ako „Spojené kráľovstvo“) boli vedené voči premiérovi za neadekvátne implementovanie opatrení na ochranu demokratických slobôd Spojeného kráľovstva. Sťažovatelia taktiež tvrdili, že predseda vlády nekonal v súlade so svojimi povinnosťami tým, že nezačal verejné vyšetrovanie predmetných zásahov. Sťažovatelia uvádzali, že vzhľadom na správu ISC bolo toto zlyhanie porušením vyšetrovacej povinnosti vyplývajúcej z článku 3 Protokolu č. 1 k Dohovoru. Ďalej spochybnili to, čo opísali ako „*neexistenciu účinného právneho rámca na zabezpečenie „podmienok, ktoré zabezpečia slobodné vyjadrenie názoru ľudu*“, ako to vyžaduje článok 3 Protokolu č. 1“.

ESLP vo svojom rozhodnutí sumarizoval viaceré expertné správy zo Spojeného kráľovstva ktoré poukazovali na zasahovanie do volebného procesu zo strany Ruska. Ako príklad je možné uviesť National Cyber Security Centre, ktoré vo výročnej správe z a rok 2023 uviedlo: *„Vláda Spojeného kráľovstva odhaduje, že je takmer isté, že ruskí aktéri sa snažili zasahovať do všeobecných volieb v roku 2019. V nasledujúcich mesiacoch, s blížiacimi sa voľbami v Spojenom kráľovstve a USA, môžeme očakávať, že integrita našich systémov bude opäť preverená. Ochrana našich demokratických a volebných procesov pred zahraničným zasahovaním, či už z Ruska alebo akéhokoľvek iného štátu, je a vždy bude absolútnou prioritou pre NCSC a my budeme naďalej podporovať kritickú prácu vlády v tejto oblasti.“*

Správa taktiež poukazuje na skutočnosť, že samotné hlasovanie prebieha tradičnou formou a preto významne znižuje pravdepodobnosť, že integrita výsledkov môže byť ovplyvnená prostredníctvom kybernetickej operácie.³⁹ V rozsudku taktiež súd citoval uznesenie Rady Európy prostredníctvom ktorého Rada Európy vyjadrila obavy okrem iného nad šírením dezinformačných kampaní zameraných na formovanie verejnej mienky a trendmi zahraničného zasahovania a manipulácie do volieb.⁴⁰ Podľa názoru Parlamentného zhromaždenia Rady Európy predstavujú tieto kampane výzvu pre demokraciu, a najmä pre volebné procesy v členských štátoch Rady Európy, a

³⁸ Ben Bradshaw, Caroline Lucas and Alyn Smit. Dvaja sťažovatelia nekandidovali v nasledujúcich voľbách a ďalší neobhájil svoje mandát.

³⁹ Bod 56.

⁴⁰ PACE Resolution 2326 (2020): Democracy hacked? How to respond? Text adopted by the Assembly on 31 January 2020 (9th Sitting).

ovplyvňujú právo na slobodu prejavu vrátane práva na prijímanie informácií a práva na slobodné voľby.⁴¹

ESLP skonštatoval, že demokracia predstavuje jediný systém, ktorý je kompatibilný so samotným Dohovorom a voľby sú imanentnou súčasťou demokratického zriadenia.⁴² Rozhodnutie vo veci *Bradshaw and Others* je prelomové nakoľko posunulo interpretáciu čl. 3 Protokolu 1 do novej pozície nakoľko dovtedajšia judikatúra sa zameriava na situácie kedy boli poškodené práva jednotlivca aktívnymi krokmi zo strany štátu.⁴³ Štát je preto povinný prijať pozitívne opatrenia na organizovanie volieb „za podmienok, ktoré zabezpečia slobodné vyjadrenie názoru ľudu pri voľbe zákonodarného zboru“.⁴⁴ Samotný ESLP nedefinuje ako konkrétne majú voľby prebiehať, resp. ktorý volebný systém je vhodnejší nakoľko krajiny majú právo organizovať si voľby podľa svojich pravidiel, avšak miera voľnej úvahy štátu je v tomto ohľade obmedzená povinnosťou rešpektovať základnú zásadu článku 3 Protokolu č. 1, a to „slobodné vyjadrenie názoru ľudu pri voľbe zákonodarného zboru“.⁴⁵

ESLP prvýkrát explicitne potvrdil, že pozitívny záväzok štátu zakotvený v čl. 3 Protokolu 1 je nutné interpretovať extenzívne nakoľko rozsah tejto povinnosti presahuje integritu výsledku volieb v užšom zmysle a zahŕňa šírenie politických názorov a informácií v období pred voľbami.⁴⁶ ESLP v tomto kontexte skonštatoval, že je nesporná skutočnosť, že niektoré štáty, resp. neštátne subjekty využili dezinformácie ako zbraň na zasahovanie do demokratických volieb a zdôraznil, že šírenie dezinformácií môže predstavovať významnú hrozbu pre demokraciu.⁴⁷

Pozitívny záväzok štátu usporiadať voľby môže byť nesplnený ak v dôsledku zasahovania nepriateľského štátu by boli práva voličov v členskom štáte obmedzené do takej miery, že by to narušilo ich samotnú podstatu t.j. slobodné vyjadrenie názoru ľudu pri voľbe -tak je možné od tohto štátu vyžadovať, aby prijal pozitívne opatrenia na ochranu integrity svojich volebných procesov a aby tieto opatrenia neustále prehodnocoval.⁴⁸ Táto povinnosť zachovania integrity volieb je taktiež prepojená s povinnosťou vyšetrovať samotné zasahovanie do volebného procesu. ESLP v tomto prípade zdôraznil špecifickosť práv a povinností zakotvených v čl. 3 protokol 1

⁴¹ Body 68-70. Súd taktiež poukázal na správu Benátskej komisie z roku 2018, ktorá sa zaoberala dezinformáciami.

⁴² Body 112 -113.

⁴³ ESLP sa zaoberal sťažnosťami zameraných na situáciu kedy štáty podľa tvrdenia sťažovateľa bránili slobodnému vyjadreniu názoru ľudu pri voľbe legislatívneho zboru. Pozri napr. *Selahattin Demirtaş v. Turkey* (no. 2) [GC], no. 14305/17, 22 December 2020, bod 386.

⁴⁴ *Communist Party of Russia and Others v. Russia*, no. 29400/05, 19 June 2012), bod 107.

⁴⁵ *Mugemangango v. Belgium* [GC], no. 310/15, 10 July 2020), bod 73. Pozri aj body 125-126 *Bradshaw and Others*. v UK.

⁴⁶ Bod 131.

⁴⁷ Body 134-135.

⁴⁸ Bod 136.

a odlíši ich od iných článkov nakoľko uviedol, že neexistuje samostatná povinnosť vyšetrovať, avšak napriek tejto absencii samostatnej povinnosti vyšetrovať sporné tvrdenia o porušení práv jednotlivca podľa článku 3 Protokolu č. 1, „*zjavné zlyhanie štátu pri vyšetrovaní dôveryhodných tvrdení o zasahovaní do svojich volieb by mohlo vyvolať problém podľa tohto článku, ak by bránilo jeho schopnosti prijať pozitívne opatrenia na ochranu voličov pred narušením samotnej podstaty ich práva využívať voľby „za podmienok, ktoré zabezpečujú slobodné vyjadrenie názoru ľudu“*“.⁴⁹

Inými slovami, štát nemá povinnosť vyšetrovať akékoľvek tvrdenie sťažovateľa o tom, že bol porušený čl. 3 Protokolu 1, avšak bez adekvátneho vyšetrovania nedokáže prijať primerané opatrenia pre ochranu integrity volieb čo môže viesť k porušeniu pozitívneho záväzku štátu a teda porušeniu predmetného čl. 3. Dôležitou otázkou bol status sťažovateľov a otázka či mali status obete v zmysle EDLP nakoľko EDLP nepredpokladá podanie žaloby *actio popularis* a úlohou súdu zvyčajne nie je preskúmať príslušné právo a prax *in abstracto*, ale určiť, či boli porušené práva sťažovateľa.⁵⁰

Porušenie čl. 3 dodatkového protokolu č. 1 EDLP je v zmysle judikatúry nutné spojiť s konkrétnym porušením. ESĽP nie je naklonený riešiť porušenia *in abstracto* a preto akékoľvek porušenie musí byť adekvátne zdokumentované podložené dôkazmi a najmä by malo smerovať k porušeniu konkrétnych práv sťažovateľa. Tento prístup ESĽP nedávno potvrdil aj v rozhodnutí *Kovačević v. Bosnia and Herzegovina*⁵¹ kde uviedol, že procesná požiadavka „statusu obete“ stanovuje, že žiadateľ musel byť „priamo dotknutý“ napadnutými zákonnými alebo ústavnými ustanoveniami, aby sa predišlo „abstraktnej“ sťažnosti.⁵²

V prípade *Bradshaw and Others* definoval ESĽP, že na preukázanie „statusu obete“ by musel žiadateľ predložiť primerané a presvedčivé dôkazy o pravdepodobnosti, že právo na prospech z volieb konaných „*za podmienok, ktoré zabezpečujú slobodné vyjadrenie názoru ľudu*“ by bolo obmedzené do takej miery, že by to narušilo jeho samotnú podstatu; samotné podozrenie alebo domnienka nebudú postačovať.⁵³

V tejto súvislosti súd konštatoval či je zasahovanie v praxi spôsobilé narušiť samotnú podstatu práva zakotveného v čl. 3 Dodatok 1 nezávisí len od intenzity zasahovania,

⁴⁹ Body 137-138.

⁵⁰ Bod 143.

⁵¹ *Kovačević v. Bosnia and Herzegovina* sťažnosť č. 43651/22 Rozhodnutie zo dňa 25 júna 2025.

⁵² MARKO, Joseph: A Fallen Curtain and Open Questions: The Grand Chamber Decision of the European Court of Human Rights in *Kovačević v. Bosnia and Herzegovina*, VerfBlog, 2025/8/11, <https://verfassungsblog.de/ecthr-voting-bosniaherzegovina/>

⁵³ V tomto bode súd odkazoval aj na svoju predchádzajúcu judikatúru *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], sťažnosť č. 47848/08, ECHR 2014, bod 101 alebo *Verein KlimaSeniorinnen Schweiz and Others v. Switzerland* [GC], sťažnosť č. 53600/20, 9 April 2024, bod. 470. Bod 145.

ale aj od opatrení zavedených na vnútroštátnej úrovni na minimalizáciu rizika, že toto zasahovanie ovplyvní výsledok volieb.⁵⁴

ESLP zdôraznil, že štáty by nemali zostať pasívne, keď čelia dôkazom, že ich demokratické procesy sú ohrozené, a majú široký „margin of appreciation“ pri výbere prostriedkov, ktoré majú prijať na boj proti takýmto hrozbám.⁵⁵ V prípade *Bradshaw and Others*, napokon ESLP odmietol sťažnosť a skonštatoval, že zo strany Spojeného kráľovstva neprišlo k porušeniu čl. 3 Protokolu 1. Ako kľúčové aspekty definoval skutočnosť, že v rokoch 2022 až 2023, po zverejnení správ, Spojené kráľovstvo schválilo viaceré legislatívne zmeny vrátane zákona o voľbách („The Elections Act“) z roku 2022, zákona o národnej bezpečnosti z roku 2023 („the National Security Act 2023“) a zákona o online bezpečnosti z roku 2023. („Online Safety Act 2023.“). Tieto legislatívne opatrenia mali za cieľ zabezpečiť ochranu pred zahraničným zasahovaním a dezinformáciami počas volieb. Podľa súdu tieto kroky Spojeného kráľovstva preukazujú pokus o vyšetrovanie a bránenie zahraničnému zasahovaniu, ktoré by mohlo ohroziť demokraciu.

Záver

Otázka ovplyvňovania volieb je prítomná v spoločnosti dlhodobo, avšak kybernetické hrozby predstavujú novú hrozbu pre uskutočnenie volieb, a ako ukazujú viaceré príklady tak táto hrozba má dopad aj na podobu legislatívy. Kybernetická hrozba pre voľby má dva základné aspekty a to okolnosti, ktoré sa týkajú konania vo volebný deň, resp. tesne po voľbách ako je spočítanie hlasov, pokus o modifikáciu výsledkov prostredníctvom hackerského útoku alebo znefunkčnenie elektronického hlasovania. Podstatne ťažšie je však možné definovať vplyv a dopad na voľby v druhom prípade kedy je cieľom organizácia volieb a samotná volebná kampaň. V tomto prípade ESLP potvrdzuje stanovisko Benátskej komisie, že dokazovanie je značne komplikovanejšie ako v prvom prípade.⁵⁶

Suverenita volieb je otázkou, ktorá zasahuje nielen ústavné, ale aj medzinárodné právo. Princíp nezasahovania do volieb v inom štáte je imanentne prepojený s princípom non-intervention, resp. právom na participáciu na politickom procese alebo právom na demokratické sebaurčenie. Z pohľadu ústavného práva je zrejmé, že usporiadanie volieb bez vonkajšieho zasahovania predstavuje fundamentálny znak existencie štátu a výkonu štátnej moci. Kybernetické hrozby otvárajú novú kapitolu možností ovplyvňovania volebného procesu a príklad ústavnej zmeny

⁵⁴ Bod 14.8.

⁵⁵ Bod 162.

⁵⁶ Pre diskusiu k regulovaniu volebných kampaní pozri aj ŘíHA, Michal: Právo křičet: K oprávnění státu zasahovat do volební soutěže v judikatuře soudů, In: *Právník*, roč. 155, č. 10, (2016), s. 885-894.

v Nórsku potvrdzuje, že konanie voči kybernetickým hrozbám v súvislosti s volebným procesom sa premieta aj do ústavného textu.

Rozhodnutie vo veci *Bradshaw and Others* otvorilo novú kapitolu interpretovania pozitívneho záväzku zakotveného v čl. 3 Dodatkového Protokolu č. 1. ESLP síce potvrdil reštriktívnejší prístup v otázke aktívnej legitimácie a taktiež v otázke kauzálneho nexusu medzi zasahovaním a výsledkom, avšak na druhej strane potvrdil existenciu pozitívneho záväzku organizovať voľby bez vonkajších zásahov bez ohľadu či ide o štátne alebo neštátne subjekty.

Súd vo svojom odôvodnení definoval základné atribúty pozitívneho záväzku a to povinnosť vykonávať aktívne kroky aby neprišlo k vonkajšiemu ovplyvňovaniu a následne adekvátne vyšetrovať možné zásahy a ich dopad na priebeh volebnej kampane ako aj dopad na volebný výsledok.⁵⁷ Prípád *Bradshaw and Others* predstavuje míľnik v chápaní pozitívneho záväzku štátu nakoľko sa jeho systematická analýza zamerala na druhú časť čl. 3 Protokolu č. 1. t.j. „za podmienok, ktoré zabezpečia slobodné vyjadrenie názoru ľudu pri voľbe zákonodarného zboru“. Inými slovami, štát ma nielen povinnosť organizovať voľby v pravidelných intervaloch, umožniť participáciu jednotlivcov v hlasovacom procese a to či už prostredníctvom aktívneho alebo pasívneho volebného práva, ale musí zabezpečiť aby výsledkom volieb bolo slobodné vyjadrenie názoru ľudu bez vonkajšieho ovplyvňovania.⁵⁸

Zoznam použitej literatúry

1. BENTHEM, V. T., HOLLIS, D. B., and DIAS, T.: Information Operations under International Law, In: *Vanderbilt Journal of Transnational Law*, 55 (2022) s. 1217-1286.

⁵⁷ V tejto súvislosti je však možné spomenúť špecifický záväzok štátu v prípade ak je v jeho jurisdikcii využívaná infraštruktúra proti inému štátu. Napríklad štát A cielene zasahuje do volebnej kampane štátu B avšak vykonáva to v štáte C. Nejde iba o hypotetický prípad, pozri napr. HUGHES, Heather. and WAISMEL-MANOR, Israel: 'The Macedonian Fake News Industry and the 2016 US Election', *PS: Political Science & Politics*, 54(1), (2021) s. 19–23.

⁵⁸ Ide do určitej miery o ďalší posun nakoľko už v Reykjavíckej deklarácii z roku 2023 členské štáty Rady Európy potvrdili svoj záväzok usporiadať voľby a referendá v súlade s medzinárodnými štandardmi a prijať všetky vhodné opatrenia proti akémukoľvek zasahovaniu do volebných systémov a procesov. Reykjavícku deklaráciu prijalo 46 členských štátov Rady Európy a Európskej únie na 4. summite v Reykjavíku, ktorý sa konal 16. – 17. mája 2023.. Pozri Appendix III of the Reykjavík Declaration Report dostupný na <https://www.coe.int/en/web/steering-committee-on-democracy/10-principles-for-democracy>. Bližšie pozri taktiež, Foreign interference in electoral processes at local and regional levels, Committee on the Monitoring of the implementation of the European Charter of Local Self-Government and on the respect of Human Rights and the Rule of Law at local and regional levels, CG(2025)48-10, 26 March 2025.

2. BUBECK, Johannes and MARINOV, Nikolay: *Rules and Allies: Foreign Election Interventions*. Cambridge: Cambridge University Press. (2019) s. 278. Online ISBN:9781108652650.
3. BUCHAN, Russell: *Cyber Espionage and International Law*, Bloomsbury Publishing (2018), s.248. ISBN 9781509945016.
4. CARROZZINI, Alina: Shooting Democracy in the Foot?: The Romanian Constitutional Court's Annulment of Presidential Elections, *VerfBlog*, 2024/12/13, Dostupné na [≤https://verfassungsblog.de/shooting-democracy-in-the-foot/≥](https://verfassungsblog.de/shooting-democracy-in-the-foot/).
5. *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], sťažnosť č. 47848/08, ECHR 2014.
6. CORN, Gary P. and TAYLOR, Robert: Sovereignty in the Age of Cyber, In: *American Journal of International Law Unbound*, 111, (2017) s. 207-212.
7. European Commission for Democracy through Law, Venice Commission, Issued on 27 January 2025, CDL-PI(2025)001-e, Urgent Report on the cancellation of election results by Constitutional Courts.
8. Foreign interference in electoral processes at local and regional levels, Committee on the Monitoring of the implementation of the European Charter of Local Self-Government and on the respect of Human Rights and the Rule of Law at local and regional levels. CG(2025)48-10, 26 March 2025.
9. HAMILTON: The Federalist Papers : No. 68 The Mode of Electing the President Friday, March 14, 1788.
10. HUGHES, Heather. and WAISMEL-MANOR, Israel: The Macedonian Fake News Industry and the 2016 US Election, In: *Political Science & Politics*, 54(1), (2021) s. 19–23.
11. International Law and Cyberspace: Finland's National Positions, (2020), s. 3-5. Dostupné na [≤https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbbde-623b-gf86-b254-07d5af3c6d85?t=1603097522727≥](https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbbde-623b-gf86-b254-07d5af3c6d85?t=1603097522727).
12. Island of Palmas (Netherlands v. USA), Award of 4 April 1928, 2 RIAA 829 (1928).
13. Kanadské centrum pre kybernetickú bezpečnosť. Dostupné na [≤https://www.cyber.gc.ca/en/guidance/cyber-threats-elections≥](https://www.cyber.gc.ca/en/guidance/cyber-threats-elections)
14. *Kovačević v. Bosnia and Herzegovina* sťažnosť č. 43651/22 Rozhodnutie zo dňa 25 júna 2025.
15. MARKO, Joseph: A Fallen Curtain and Open Questions: TheGrand Chamber Decision of the European Court of Human Rights in *Kovačević v. Bosniaand Herzegovina*, *VerfBlog*, 2025/8/11, [≤https://verfassungsblog.de/ecthr-voting-bosniaherzegovina/≥](https://verfassungsblog.de/ecthr-voting-bosniaherzegovina/).

16. MATUŠKA, Peter: Rumunský precedens: ústavnoprávne aspekty anulovania výsledku volieb v Slovenskej republike a suverenita volieb, In: *Právnik*, roč. 164, č. 11. (2025), s. 1034—1054.
17. Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14.
18. MILANOVIC Marko: Revisiting Coercion as an Element of Prohibited Intervention in International Law, In: *American Journal of International Law*, 117(4), (2023) s. 601–650.
19. PACE Resolution 2326 (2020): Democracy hacked? How to respond? Text adopted by the Assembly on 31 January 2020 (9th Sitting).
20. PIJPERS, Peter B.M.J.: Careful What You Wish For Tackling Legal Uncertainty in Cyberspace, In: *Nordic Journal of International Law*, 92 (2023), s. 394–421.
21. POTTER, Simon. J: Broadcasting in the Cause of Peace: Regulating International Radio Propaganda in Europe, 1921–1939. In: *The International History Review*, 45(6), (2023). s. 843–864.
22. REEDER, Tyson: "Jefferson's Election as President", *Serpent in Eden: Foreign Meddling and Partisan Politics in James Madison's America*, New York, 2024. ISBN 978-0197628591.
23. REIMANN, Nils: Foreign Electoral Interference : Normative Implications In Light of International Law, Human Rights, and Democratic Theory. sui generis, Zurich, Verlag, 2023, s. 290. ISBN 978-3-907297-37-7.
24. ŘÍHA, Michal: Právo křičet: K oprávnění státu zasahovat do volební soutěže v judikatuře soudů, In: *Právnik*, roč. 155, č. 10, (2016), s. 885-894.
25. SCHMITT, Michael. N: "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, In: *Chicago Journal of International Law*: Vol. 19: No. 1, (2018) s. 3 -67.
26. SCHMITT, Michael. N: Foreign Cyber Interference in Elections, Foreign Cyber Interference in Elections, In: *International Law Studies*. Vol. 97 (2021), s. 739-764.
27. SCHMITT, Michael. N: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press; 2017. s. 648. Online ISBN:9781316822524
28. TSAGOURIAS, Nicholas: Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace', in BROEDERS, Dennis. and BERG, Van Den Berg (eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy*, Bloomsbury Publishing (2020), ISBN 9781786614940.
29. *Verein Klima Seniorinnen Schweiz and Others v. Switzerland [GC]*, sťažnosť č. 53600/20, § 466, 9 April 2024.
30. *Vogt proti Nemecku* (26. september 1995, séria A č. 323).

31. WHEATLEY, Steven: Election hacking, the rule of sovereignty, and deductive reasoning in customary international law, In: *Leiden Journal of International Law*, 36(3), (2023) s. 675–698.

Kontaktné údaje

JUDr. Peter Matuška, PhD., LL.M.
peter.matuska@flaw.uniba.sk
Katedra ústavného práva
Univerzita Komenského v Bratislave
Právnická fakulta

ZODPOVEDNOSŤ ŠTÁTU ZA VOLEBNÚ LEGISLATÍVU V KONTEXTE DIGITÁLNYCH HROZIEB

STATE RESPONSIBILITY FOR ELECTORAL LEGISLATION IN THE CONTEXT OF DIGITAL THREATS

Branislav Korec¹

Abstrakt: Digitálne hrozby predstavujú významnú výzvu v digitálnom veku, keďže rýchle šírenie nepravdivých informácií ovplyvňuje verejné názory a politické rozhodnutia občanov. Volebná kampaň, ako kľúčová fáza volebného procesu, je náchylná na deformáciu vplyvom dezinformácií a záujmových skupín. Tento problém zasahuje do práv občanov na aktívne a pasívne volebné právo, garantovaných Ústavou SR a medzinárodnými normami. Dezinformácie narúšajú schopnosť voličov vytvoriť si kvalifikovaný úsudok, čím ohrozujú rovnosť volebného práva a legitímnosť volieb. Pasívne volebné právo, teda právo byť volený, je ohrozené cieľenými diskreditačnými kampaňami, ktoré znižujú dôveru v politických predstaviteľov. Z tohto pohľadu je právna regulácia volebnej kampane nevyhnutná na ochranu integrity volebného procesu a ochranu základných práv všetkých účastníkov volebnej súťaže, čím vzniká otázka, či súčasná volebná legislatíva Slovenskej republiky dostatočne reaguje na digitálne výzvy. Rovnako aj rozhodovacia činnosť EŠLP, ako aj prelomové rozhodnutia (napríklad Rumunského ústavného súdu) nám dávajú možnosť komparovať kvalitu postupov ako aj volebnej legislatívy v európskom priestore.

Kľúčové slová: volebná kampaň, digitálne hrozby, sloboda politického prejavu, dezinformácie

Abstract: Digital threats pose a significant challenge in the digital age, as the rapid spread of false information influences public opinion and political decisions. The election campaign, as a key stage of the electoral process, is susceptible to distortion due to disinformation and interest groups. This issue affects citizens' rights to active and passive suffrage, guaranteed by the Constitution of the Slovak Republic and international standards. Disinformation disrupts voters' ability to form qualified judgments, thus threatening the equality of voting rights and the legitimacy of elections. The right to stand for election, passive suffrage, is jeopardized by targeted

¹ Právnická fakulta Univerzity Komenského v Bratislave, Katedra ústavného práva.

discrediting campaigns that reduce trust in political representatives. From this perspective, legal regulation of the election campaign is necessary to protect the integrity of the electoral process and safeguard the fundamental rights of all participants in the electoral competition. This raises the question of whether the current electoral legislation of the Slovak Republic adequately responds to digital challenges. Similarly, the case law of the European Court of Human Rights, as well as groundbreaking decisions (such as those of the Romanian Constitutional Court), provides an opportunity to compare the quality of procedures and electoral legislation in the European space.

Key words: election campaign, digital threats, freedom of political expression, disinformation

Úvod

Digitálne hrozby predstavujú jednu z najväčších výziev digitálneho veku. V dobe, kedy veľká časť obyvateľstva čerpá informácie predovšetkým z online prostredia, rýchlo sa šíriace nepravdivé a zavádzajúce informácie ovplyvňujú názory, správanie a do značnej miery aj politické rozhodnutia občanov jednotlivých krajín. Práve predmetné zmeny v spôsobe prijímania informácií, by mala reflektovať aj volebná legislatíva štátov.

Napríklad volebná kampaň, ako jedna z najvýznamnejších etáp volebného procesu, je jednoznačne najohrozenejšou časťou volebného procesu. Volebná kampaň predstavuje prostriedok formovania verejnej mienky, no vplyvom dezinformácií a hybridného pôsobenia záujmových skupín je táto vystavená značnej deformácii.

Výkon aktívneho, ako aj pasívneho volebného práva má byť pritom fundamentálnym prostriedkom participácie občanov na správe vecí verejných. Možno konštatovať, že do aktívneho a pasívneho volebného práva – práv garantovaných Ústavou Slovenskej republiky, ako aj medzinárodnými dokumentami čoraz intenzívnejšie a masívnejšie zasahujú dezinformácie a iné formy klamlivého obsahu. Tieto svojím charakterom oslabujú materiálne predpoklady uplatnenia týchto práv (aktívneho, ako aj pasívneho volebného práva). To v konečnom dôsledku ohrozuje integritu volebného procesu a ich vplyv sa odrazí na samotných výsledkoch volieb.

Z pohľadu aktívneho volebného práva, teda práva voliť, sa dezinformácie a iné formy klamlivého obsahu prejavujú predovšetkým v podobe systematického narúšania schopnosti jednotlivca vytvoriť si kvalifikovaný a slobodný úsudok o politickej „ponuke“. Šírenie nepravdivých alebo manipulatívnych tvrdení o subjektoch volebnej kampane, ako aj o ich volebných programoch či samotnom mechanizme volieb vedie k deformácii volebnej vôle, pričom volič sa rozhoduje nie na základe overených faktov, ale pod vplyvom skresleného informačného prostredia. Takto dochádza k

oslabeniu princípu rovnosti volebného práva, keďže určitá časť voličov je vystavená neprimeranému tlaku manipulatívnych naratívov, čo v konečnom dôsledku spochybňuje legitimitu výsledku volieb.

Na druhej strane, pasívne volebné právo, teda právo byť volený, je dezinformačnými praktikami ohrozené predovšetkým prostredníctvom útokov na integritu a česť kandidátov. Cílené diskreditačné kampane založené na falošných tvrdeniach, môžu odradiť voličov od podpory konkrétnej osoby, čím sa neprimerane zasahuje do jej ústavou zaručeného práva uchádzať sa o volený mandát za podmienok spravodlivej a rovnnej volebnej súťaže. Tento efekt má nielen individuálny rozmer, ale aj širší systémový dopad – dochádza k erózii

dôvery v politických predstaviteľov všeobecne, čím sa oslabuje legitimita zastupiteľských orgánov ako takých.

Predmetné konanie predstavuje zásah do ústavne garantovaných práv, čo by sa nemalo ponechať bez odozvy. V takomto kontexte sa právna regulácia volebnej kampane javí ako nástroj, ktorý síce môže byť predmetom diskusie o hraniciach zásahu do slobody prejavu, no zároveň je nevyhnutný pre zachovanie rovnosti zbraní, integrity volebného procesu a ochrany základných práv všetkých účastníkov volebnej súťaže.

Reflektuje volebná legislatíva v podmienkach Slovenskej republiky výzvy digitálnej revolúcie? Ako na ňu reagoval slovenský zákonodarcia a je potrebné novelizovať niektoré ustanovenia zákonov, alebo nám postačí súčasná právna úprava?

Ako by však mal štát zasahovať do volebnej kampane? Na konkrétnych prípadoch budeme ilustrovať rôzne typy zásahov štátov ako zo Slovenskej republiky, tak zo zahraničia.

Legislatívne vymedzenie volieb a volebnej kampane

Článok 1 ods. 1 Ústavy Slovenskej republiky (ďalej len „Ústavy SR“) hovorí, že „Slovenská republika je zvrchovaný, demokratický a právny štát. Neviaže sa na nijakú ideológiu ani náboženstvo.“ Práve demokratické usporiadanie Slovenskej republiky je kľúčový ústavný princíp, na ktorom stojí novodobá Slovenská republika. V spojení s článkom 2 ods. 1 Ústavy SR, ktorý hovorí že „Štátna moc pochádza od občanov, ktorí ju vykonávajú prostredníctvom svojich volených zástupcov alebo priamo.“ Suverenita ľudu, ktorá je obsiahnutá v článku 2 odseku 1 v spojitosti s princípom demokratického usporiadania Slovenskej republiky vytvára priestor na zakotvenie politických práv v ďalšej hlave Ústavy SR.

Práve v druhej hlave Ústavy SR, ktorá sa venuje základným právam a slobodám, konkrétne v treťom oddieli, ktorý sa venuje politickým právam, môžeme nájsť články 30 a 31 Ústavy SR ktoré sa venujú najdôležitejším politickým právam v demokratickej spoločnosti, a to slobodným voľbám.

Článok 30 Ústavy SR znie: „(1) *Občania majú právo zúčastňovať sa na správe verejných vecí priamo alebo slobodnou voľbou svojich zástupcov. Cudzinci s trvalým pobytom na území Slovenskej republiky majú právo voliť a byť volení do orgánov samosprávy obcí a do orgánov samosprávy vyšších územných celkov.*

(2) *Voľby sa musia konať v lehotách nepresahujúcich pravidelné volebné obdobie ustanovené zákonom.*

(3) *Volebné právo je všeobecné, rovné a priame a vykonáva sa tajným hlasovaním. Podmienky výkonu volebného práva ustanoví zákon.*

(4) *Občania majú za rovnakých podmienok prístup k voleným a iným verejným funkciám.“*

Článok 30 Ústavy SR pôsobí na prvý pohľad veľmi všeobecne, čo môže vyvolávať dojem, že jeho obsahom nie sú priamo základné práva, ale predovšetkým ústavné princípy, ktoré majú určovať rámec uskutočňovania volieb. Samotné podmienky výkonu volebného práva, ako aj pravidlá prípravy a priebehu volieb, sú totiž podrobnejšie rozpracované vo volebných zákonoch, na ktoré ústava výslovne odkazuje v článku 30 odsekoch 2 a 3.

Nemožno však prehliadnuť, že uvedený článok priznáva aj konkrétne, priamo uplatniteľné práva jednotlivcov, čo opakovane potvrdzuje judikatúra Ústavného súdu SR.²

Ústava SR predovšetkým nastrojuje právny režim, v ktorom účasť voliča v ktorýchkoľvek voľbách má povahu oprávnenia a nezakladá sa ním povinnosť voliča zúčastniť sa aktívne na správe verejných vecí uplatnením aktívneho alebo pasívneho volebného práva.³

Drgonec zhrnul článok 30 Ústavy SR tak, že „*Pokiaľ ide o spôsob ustanovovania zákonodarného orgánu, ústava vyžaduje ‚slobodné voľby svojich zástupcov občanmi‘ (čl. 30 ods. 1 ústavy), ktoré sa uskutočňujú ‚v lehotách nepresahujúcich pravidelné volebné obdobie‘ (čl. 30 ods. 2 ústavy) prostredníctvom ‚všeobecného, rovného a priameho volebného práva s tajným hlasovaním‘ (čl. 30 ods. 3 ústavy) a za dodržania ‚rovnakých podmienok prístupu občanov k voleným verejným funkciám‘ (čl. 30 ods. 4 ústavy), ktorými v tomto prípade sú funkcie poslancov v zákonodarnom orgáne.“⁴*

Rovnako právo zúčastňovať sa na správe vecí verejných je garantované aj v Listine základných práv a slobôd. Listina v čl. 21 hovorí:

„(1) *Občania majú právo zúčastňovať sa na správe verejných vecí priamo alebo slobodnou voľbou svojich zástupcov.*

² DRGONEC, J.: Ústava Slovenskej republiky. 2. vydanie. Bratislava: C. H. Beck, 2019, s. 734.

³ Tamtiež.

⁴ DRGONEC, J.: Ústava Slovenskej republiky. 2. vydanie. Bratislava: C. H. Beck, 2019, s. 547 – 548. Pozri tiež: Uznesenie Ústavného súdu SR sp. zn. PL. ÚS 22/2000.

(2) *Voľby sa musia konať v lehotách, ktoré nepresahujú pravidelné volebné obdobia ustanovené zákonom.*

(3) *Volebné právo je všeobecné a rovné a vykonáva sa tajným hlasovaním. Podmienky výkonu volebného práva ustanoví zákon.*

(4) *Občania majú za rovnakých podmienok prístup k voleným a iným verejným funkciám.“*

Medzinárodnoprávny rozmer ochrany práva zúčastňovať sa na správe vecí verejných je obsiahnutý aj v čl. 25 Medzinárodného paktu o občianskych a politických právach. Článok 25 Medzinárodného paktu o občianskych a politických právach znie: *“Každý občan má právo a možnosť bez akýchkoľvek rozdielov uvedených v článku 2 a bez neodôvodnených obmedzení: a) zúčastňovať sa na vedení verejných záležitostí priamo alebo prostredníctvom slobodne volených zástupcov; b) voliť a byť volený v pravidelných voľbách, ktoré sa budú konať na základe všeobecného a rovného hlasovacieho práva, tajným hlasovaním zabezpečujúcim slobodu hlasovania; c) vstúpiť za rovnakých podmienok do verejných služieb svojej krajiny.“*

Medzinárodný pakt o občianskych a politických právach výslovne predpokladá právo každého občana zúčastňovať sa na správe verejných záležitostí priamo alebo prostredníctvom slobodne zvolených zástupcov.

Rovnako EDLP v článku 3 hovorí: *„Vysoké zmluvné strany sa zaväzujú konať v rozumných intervaloch slobodné voľby s tajným hlasovaním za podmienok, ktoré zabezpečia slobodné vyjadrenie názorov ľudu pri voľbe zákonodarného zboru.“* Zaujímavosťou je, že pôvodný dohovor neobsahoval ochranu volebného práva. Tento rozmer získal až dodatkovým protokolom č.1.

Právo na slobodné voľby zahŕňa právo voliť a právo byť volený.⁵ Okrem toho to pre členské štáty znamená aj pozitívny záväzok zabezpečiť podmienky, za ktorých si ľudia môžu slobodne vytvárať a vyjadrovať svoje názory a vyberať si svojich zástupcov.

ESLP predmetné konštatovanie potvrdil, keď konštatoval že *„slobodné voľby a sloboda prejavu, najmä sloboda politickej diskusie, spoločne tvoria základ akéhokoľvek demokratického systému“*.⁶ ESLP ďalej uviedol, že obe práva sú navzájom prepojené a pôsobia tak, aby sa navzájom posilňovali, pričom sloboda prejavu je jednou z podmienok potrebných na zabezpečenie slobodných volieb. Aby boli práva zaručené čl. 3 dodatkového protokolu účinné, ochrana sa vzťahuje aj na predvolebnú kampaň. Z tohto dôvodu je v období pred voľbami obzvlášť dôležité, aby sa názory a

⁵ Mathieu-Mohin a Clerfayt v. Belgicku. Rozsudok z 2. marca 1987 k sťažnosti č. 926789/1 a Ždanoka v. Lotyšsko z 16. Marca 2006 k sťažnosti č. 58278/00.

⁶ Bowman v. Spojené kráľovstvo. Rozsudok z 19. februára 1998 k sťažnosti č. 24839/94.

informácie všetkých druhov mohli voľne šíriť.⁷ Shattock, konštatuje, že ochrana slobodných volieb zahŕňa aj kvalitatívny rozmer informovanosti voliča a umožňuje štátom primerane reagovať na dezinformačné naratívy, pokiaľ ich zásahy spĺňajú test nevyhnutnosti a proporcionality.⁸ Podľa ESĽP majú členské štáty pozitívny záväzok zabezpečiť efektívnu slobodu prejavu: ESĽP požaduje vytvoriť priaznivé prostredie pre účasť všetkých dotknutých osôb na verejnej diskusii, ktorá im umožní bez obáv vyjadrovať svoje názory a nápady. Štát sa musí nielen zdržať akéhokoľvek zasahovania do slobody prejavu jednotlivca, ale musí mať aj pozitívny záväzok chrániť jeho právo na slobodu prejavu pred útokmi, vrátane útokov zo strany súkromných osôb.⁹

ESĽP uznal, že za určitých okolností môžu byť práva podľa čl. 10 EDĽP a čl. 3 dodatkového protokolu v rozpore a že v období pred voľbami alebo počas nich možno považovať za nevyhnutné zaviesť určité obmedzenia slobody prejavu, ktoré by inak neboli prijateľné, aby sa tak zabezpečilo slobodné vyjadrenie názoru ľudí pri voľbe zákonodarného zboru.¹⁰ ESĽP tiež uznal, že pri hľadaní rovnováhy medzi týmito dvoma právami majú členské štáty priestor na voľnú úvahu, ako ho spravidla majú v súvislosti s organizáciou ich volebných systémov. Súčasne zdôraznil, že akékoľvek obmedzenia slobody prejavu musia byť úmerné legitímnemu cieľu. Uviedol napríklad, že čl. 10 EDĽP ako taký nezakazuje diskusiu ani šírenie získaných informácií, aj keď existuje silné podozrenie, že tieto informácie nemusia byť pravdivé.¹¹

ESĽP vo svojej rozhodovacej činnosti označuje práva podľa článku 3 dodatkového protokolu k EDĽP ako nie absolútne. Existuje teda priestor pre nevyhnutné obmedzenia. Členským štátom treba v tejto oblasti poskytnúť širokú mieru voľnej úvahy. Pri skúmaní súladu s čl. 3 dodatkového protokolu sa ESĽP zameral predovšetkým na dve kritériá: či prišlo k svojvôli alebo disproporcionalite a či obmedzenie zasahovalo do slobodného vyjadrovania názoru ľudí.¹²

⁷ Bowman v. Spojené kráľovstvo. Rozsudok z 19. februára 1998 k sťažnosti č. 24839/94.; Orlovskaya Iskra v. Rusko, Rozsudok z 21. februára 2017 k sťažnosti č. 42911/08.

⁸ Shattock, E. (2022). Free and Informed Elections? Disinformation and Democratic Elections under Article 3 of Protocol 1 of the ECHR. *Human Rights Law Review*, 22(4), ngaco23. DOI: 10.1093/hrlr/ngaco23.

⁹ Dink v. Turecku. Rozsudok z 14. septembra 2010 k sťažnosti č. 2668/07, 6102/08, 30079/08, 7072/09 a 7124/09.

¹⁰ Bowman v. Spojené kráľovstvo. Rozsudok z 19. februára 1998 k sťažnosti č. 24839/94.; Orlovskaya Iskra v. Rusko, Rozsudok z 21. februára 2017 k sťažnosti č. 42911/08.

¹¹ Salov v. Ukrajine. Rozsudok z 6. septembra 2005 k sťažnosti č. 655118/01.

¹² Mathieu-Mohin a Clerfayt v. Belgicku. Rozsudok z 2. marca 1987 k sťažnosti Č. 926789/1 a Ždanoka v. Lotyšsko z 16. Marca 2006 k sťažnosti č. 58278/00.

Druhým relevantným článkom Ústavy SR, ktorý vymedzuje nie konkrétne právo, ale ústavný princíp, je článok 31. K jeho zakotveniu prišlo práve v kontexte spoločenských zmien po roku 1989. Jeho hlavným účelom je ochrana demokratickej súťaže politických síl v demokratickej spoločnosti.¹³ Článok 31 znie: „*Zákonná úprava všetkých politických práv a slobôd a jej výklad a používanie musia umožňovať a ochraňovať slobodnú súťaž politických síl v demokratickej spoločnosti.*“

Identickú úpravu obsahuje aj Listina a to v čl. 22: „*Zákonná úprava všetkých politických práv a slobôd a jej výklad a používanie musí umožňovať a ochraňovať slobodnú súťaž politických síl v demokratickej spoločnosti.*“

Volebná kampaň, ako jedna z najvýznamnejších etáp volebného procesu, je obdobím zvýšeného záujmu obyvateľstva štátu o veci verejné. Rovnako je obdobím zvýšeného významu informácií o verejných záležitostiach.¹⁴ V skutočnosti je len ťažko predstaviteľné, že bez volebnej kampane by kandidát získal priazeň voličov a následne mandát. Majerčák definuje volebnú kampaň ako „*štádium volebného procesu, v rámci ktorého sa vo voľbách kandidujúce subjekty usilujú maximalizovať rôznymi formami volebnej agitácie svoj volebný zisk*“.¹⁵ Avšak nato, aby nedochádzalo k neprimeranému porušovaniu základných práv a slobôd, je priam nevyhnutná správne nastavená a efektívna právna úprava volebnej kampane.¹⁶

Regulácia volebnej kampane je záujmom každého suverénneho demokratického štátu, a to nie len preto, aby dokázala garantovať obyvateľom základné právo na informácie, ale aj preto, aby zabezpečila férovosť slobodnej súťaže politických síl a rovnosť (pasívneho) volebného práva. „*Záväzok Národnej rady SR pri prijímaní zákonov upravujúcich politické práva a slobody schváliť iba také zákony, ktorými sa umožní a chráni slobodná súťaž politických síl v spoločnosti. Obsahom princípu v čl. 31 je zároveň aj záväzok ostatných orgánov verejnej moci uplatňovať zákony upravujúce politické práva jedine spôsobom, ktorý umožní a ochráni slobodnú súťaž politických síl.*“¹⁷ Z rozhodnutia Ústavného súdu SR jasne vyplýva, že limituje zákonodarnú moc pri tvorbe tých zákonov a ich novelizácií, ktoré sa dotýkajú politických práv tretieho oddielu druhej hlavy Ústavy SR.

Obdobne argumentoval aj EŠLP, keď pre účinné garantovanie práva zúčastňovať sa na správe verejných vecí prostredníctvom slobodnej voľby zástupcov, resp. uplatnenie práva na slobodné voľby v súlade s dohovorom je tiež nevyhnutná

¹³ DRGONEC, J.: Ústavné právo hmotné. Bratislava : C. H. Beck, 2018, s. 155

¹⁴ Nález Ústavného súdu SR sp. zn. PL. ÚS 15/98.

¹⁵ MAJERČÁK, T. a kol.: Sloboda prejavu a jej limity - IV. ústavné dni. Košice UPJŠ 2016, s. 101

¹⁶ Uznesenie Ústavného súdu SR sp. zn. PL. ÚS 22/2000.

¹⁷ Nález Ústavného súdu SR sp. zn. PL. ÚS 19/98.

existencia jasných, jednoznačných a zrozumiteľných ustanovení volebných zákonov.¹⁸

ESLP rovnako konštatoval, vychádzajúc z odporúčaní Benátskej komisie v Kódexe dobrej praxe vo volebných veciach, že podstatná zmena volebných zákonov by mala prebiehať najmenej rok pred konaním volieb, a to najmä pokiaľ predmetom zmien majú byť podmienky týkajúce sa možnosti zúčastniť sa volieb.¹⁹

Ak má takáto právna úprava chrániť slobodné rozhodovanie občanov, je na mieste otázka, či (nie) je nutnosťou legislatívne sa vysporiadať s narastajúcim trendom cieľenej manipulácie občanov prostredníctvom rôznych informačných tokov, najmä počas volebnej kampane. Nie je ničím zvláštne, že sa (dez)informácie v čase získavania politickej podpory stávajú stratégiou na zdiskreditovanie oponentov a na nasmerovanie sympatie voličov na jednu alebo druhú stranu.

Ak by sa aj vyskytlo podozrenie, že prišlo k porušeniu ústavných práv vo volebnej kampani, v podmienkach Slovenskej republiky existuje viacero procesnoprávných nástrojov, ktoré smerujú k eliminácii možných zásahov do slobodného a riadneho priebehu volieb. Patria sem predovšetkým prostriedky súdnej ochrany, ako je žaloba na správnom súde proti rozhodnutiu o nezaregistrovaní kandidáta alebo kandidátnej listiny, ako aj možnosť súdne napadnúť nezákonnosť, resp. neústavnosť volieb. V prípade volieb do Národnej rady SR, volieb do Európskeho parlamentu a volieb prezidenta SR je príslušným orgánom na rozhodovanie o zákonnosti a ústavnosti volieb Ústavný súd SR, zatiaľ čo voľby do orgánov územnej samosprávy spadajú do právomoci novozriadeného Najvyššieho správneho súdu Slovenskej republiky.

Právna úprava volebnej kampane v podmienkach Slovenskej republiky

Slovenský Normotvorca ukotvil problematiku volieb v slovenskom právnom poriadku najmä v (i) zákone číslo 181 z 29. mája 2014 o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov (ďalej len „*zákon o volebnej kampani*“), (ii) zákone číslo 180 z 29. mája 2014 o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov (ďalej len „*zákon o podmienkach výkonu volebného práva*“) a (iii) zákone číslo 85 zo 4. februára 2005 o politických stranách a politických hnutiach (ďalej len „*zákon o politických stranách*“).

¹⁸ Porovnaj rozhodnutie ESLP vo veci Koutmeridis a Zaharakis v. Grécku. Rozsudok z 10. apríla 2008 k sťažnosti č. 27863/05, č. 27863/05 a č. 28422/05.

¹⁹ DOMIN, M. In: OROSZ, Ladislav – SVÁK, Ján. a kol.: Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava : Wolters Kluwer SR s. r. o., 2021, s. 451-452, Porovnaj tiež: Rozsudok ESLP vo veci Ekoglasnost v. Bulharsko zo 6. novembra 2012 k sťažnosti č. 30386/05.

Kedže moderné technológie a s nimi spojené digitálne hrozby sa najviac dotýkajú obdobia pred voľbami, teda najmä obdobia počas volebnej kampane, bližšie sa pozrieme na ustanovenia zákona o volebnej kampani.

Normotvorca v naposledy citovanom zákone podľa nášho názoru reflektoval právnu úpravu spôsobom adekvátnym pomerom v spoločnosti, v čase nadobudnutia jeho účinnosti. Avšak, podľa Globálnej digitálnej správy 2018 zo 7,6 miliardy obyvateľov planéty využíva internet približne 4 miliardy osôb (t. j. 53 % celkovej populácie) a 3,2 miliardy sú aktívnymi používateľmi sociálnych médií (42 % celkovej populácie). Medzi rokmi 2017 a 2018 došlo k nárastu počtu používateľov internetu o 7 % a počtu aktívnych používateľov sociálnych médií o 13 %. Priemerný používateľ internetu trávi online približne 6 hodín denne, pričom značná časť tohto času je venovaná platformám ako Facebook (viac ako 2 miliardy používateľov), YouTube (1,5 miliardy), Instagram (800 miliónov) a Twitter (330 miliónov). Sociálne siete, ktoré denne využíva približne 2 miliardy osôb, sa tak stali integrálnou súčasťou súčasných politických kampaní. Ich účinok na verejnosť je determinovaný viacerými faktormi, ako sú zvolené komunikačné kanály (napr. Twitter verzus Instagram), špecifické charakteristiky a predispozície publika, motivácia používateľov či celkový rámec politickej kampane. Podľa správy *Reuters Institute Digital News Report 2017* predstavujú sociálne médiá dominantný zdroj spravodajstva pre osoby vo veku 18 až 34 rokov.²⁰

Avšak, aktuálne dáta poukazujú na radikálny posun v mediálnom a komunikačnom prostredí, ktorý potenciálne vyžaduje revíziu legislatívneho rámca. Podľa správy *Digital News Report 2023* od Reuters Institute približne 30 % respondentov uviedlo, že primárne získavajú správy prostredníctvom sociálnych médií, zatiaľ čo len 22 % spravodajské weby či aplikácie.²¹

V roku 2024 táto dynamika pokročila: správanie publika sa posunulo od tradičného „web-správy“ smerom k video-platformám a posielaniu správ cez aplikácie.²² Príkladom posunu je, že vyhľadávanie a sociálne médiá už preberajú primárnu úlohu

²⁰ REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. *Digital News Report 2017* [online]. Oxford: Reuters Institute, University of Oxford, 2017 [cit. 2025-09-12]. Dostupné na: <https://www.digitalnewsreport.org/survey/2017/>

²¹ REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. *Digital News Report 2023* [online]. Oxford: Reuters Institute, University of Oxford, 2023 [cit. 1.11.2025]. Dostupné na: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023>

²² REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. *Digital News Report 2024* [online]. Oxford: Reuters Institute, University of Oxford, 2024 [cit. 1.11.2025]. Dostupné na: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024>

ako vstupné brány k online správam, zatiaľ čo priama návšteva spravodajských webov stratila relatívnu váhu.²³

Rovnako narastá počet ľudí, ktorí sa správam vyhýbajú – v roku 2024 až 39 % respondentov uviedlo, že sa niekedy alebo často správam vyhýbajú (oproti 29 % v roku 2017).²⁴ Tento posun indikuje, že mediálna komunikácia sa stáva menej stabilnou a viac závislou od algoritmov, platformových stratégií a rýchlych zmien koncových užívateľov.

Slovenský normotvorca § 2 ods.1 zákona o volebnej kampani rámcuje legálnu definíciu volebnej kampane. Touto sa rozumie *„akákoľvek činnosť politickej strany, politického hnutia, koalície politických strán a politických hnutí a kandidátov, za ktorú sa obvykle platí úhrada, smerujúca k propagácii ich činnosti, cieľov a programu za účelom získania funkcie volenej podľa osobitného predpisu. Rozumie sa tým činnosť v prospech aj v neprospech subjektov podľa prvej vety.“*

Ustanovenie § 14 ods.1 zákona síce obsahuje imperatív zakazujúci „zverejňovať informácie o kandidujúcich politických stranách, kandidujúcich koalíciách politických strán, kandidátoch na prezidenta a kandidátoch na funkcie do orgánov územnej samosprávy v ich prospech alebo neprospech v rozhlasovom vysielaní, v televíznom vysielaní, v rámci audiovizuálnej mediálnej služby na požiadanie, v periodických publikáciách, neperiodických publikáciách a v agentúrnom spravodajstve je 48 hodín pred dňom konania volieb a v deň konania volieb až do skončenia hlasovania zakázané,“ avšak „ustanovenia odseku 1 sa nevzťahujú na vysielanie prostredníctvom internetu.“ Z uvedeného potom logicky vyplýva, že internet ako online priestor nie je dotknutý normami predmetného zákona. Nie je tomu ale úplne tak. Komparatívne možno doplniť, že, Meyer a Brown poukazujú na to, že efektívna právna reakcia na digitálne zasahovanie do volebných procesov nespočíva v rozširovaní tradičných mediálnych moratórií na online prostredie, ale v kombinácii štátnej regulácie s internými povinnosťami platforiem a to najmä transparentnosťou politickej inzercie, označovaním zdrojov financovania a povinnosťou auditovateľného moderovania obsahu počas kampane.²⁵

²³ STATISTA. *Main Gateway to Online News Worldwide from 2014 to 2024* [online]. Hamburg: Statista GmbH, 2024 [cit.1.11.2025]. Dostupné na: <https://www.statista.com/chart/32452/gateways-to-online-news/>

²⁴ YOUNGOV. *3 Key Findings About News Consumption from the Digital News Report 2024* [online]. London: YouGov, 2024 [cit.1.11.2025]. Dostupné na: <https://business.yougov.com/content/49776-3-key-findings-about-news-consumption-from-the-digital-news-report-2024>

²⁵ Marsden, C. T., Meyer, T., & Brown, I. (2020). *Platform values and democratic elections: How can the law regulate digital disinformation?* Computer Law & Security Review, 36, 105373. DOI: 10.1016/j.clsr.2019.105373.

Čo je však potrebné považovať za vysielanie prostredníctvom internetu interpretovala Rada pre vysielanie a retransmisiu zdôrazňujúc, že ide len o také vysielanie, ktoré je realizované výhradne prostredníctvom internetu. Naopak, vysielanie programovej služby, ktorá je v totožnej forme vysielaná aj iným spôsobom ako prostredníctvom internetu, teda „klasickým“ rozhlasovým alebo televíznym vysielaním, nebude spod zákonnej regulácie vysielania vyňaté.²⁶

Spod zákonnej regulácie vysielania preto nebude vyňaté tzv. online vysielanie televízie, ktoré je súčasne vysielané aj prostredníctvom „klasického“ televízneho vysielania. Vyňatie vysielania prostredníctvom internetu zo zákazu formulovaného v odseku 1 komentovaného paragrafu, podobne ako jeho vyňatie z obmedzení týkajúcich sa vysielania politickej reklamy (§ 12 volebného kódexu), súvisí pravdepodobne aj s tým, že na vysielanie prostredníctvom internetu sa nevyžaduje získanie licencie, ale len splnenie oznamovacej povinnosti.²⁷

Rovnako aj Ústavný súd SR rozhodol, že § 14 zákona o volebnej kampani sa nevzťahuje na zverejnenie informácií o kandidujúcich subjektoch na Facebooku tesne alebo počas moratória. Rovnako nie je dôležité, či by zverejnené informácie boli v prospech alebo v neprospech dotknutých subjektov volebnej kampane. Takéto zverejnenie by teda nebolo porušením zákona, ak by išlo o bezodplatnú činnosť, mimo online stránok televízií a ostatných vysielateľov, ktorý spadajú pod reguláciu § 14 odseku 1.²⁸

Nepopierateľný rozmach digitalizácie *de facto* umožňuje preniesť politický boj vo volebnej kampani do značne právom neupraveného online priestoru. Sledovanosť youtubových kanálov a sociálnych sietí v podstate plne nahrádza mainstream.

§ 15 zdanlivo normatívne vyčerpávajúco pokrýva možné negatívne ingerencie do volebnej kampane. Z uvedeného ustanovenia vyplýva, že *„každý, kto vedie volebnú kampaň podľa tohto zákona, je povinný zabezpečiť, aby odvysielaná politická propagácia, zverejnená platená inzercia, zverejnené volebné plagáty a všetky ďalšie spôsoby vedenia volebnej kampane obsahovali údaje o objednávateľovi a dodávateľovi v rozsahu meno, priezvisko a obec trvalého pobytu, ak ide o fyzickú osobu, a názov a sídlo a identifikačné číslo organizácie, ak ide o právnickú osobu; to isté sa vzťahuje aj na prezentáciu volebných prieskumov a volebných ankiet.“*

Podľa rozhodnutia Ústavného súdu SR, osoby aktívne sa zúčastňujúce na volebnej kampani môžu porušiť právo na rovnosť šancí tým, že v rámci volebnej kampane

²⁶ DOMIN, M.: Zákon o volebnej kampani - komentár. 2019. Bratislava : Wolters Kluwer. s. 169.

²⁷ Tamtiež.

²⁸ DOMIN, M.: Zákon o volebnej kampani - komentár. 2019. Bratislava : Wolters Kluwer. s. 170. Porovnaj tiež: Uznesenie ÚS SR z 25. februára 2015, sp. zn. PL. ÚS 62/2014. Podobne Ústavný súd SR rozhodol aj v rozhodnutiach z 25. februára 2015, sp. zn. PL. ÚS 33/2014 a z 18. februára 2015, sp. zn. PL. ÚS 34/2014.

nezákonným alebo neústavným spôsobom pôsobia v prospech alebo v neprospech jednej politickej sily.²⁹ Toto rozhodnutie ale nemôžeme uplatniť na zákonom neregulovaný priestor a zákonom neregulované osoby.

Zároveň je potrebné zdôrazniť, že povinnosť zabezpečiť transparentnosť volebnej kampane sa nevzťahuje na fyzické osoby mimo okruhu subjektov volebnej kampane. Môžeme teda konštatovať, že pod pojem každý, kto vedie volebnú kampaň, môžeme subsumovať politické strany, ich koalície a kandidátov. Toto vymedzenie je veľmi úzke a dáva priestor viesť kampaň v prospech subjektov volebnej kampane rôznym osobám so širokým dopadom. Šírenie prejavov s politicky senzitívnym obsahom na internete v čase volebného moratória je veľmi slabo regulované zákonom o volebnej kampani. V praxi nie je predstaviteľné, že aktivity v prospech kandidáta vykonávané prostredníctvom fyzických osôb mimo radov politikov (napríklad influencera na sociálnej sieti), bez preukázanej objednávky takejto ich činnosti, budú postihnuté normami komentovaného zákona. Taktiež rôzne youtubové vysielanie politicky senzitívneho obsahu nie je možné považované za politickú propagáciu, ak absentuje prvok zmluvného vzťahu medzi treťou osobou a subjektom volebnej kampane. Z uvedeného preto vyplýva, že takéto legislatívne vákuum môže byť zneužitie na vedenie politického boja nie len samotnými subjektami volebnej kampane, ale aj subjektmi s určitým zisťným záujmom na výsledku volieb a s tým súvisiaceho usporiadania spoločnosti po nich.

Aj keď doplnenie súčasnej volebnej legislatívy v podmienkach Slovenskej republiky je nevyhnutné, je dôležité poukázať aj na to, že ESLP uznal, že vzhľadom na dôležitú úlohu, ktorú internet zohráva pri zlepšovaní prístupu verejnosti k spravodajstvu a uľahčovaní šírenia informácií, funkciu bloggerov a používateľov sociálnych médií možno v súvislosti s ochranou čl. 10 prirovnať k „verejnému strážnemu psovi“.³⁰ Táto ochrana sa môže rozšíriť na prístup k (verejne prístupným) informáciám, ak slúžia na uplatňovanie práva na slobodu prejavu.

ESLP rovnako uznal právo fyzických a právnických osôb na prístup na internet, pretože vo svojom rozsudku proti hromadnému blokovaniu online obsahu uviedol, že *„internet sa v súčasnosti stal jedným z hlavných spôsobov uplatňovania práva na slobodu prejavu a informácií, pretože poskytuje základné nástroje účasti na aktivitách a diskusiách týkajúcich sa politických otázok a otázok všeobecného záujmu“*.³¹ Článok 10

²⁹ Uznesenie Ústavného súdu SR sp. zn. PL. ÚS 51/2018.

³⁰ Magyar Helsinki Bizottság v. Maďarsko. Rozsudok z 8. novembra 2016 k sťažnosti č. 18030/11. Pozri tiež: Animal Defenders International v. Spojené kráľovstvo. Rozsudok z 22. apríla 2013 k sťažnosti č. 48876/08.

³¹ Ahmet Yildirim v. Turecko. Rozsudok z 18. decembra 2012 k sťažnosti č. 3111/10. Pozri tiež: Cengiz a ďalší v. Turecko. Rozsudok z 1. decembra 2015 k sťažnosti č. 48226/10 a 14027/11.

EDLP garantuje slobodu prejavu, ktorá zahŕňa aj slobodu prijímať a rozširovať informácie a myšlienky bez ohľadu na štátne hranice. Blokovanie prístupu nielen k webovým stránkam, ktoré sú predmetom konania, ale aj k webovým stránkam hostiteľa či tretích osôb, má za následok znemožnenie prístupu k množstvu informácií, čím dochádza k zásahu do základného práva používateľov internetu. ESLP zdôraznil, že takýto zásah môže byť v súlade s EDLP iba za predpokladu existencie precízneho a prísneho právneho rámca, ktorý zahŕňa účinnú súdnu kontrolu, ako garanciu proti svojvoľnému alebo neprimeranému obmedzovaniu slobody prejavu.³²

Prelomové rozhodnutia ESLP

Prelomovým sa nateraz v judikatúre ESLP zdá rozhodnutie v prípade *Bradshaw a spol. proti Spojenému kráľovstvu*. ESLP dospel k záveru, že nedošlo k porušeniu článku 3 Protokolu č. 1 k Európskemu dohovoru o ľudských právach aj napriek dôveryhodným dôkazom, že vláda Ruskej federácie zasahovala vo viacerých prípadoch do politiky Spojeného kráľovstva. Aj pod ťarchou kritiky, že Spojené kráľovstvo konalo neskoro a s nepresvedčivými opatreniami, ESLP rozhodol, že tieto spomenuté nedostatky nie sú „dostatočne závažné, aby narušili samotnú podstatu práva žiadateľov“. ESLP rozhodol, že článok 3 protokolu č. 1 k dohovoru môže zaviazat štát, aby vyšetril zasahovanie do svojich volieb len vtedy, ak by to bránilo prijatiu opatrení na ochranu práva občanov na prospech z volieb „za podmienok, ktoré zabezpečujú slobodné vyjadrenie názoru ľudí“. ³³ V rokoch 2022 až 2023 vláda Spojeného kráľovstva po zverejnení správ o údajnej manipulácii volieb zo strany Ruskej federácie prijala niekoľko zákonov, vrátane zákona o voľbách 2022, zákona o národnej bezpečnosti 2023 a zákona o online bezpečnosti 2023. Cieľom týchto legislatívnych opatrení bolo zabezpečiť ochranu pred zahraničným zasahovaním a šírením dezinformácií počas volieb. Podľa ESLP tieto kroky Spojeného kráľovstva dokazujú pokus vyšetriť a brániť zahraničnej intervencii, ktorá by mohla ohrozovať slobodné a demokratické voľby. To v konečnom dôsledku viedlo k tomu, že ESLP nezistil žiadne porušenie článku 3 protokolu č. 1 k dohovoru.

ESLP jasne v tomto prípade nastavil smer nezasahovania do výsledkov volieb, aj pri preukázateľnej manipulácii. Je samozrejme potrebné skúmať rozsah a mieru zasahovania do slobodného výberu voličov.

³² Tamtiež.

³³ *Bradshaw a spol. v. Spojené kráľovstvo*. Rozsudok z 16. január 2023, k sťažnosti č. 15653/22.

Rozhodnutie Rumunského ústavného súdu

Aj v kontexte rozhodnutia Bradshaw a spol. proti Spojenému kráľovstvu je zaujímavý prípad z Rumunska, konkrétne z prezidentských volieb. Rumunsko sa v decembri 2024 ocitlo v bezprecedentnej situácii, keď Ústavný súd Rumunska (Curtea Constituțională a României) (ďalej len „CCR“) zrušil celý proces prezidentských volieb. Verdikt, ktorý padol 6. decembra 2024, dva dni pred plánovaným druhým kolom, je v dejinách postsocialistickej Európy unikátny a vyvolal rozsiahlu politickú i odbornú diskusiu.

Podľa čl. 146 písm. f) Ústavy Rumunska patrí do právomoci CCR preskúmať ústavnosť a zákonnosť volieb, ako aj potvrdzovať ich výsledky. Rozhodnutia CCR sú pritom konečné a všeobecne záväzné. Na tomto základe mohol súd zasiahnuť nielen vo vzťahu k výsledkom, ale aj k celému priebehu volieb. Zákonný rámec tvoril predovšetkým zákon č. 370/2004 o voľbe prezidenta, doplnený vládnymi nariadeniami, ktoré určovali konkrétne termíny a organizačný kalendár.

Na úvod je dôležité chronologicky zarámcovať priebeh udalostí. 24. november 2024 sa uskutočnilo prvé kolo prezidentských volieb. Výsledky stanovili postupujúcich kandidátov do druhého kola. 2. december 2024 CCR prijal Rozhodnutie č. 31/2024, ktorým potvrdil zákonnosť prvého kola a určil dvojicu kandidátov do druhého kola plánovaného na 8. decembra. 4. december 2024 po zasadnutí Najvyššej rady národnej bezpečnosti (CSAT) boli odtajnené správy bezpečnostných služieb (SRI, SIE, STS a ďalších), ktoré obsahovali závažné informácie o narušení integrity volieb a o podozrivom financovaní kampane jedného z kandidátov. 6. december 2024 CCR vydal Rozhodnutie č. 32/2024, ktorým v plnom rozsahu anuloval prezidentské voľby a nariadil ich zopakovanie od začiatku. Rozhodnutie zdôvodnil vážnym narušením princípov spravodlivých a slobodných volieb. Druhé kolo, ktoré sa malo konať 8. december 2024 sa neuskutočnilo. V apríli odvolací súd v Ploješti spôsobil kontroverziu, keď dočasne pozastavil účinnosť rozhodnutia CCR. Tento krok však nemohol zvrátiť organizáciu nových volieb, pretože rozhodnutia CCR majú nadradený charakter a sú *erga omnes* záväzné.

Ako teda hodnotiť tento bezprecedentný zásah zo strany CCR? V prvom rade je dôležité podotknúť, že CCR nemá možnosť posudzovať *ex offio* výsledky a priebeh volieb, ako aj volebnej kampane. Zásadný argument odporcov rozhodnutia je teda nedostatočná procesná legitimita CCR. CCR môže na návrh oprávnených subjektov kontrolovať priebeh volieb, ale to až 3 dni po ich skončení. Ďalším argumentom odporcov rozhodnutia CCR je to, že len 4 dni pred prijatím rozhodnutia zrušiť výsledky prvého kola prezidentských volieb, tieto výsledky potvrdil. Obdobná dezinformačná kampaň, ktorú potvrdili aj spravodajské služby, prebiehala aj pred parlamentnými voľbami. Pri tomto obdobnom zasahovaní do volebnej kampane a integrity volieb ale CCR nezasiahol. Rovnako aj údajné podozrenia z masívneho

zásahu do volebnej kampane sa zdajú byť otázne, keďže nad všetku pochybnosť neboli tieto informácie v čase prijatia rozhodnutia CCR potvrdené. Postup CCR odsúdila aj protikandidátka pána Calina Georgescu, ktorý vyhral prvé kolo zrušených prezidentských volieb. Zásah do volieb zo strany cudzích štátov nie je ničím neobvyklí. V európskom priestore je ale bezprecedentné, aby sa na základe takéhoto zásahu, ktorý nie je jasne preukázaný, pristúpilo k tak reštriktívnemu kroku, ako je zrušenie výsledkov demokratických volieb. Aj s poukázaním na ostatné procesné a vecné nezrovnalosti v kontexte rozhodnutia CCR môžeme konštatovať, že prístup ktorý nastolil CCR nie je nasledovania hodný v demokratickom a právnom štáte v európskom priestore.

Záver

Ako sme už naznačili v príspevku, legislatívna úprava volieb a volebnej kampane v podmienkach Slovenskej republiky zlyháva v dvoch rovinách. Nedostatočné vymedzenie priestoru, kde sa vedie dnes politický zápas je problém, s ktorým by sa mal slovenský zákonodarca vysporiadať. Rovnako aj vymedzenie, kto každý vedie politickú kampaň v prospech subjektov volebnej kampane vykazuje značné nedostatky. V tomto kontexte je možno vhodné zamyslieť sa nad znovuzavedením tretích osôb do volebnej kampane.

Ako nám vyplýva aj z rozhodnutí ESLP, Ústavného súdu SR, ale ako ukazujú aj prípady zo Spojeného kráľovstva no najmä z Rumuska, výzvy digitálnej revolúcie budú narastať a štáty budú musieť regulovať podrobnejšie slobodnú demokratickú súťaž. Treba byť ale veľmi zdržanlivý pri zásahoch do slobodného priebehu volieb a volebnej kampane. Naopak rušenie platných výsledkov volieb vnímame ako bezprecedentný zásah do vôle ľudu, ktorý si v pravidelných intervaloch má slobodne voliť svojich volených zástupcov.

Zoznam použitej literatúry

1. DOMIN, Marek: Zákon o volebnej kampani - komentár. Bratislava : Wolters Kluwer, 2019. 228 s. ISBN978-80-571-0008-9.
2. DRGONEC, Ján: Ústava Slovenskej republiky. 2. vydanie. Bratislava : C. H. Beck, 2019. 1792s. ISBN: 978-80-89603-74-9.
3. DRGONEC, Ján: Ústavné právo hmotné. 1. vydanie. Bratislava: C. H. Beck, 2018. 528 s. ISBN 978-80-89603-57-2.
4. OROSZ, Ladislav – SVÁK, Ján a kol.: Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava : Wolters Kluwer SR s. r. o., 2021. 892 s. ISBN978-80-571-0381-3.
5. MAJERČÁK, T. a kol.: Sloboda prejavu a jej limity - IV. ústavné dni. Košice UPJŠ 2016. 228 s. ISBN 978-80-8152-392-2.

6. Marsden, C. T., Meyer, T., & Brown, I. (2020). *Platform values and democratic elections: How can the law regulate digital disinformation?* Computer Law & Security Review, 36, 105373. DOI: 10.1016/j.clsr.2019.105373.
7. Shattock, E. (2022). Free and Informed Elections? Disinformation and Democratic Elections under Article 3 of Protocol 1 of the ECHR. *Human Rights Law Review*, 22(4), ngaco23. DOI: 10.1093/hrlr/ngaco23.
8. Digital News Report, 2017 [online]. Dostupné na <<https://www.digitalnewsreport.org/survey/2017/> > [cit. 12.09.2025].
9. REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. Digital News Report 2023 [online]. Oxford: Reuters Institute, University of Oxford, 2023 [cit. 2025-11-06]. Dostupné na: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023>.
10. REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. Digital News Report 2024 [online]. Oxford: Reuters Institute, University of Oxford, 2024 [cit. 2025-11-06]. Dostupné na: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024>.
11. STATISTA. Main Gateway to Online News Worldwide from 2014 to 2024 [online]. Hamburg: Statista GmbH, 2024 [cit. 2025-11-06]. Dostupné na: <https://www.statista.com/chart/32452/gateways-to-online-news/>.
12. YUGOV. 3 Key Findings About News Consumption from the Digital News Report 2024 [online]. London: YouGov, 2024 [cit. 2025-11-06]. Dostupné na: <https://business.yougov.com/content/49776-3-key-findings-about-news-consumption-from-the-digital-news-report-2024>.

Kontaktné údaje

Mgr. Branislav Korec, LL.M.

korec17@uniba.sk

Katedra ústavného práva

Právnická fakulta Univerzity Komenského v Bratislave

ZODPOVEDNOSŤ ŠTÁTU ZA BEZPEČNOSŤ V KYBERNETICKOM PRIESTORE A LIMITY JEHO INTERVENČNO-REGULAČNEJ PRÁVOMOCI

THE STATE'S RESPONSIBILITY FOR SECURITY IN CYBERSPACE AND THE LIMITS OF ITS INTERVENTION AND REGULATORY AUTHORITY

Dávid Židek¹

Abstrakt: Príspevok analyzuje zodpovednosť štátu za bezpečnosť v kybernetickom priestore a limity jeho intervenčno-regulačnej právomoci. Cieľom je preskúmať, či a akým spôsobom možno kybernetický priestor považovať za objekt verejného záujmu, a aké právne nástroje má štát k dispozícii na jeho ochranu. Metodologicky sa príspevok opiera o právnu analýzu, ústavnoprávnu interpretáciu a komparatívne skúmanie regulačných prístupov. Príspevok identifikuje kybernetický priestor ako nový verejný statok, v ktorom sa realizujú základné ľudské práva a slobody, čím vzniká štátu povinnosť zabezpečiť jeho dostupnosť, neutralitu a bezpečnosť pre svojich občanov. Závety poukazujú na potrebu reflexívnej regulácie, ktorá zohľadňuje technologickú dynamiku a vyžaduje okrem spolupráce verejného a súkromného sektora aj flexibilnú a pohotovú, (nie nevyhnutne) právnu reflexiu. Príspevok upozorňuje na riziká digitálneho autoritarizmu a potrebu demokratickej kontroly zásahov do virtuálneho prostredia. Vedecký prínos spočíva v rozšírení teórie verejného záujmu o digitálny rozmer a v návrhoch na optimalizáciu právnych mechanizmov štátnej intervencie v kybernetickom priestore za účelom garancie digitálnych práv občanov v súčasnosti už subsumovateľných do rámca základných ľudských práv a slobôd.

Kľúčové slová: kybernetický priestor, zodpovednosť štátu, právomoc štátu, intervenčno-regulačné nástroje

Abstract: This paper examines the state's responsibility for cybersecurity and the limits of its interventionist-regulatory authority in the digital domain. The primary objective is to determine whether cyberspace can be classified as an object of public interest and to identify the legal instruments available to the

¹ Katedra ústavného práva, Právnickej fakulty Univerzity Komenského v Bratislave.

state for its protection. The methodology is based on legal analysis, constitutional interpretation, and comparative assessment of regulatory frameworks. The study conceptualizes cyberspace as a new public asset where fundamental rights and freedoms are exercised, thereby imposing obligations on the state to ensure its accessibility, neutrality, and security for its citizens. Key findings highlight the necessity of reflexive regulation that accommodates technological dynamism, fosters cooperation between public and private sectors and also flexible, responsive, (not necessarily) legal reflection. The paper addresses risks associated with digital authoritarianism and emphasizes the importance of democratic oversight in virtual interventions, particularly regarding freedom of expression, surveillance, and automated decision-making. The scientific contribution lies in expanding the theory of public interest to encompass digital environments; the practical relevance is reflected in recommendations for optimizing legal mechanisms of state intervention in cyberspace while preserving individual autonomy and aligning with the principles of the rule of law.

Key words: cyberspace, state responsibility, state authority, intervention-regulatory tools

Úvod

Plynutím času kybernetický priestor postupne transformuje svoj charakter vo vzťahu k objektívnej (fyzickej) realite z komplementárneho na substitutívny. Povedané inak - postupne sa usiluje o jej nahradenie. (Nie len) digitalizácia verejných služieb a elektronická komunikácia vytvorili nový rozmer ľudskej interakcie, ktorý presahuje tradične chápané hranice štátneho územia (priestoru) a to najmä (avšak nie výlučne) z pohľadu právneho.

Takýto vývoj je však prirodzene nasledovaný aj novými hrozbami v podobe kybernetických útokov, šírenia dezinformácií, narušovania súkromia ale aj manipulácie dátami ohrozujúcich nie len jednotlivcov, ale aj štát v jeho najširšom chápaní. Práve štát v pozícii garanta verejného poriadku a ochrancu základných ľudských práv a slobôd čelí výzve zabezpečiť bezpečnosť v kybernetickom priestore bez toho, aby prekročil limity svojej právomoci.

Možno virtuálny priestor považovať za objekt verejného záujmu? Má štát povinnosť zabezpečiť bezpečie vo virtuálnom priestore rovnako, ako tomu je v skutočnej – objektívnej fyzickej realite? V prípade, že áno, aké sú ústavné limity a spôsoby jeho intervencie vo virtuálnom prostredí?

Cieľom tohto článku je analyzovať ústavnoprávne aspekty zodpovednosti štátu za bezpečnosť v kybernetickom priestore, identifikovať právne limity jeho intervenčno-

regulačnej právomoci a posúdiť, do akej miery sú existujúce právne intervenčné mechanizmy schopné reagovať na dynamiku digitálneho (virtuálneho) prostredia. V príspevku sa autor zamýšľa aj nad právnymi dôsledkami konceptov akými sú digitálna ústava a vznik digitálnej územnej zvrchovanosti, pričom sa usiluje o nachádzanie rovnováhy medzi ochranou verejného záujmu a zachovaním individuálnych práv na rozmedzí digitálneho autoritarizmu a demokratickej kontroly.

Kybernetický priestor ako objekt verejného záujmu

Zachovávajúc tradičnú (konzervatívnu) štruktúru príspevku sa žiada pre účely ďalšej analýzy a možnosti zodpovedania otázky či je možné kybernetický priestor považovať za objekt verejného záujmu vymedziť tieto dva pojmy a to čo najširším možným spôsobom za účelom zamedzenia novej limitácie ich chápania v ďalších častiach príspevku.

Z akademického pohľadu možno uviesť, že kybernetický priestor predstavuje komplexný, dynamický a multidimenzionálny systém, ktorý zahŕňa digitálne infraštruktúry, softvérové prostredia, dátové toky, komunikačné kanály ale aj interakcie medzi používateľmi, technológiami a inštitúciami.²

Vo vzťahu k pojmu „kybernetický priestor“ sa pre účely tohto príspevku možno stotožniť s jeho legálnou definíciou podľa ustanovenia § 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, podľa ktorého sa kybernetickým priestorom rozumie globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktívované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi. Synonymom tohto pojmu môže byť v tomto zmysle aj pojem „digitálny“ alebo „virtuálny“ priestor.

Ak ide o definíciu pojmu „objekt verejného záujmu“, situácia je o niečo náročnejšia. Napriek tomu, že v ústavnoprávnom rámci nachádzame jeho definíciu napríklad v ústavnom zákone č. 357/2004 Z. z. o ochrane verejného záujmu, ide o veľmi limitované a individualizované vymedzenie výlučne pre účely tohto ústavného zákona. Nemožno tak odporovať ani vedeckému názoru, že tento pojem je právne neurčitým pojmom.³ Z akademického hľadiska pojem „verejný záujem“ možno definovať ako hodnotu resp. cieľ, ktorý presahuje individuálny prospech a slúži spoločnosti ako celku.⁴

² BREZULA, J.: Aspekty kybernetickej bezpečnosti na Slovensku a vo svete. Krízový manažment. Žilina: Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 2017, roč. 16, č. 2, s. 83–88.

³ Možno odkázať napríklad na: KONEČNÝ, S.: Verejný záujem: Príspevok k teórii a praxi verejnej politiky. In: Právny obzor, roč. 105, č. 2/2022 alebo TEKELI, J.: Verejný záujem ako právna kategória v ústavnom systéme Slovenskej republiky. In: Právny obzor, roč. 104, č. 4/2020, s. 289–305.

⁴ K uvedenému pozri napríklad: PÍRY, M.: Verejný záujem ako neurčitý právny pojem v správnom práve. In: Justičná revue, roč. 69, č. 11, s. 1205–1215.

Kybernetický priestor sa stal neoddeliteľnou súčasťou verejného záujmu, a to najmä v kontexte ochrany kritickej infraštruktúry, verejnej správy ale aj novovznikajúcich tzv. digitálnych práv občanov⁵. Podľa Správy o kybernetickej bezpečnosti v Slovenskej republike za rok 2024⁶, ktorú publikoval Národný bezpečnostný úrad, došlo k výraznému nárastu kybernetických incidentov, pričom štát musel aktívne zasahovať do digitálneho prostredia s cieľom ochrániť verejné inštitúcie a základné služby.⁷ Vzhľadom na čoraz zásadnejší význam pre fungovanie súčasnej spoločnosti sa stále častejšie objavuje potreba jeho vnímania ako objektu verejného záujmu reflektujúceho princípy právneho štátu, ochrany základných práv a slobôd ako aj zodpovednosti v jej najširšom chápaní.

Vedecký diskurz o kybernetickom priestore ako objekte verejného záujmu zároveň otvára otázky o jeho ontologickom statuse⁸ – či ide o priestor, ktorý je možné vlastniť, spravovať alebo regulovať analogicky k fyzickému svetu, alebo či si vyžaduje nové paradigmy správy a zodpovednosti. V tejto súvislosti sa objavujú koncepty ako digitálna suverenita⁹ či kybernetická diplomacia¹⁰, ktoré reflektujú potrebu medzinárodnej koordinácie a rešpektovania digitálnych práv v nadnárodnom kontexte.

Kybernetický priestor ako digitálne prostredie, v ktorom sa realizujú základné práva a slobody tak nadobúda charakter verejného statku¹¹, ktorého ochrana a správa je otázkou verejného záujmu. Štát v tomto prostredí zohráva kľúčovú úlohu pri

⁵ Možno odkázať napríklad na Európsku deklaráciu o digitálnych právach, pričom tieto zahŕňujú najmä právo na prístup k internetu, ochranu osobných údajov a súkromia, právo na digitálnu bezpečnosť, slobodu prejavu a informácií vo virtuálnom priestore, právo na digitálnu identitu ale aj prístup k digitálnym verejným službám. Bližšie pozri: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>.

⁶ Dostupné online: <https://www.nbu.gov.sk/sprava-o-kybernetickej-bezpecnosti-v-slovenskej-republike-v-roku-2024/>

⁷ Správa dostupná online: <https://www.nbu.gov.sk/data/att/3288.pdf>

K uvedenému tiež pozri: LOVEČEK, T.: Nové legislatívne bezpečnostné požiadavky na ochranu kritickej infraštruktúry. Bezpečnosť v praxi [online]. Bratislava: Fórum bezpečnostných profesionálov, 2025. Dostupné na internete: <https://www.bezpecnostvpraxi.sk/aktuality/nove-legislativne-bezpecnostne-poziadavky-na-ochranu-kritickej-infrastruktury-aktbvp.htm>

⁸ Pozri napríklad: KUČERA, T.: Ontologický status kybernetického priestoru: filozofické aspekty digitálnej reality. In: Filozofia. Bratislava: Ústav filozofie SAV, roč. 75, č. 3, 2020, s. 195–210.

⁹ Pozri: GERA, M., HUSOVEC, M., SZILVA, Š., ZABUŇKOVÁ, P.: Digitálna verejná správa a ľudské práva. Bratislava: European Information Society Institute, 2015.

¹⁰ K uvedenému napríklad: VALUCH, J. Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti. Bratislava: Wolters Kluwer SR, s.r.o., 2020. 160 s. alebo ANDRAŠKO, J., MESARČÍK, M., SOKOL, P.: Právo kybernetickej bezpečnosti. 1. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. 186 s.

¹¹ KASPERSKI, M.: Cybersecurity as a public good: The role of the state in securing cyberspace. Journal of Cyber Policy [online]. 2021, 6(2), 254–272.

definovaní pravidiel, zodpovednosti a mechanizmov ochrany základných ľudských práv a slobôd realizovaných v tomto priestore.

Ústavnoprávnou optikou možno povedať, že kybernetický priestor sa stáva miestom výkonu (realizácie) základných ľudských práv a slobôd, akými sú najmä sloboda prejavu, právo na informácie, ochrana súkromia, právo na bezpečnosť či ochrana osobných údajov. Tieto práva musia byť garantované nie len v reálnom – fyzickom priestore ale aj v tom digitálnom (virtuálnom). Právne normy musia reflektovať špecifiká kybernetického priestoru, ako je jeho decentralizovanosť, ale aj technická komplexnosť.

Kybernetický priestor ako objekt verejného záujmu si vyžaduje aj právnu ochranu jeho dostupnosti a neutrality. Princíp sieťovej neutrality¹², ktorý zakazuje diskrimináciu dátového prenosu zo strany poskytovateľov internetu, je taktiež kľúčový pre zabezpečenie rovného prístupu k informáciám a slobodnej súťaže. Právo musí zároveň chrániť kybernetický priestor pred monopolizáciou, komercializáciou a zneužitím dominantného postavenia digitálnych platforiem. Možno skonštatovať, že v digitálnej ére nemožno bezpečnosť chápať len ako ochranu fyzického územia. Virtuálny priestor sa stáva novým rozmerom štátnej suverenity, analogickým k pevnine, vzduchu a moru.

Osobitnú pozornosť si preto zasluhuje aj (už načrtnutá) otázka právnej zodpovednosti v kybernetickom priestore. Vzhľadom na anonymitu, automatizáciu a algoritmické rozhodovanie je identifikácia subjektov zodpovednosti často problematická. Právo musí preto vyvíjať nové koncepty, ako je zodpovednosť za softvérové chyby, algoritmickú diskrimináciu či škody spôsobené umelou inteligenciou¹³. Zároveň je potrebné posilniť právne mechanizmy ochrany jednotlivcov pred zneužitím ich digitálnej identity, sledovaním či manipuláciou.

Dostávame sa tak k zodpovedaniu otázok, či vzniká však štátu povinnosť (zodpovednosť) regulovať virtuálne prostredie, aké sú intervenčno-regulačné nástroje, ktorými to dokáže a či možno intervenčnú právomoc štátu odvodzovať od teórie spoločenskej zmluvy¹⁴.

Intervenčno-regulačné nástroje štátu

Z pohľadu ochrany verejného záujmu je nevyhnutné, aby štát práve prostredníctvom intervenčno-regulačných nástrojov reflektovaných v legislatíve zabezpečil ochranu

¹² Pozri napríklad: VAN SCHEWICK, B.: Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like. *Stanford Law Review*, 2013, roč. 67, č. 1, s. 1–166.

¹³ K zodpovednosti vo vzťahu k automatizácii a umelej inteligencii v mobilite pozri bližšie HODÁS, M., ŽIDEK, D.: Niektoré právne aspekty inteligentnej mobility. In: *Právo a bezpečnosť*, 01/2022, s. 7–27.

¹⁴ K uvedenému pozri napríklad: HOBBS, T.: *Leviathan, or the Matter, Forme and Power of a Common-Wealth Ecclesiasticall and Civil*. London : Andrew Crooke, 1651 alebo TURČAN, C.: *Úvod do teórií spoločenskej zmluvy*. Nitra : Univerzita Konštantína Filozofa v Nitre, 2022.

kybernetického priestoru pred hrozbami, ktoré môžu ohroziť verejný poriadok, národnú bezpečnosť či fungovanie ústavných inštitúcií.

Každý demokratický právny štát reguluje fungovanie a zabezpečuje smerovanie (vlastnej) spoločnosti prostredníctvom práva – právnych nástrojov. Medzi tieto možno v závislosti od ich charakteru zaradiť aj skupinu intervenčno-regulačných nástrojov štátu, ktoré v oblasti virtuálneho priestoru predstavujú komplexný systém právnych, technologických a inštitucionálnych mechanizmov, ktorých cieľom je zabezpečiť rovnováhu medzi ochranou verejného záujmu, garantovaním základných práv jednotlivca a udržiavaním funkčnosti samotného digitálneho priestoru. Štát sa tak stáva aktérom, ktorý musí reagovať na doposiaľ neznáme formy hrozieb v stále rozvíjajúcom sa novom – digitálnom prostredí.

Intervencia štátu v digitálnom priestore sa neobmedzuje len na represívne opatrenia, ale zahŕňa aj preventívne, korektívne a stimulačné nástroje, ktoré majú za cieľ formovať správanie (nie len) technologických subjektov.¹⁵ Pre teoretickú komplexnosť možno uviesť, že z hľadiska právnej teórie možno intervenčno-regulačné nástroje rozdeliť na normatívne, inštitucionálne a procedurálne¹⁶.

V kontexte digitálnej suverenity štátu¹⁷ sa čoraz viac presadzuje potreba tzv. reflexívnej regulácie¹⁸, založenej na flexibilnom prispôbovaní regulačných zásahov v oblasti technologického vývoja. Všeobecne tak možno uviesť, že v oblasti digitálnych technológií sú rigidné normatívne rámce neželané. Reflexívna regulácia však predpokladá úzku spoluprácu medzi verejným a súkromným sektorom, čo

¹⁵ DOBROVODSKÝ, R., HARGAŠOVÁ, L., HOLDOŠ, J. a kol.: *Národná koncepcia ochrany detí v digitálnom priestore* [online]. Bratislava: Ministerstvo práce, sociálnych vecí a rodiny SR, 2021. Dostupné na:

<https://nks.gov.sk/wp-content/uploads/2025/SM/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf>

¹⁶ WEINBERGER, O.: *Inštitucionalizmus: Nová teória konania, práva a demokracie*. Bratislava: Kalligram, 2010 alebo RANGL, J.: Povaha práva v teórii a praxi. *Právny obzor*, roč. 103, č. 4, 2020, s. 290–305.

¹⁷ K digitálnej suverenite v kontexte regulácie online platforiem pozri: BAYER, J., STARK, A.: Digital sovereignty and the regulation of online platforms in the EU. *Internet Policy Review* [online]. 2020, 9(4), 1–20.

¹⁸ K uvedenému pozri napríklad: TEUBNER, G.: Reflexive Law in the Context of Regulatory Reform. In: *Regulatory Reform and Reflexive Regulation: Beyond Command and Control*. Oxford: Oxford University Press, 2023 alebo ZÁBAVSKÁ, D.: Reflexívna regulácia v kontexte právneho rámca 3D biotlače. In: *Zborník príspevkov z konferencie Právo – technológie – spoločnosť 2024*. Bratislava: Právnická fakulta UK, 2024, s. 45–58.

predstavuje ďalšiu výzvu v oblasti regulácie digitálneho prostredia^{19,20}. Riziko nadmernej regulácie je rovnako závažné ako riziko jej absencie. Preto je potrebné, aby štátne zásahy boli koncipované na základe dôkazov, multidisciplinárnej expertízy a v súlade s princípmi právneho štátu. Intervenčno-regulačné nástroje štátu v oblasti virtuálneho priestoru tak predstavujú nielen technickú výzvu, ale aj bazálnu otázku demokratickej legitimacy, právnej kultúry a schopnosti spoločnosti udržať kontrolu nad digitálnym vývojom bez toho, aby stratila autonómiu jednotlivca.²¹

Nemožno tiež neotvoriť otázku legitimacy zásahov štátu do virtuálneho priestoru²², najmä v prípadoch, keď dochádza k obmedzovaniu slobody prejavu, sledovaniu digitálnych aktivít alebo automatizovanému rozhodovaniu bez ľudského zásahu. Preto je nevyhnutné, aby intervenčno-regulačné nástroje boli podrobené demokratickej kontrole, súdnemu preskúmaniu a etickej reflexii, ktorá zohľadňuje nielen právne, ale aj sociálne, kultúrne a technologické dimenzie digitálneho prostredia.

Za veľmi špecifický (cielený) nástroj umožňujúci intervenciu (a tým aj reguláciu) vo virtuálnom priestore²³ možno považovať najmä blokovanie „neželaného“ obsahu. Národná rada Slovenskej republiky v roku 2022 prijala novelizačný zákon²⁴, ktorý okrem iného novelizoval aj zákon o kybernetickej bezpečnosti²⁵ a priznal nové právomoci Národnému bezpečnostnému úradu Slovenskej republiky, ktoré tomuto úradu umožňovali rozhodovať o blokovaní škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky, zabezpečovať vykonanie tohto rozhodnutia a vykonávať takéto blokovanie. Za vyzdvihnutie stojí aj skutočnosť, že Národný bezpečnostný úrad rozhodoval o blokovaní ako aj spôsobom tohto blokovania *ex offio* ale aj na základe žiadosti iného štátneho orgánu. Taktiež možno dodať, že išlo

¹⁹ Jedným dychom je však potrebné dodať, že táto spolupráca sa v praxi často ukazuje ako neefektívna aj s ohľadom na rozdielne ciele subjektov pôsobiacich vo verejnom a súkromnom sektore. Kým elementárnym cieľom subjektov súkromného sektora je dosahovanie zisku a expanzie, cieľom subjektov verejného sektora je zabezpečovanie verejných statkov (v tomto smere najmä bezpečia vo virtuálnom priestore).

²⁰ K uvedenému pozri napríklad: CARR, M.: Public-private partnerships in national cyber-security strategies. International Affairs [online]. 2016, 92(1), 43–62.

²¹ Konečný, S.: Verejný záujem: Príspevok k teórii a praxi verejnej politiky. Právny obzor, 105(2), 97–112.

²² Vysoko aktuálnym sa stáva aj otázka tzv. digitálnej proporcionality, ktorá skúma primeranosť zásahov štátu voči cieľom, ktoré majú byť dosiahnuté.

²³ Pod tieto nástroje autor účelovo nezahrnul trestnoprávnu represiu štátu z dôvodu, že túto možno považovať za univerzálne (a teda aj vo virtuálnom priestore) aplikovateľný nástroj, ktorý nemá špecifický charakter. Príkladom možno uviesť trestné činy podľa § 370, § 360b Trestného zákona č. 300/2005 Z. z.

²⁴ Zákon č. 55/2022 Z. z. o niektorých opatreniach v súvislosti so situáciou na Ukrajine

²⁵ Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

o konanie administratívnoprávneho (správneho) charakteru, ktorého výsledkom bol individuálny správny akt.

Či možno v tomto prípade hovoriť o príliš širokej (ústavné poverenie prekračujúcej) diskrečnej právomoci štátneho orgánu alebo je možné považovať koncentráciu rozhodovacej právomoci o selektívnom obmedzení ústavnej slobody prejavu za žiadané (vzhľadom na absenciu meritórneho ústavného rozhodnutia) ponechávame na zvážení čitateľa.

Za ďalšie takéto nástroje možno označiť aj odoberanie licencií, vykonávanie inšpekcií a auditov, poskytovanie dotácií a grantov (slúžiacich na želanú moderáciu vývoja v určitých segmentoch digitálneho prostredia), udeľovanie daňových stimulov, vydávanie etických kódexov resp. odporúčaní a usmernení (ktoré však nemajú právne záväzný charakter).

Digitálny autoritarizmus vs. demokratická kontrola

V kontexte narastajúcej digitalizácie verejného života, spoločnosti, štátneho dohľadu sa čoraz častejšie objavuje napätie medzi ochranou základných práv a efektívnym výkonom verejnej moci.

Digitálny autoritarizmus²⁶, ako koncept²⁷, označuje využívanie digitálnych technológií štátom na účely kontroly, manipulácie a represie, pričom sa opiera o centralizované dátové štruktúry, masové sledovanie, cenzúru a selektívne potláčanie disentu. Tento fenomén sa neobmedzuje len na autokratické režimy, ale preniká aj do demokratických systémov prostredníctvom tzv. „soft surveillance“²⁸ mechanizmov, ktoré sú často legitimizované diskurzom bezpečnosti, efektivity alebo verejného záujmu.²⁹

Na druhej strane stojí legitimita demokratickej kontroly, ktorá predpokladá existenciu právneho štátu, a teda aj ochranu individuálnych práv a slobôd. V digitálnom prostredí sa demokratická kontrola realizuje prostredníctvom právnych noriem, inštitucionálnych mechanizmov a občianskeho dohľadu, ktoré majú za cieľ

²⁶ Pozri napríklad: FELDSTEIN, S.: Digital Authoritarianism: AI Surveillance and the Threat to Human Rights. *Journal of Democracy*, 2020, roč. 31, č. 1, s. 40–53 a tiež DEIBERT, R. J.: The road to digital unfreedom: The rise of the surveillance state. *Journal of Democracy* [online]. 2019, 30(1), 20–34.

²⁷ Digitálny autoritarizmus možno tiež vymedziť ako pojem označujúci využívanie digitálnych technológií autoritárskymi režimami na kontrolu, sledovanie, manipuláciu a obmedzovanie slobody prejavu, prístupu k informáciám či občianskych práv. Ide o fenomén, pri ktorom sa nástroje ako umelá inteligencia, biometrická identifikácia, cenzúra internetu, sledovanie sociálnych sietí či digitálna propaganda používajú na upevnenie moci štátu a potláčanie opozície.

²⁸ Typickým príkladom je tzv. dobrovoľné zdieľanie údajov (napríklad v podobe súhlasu s tzv. súbormi cookies), ale aj sociálne siete a ďalšie.

²⁹ GŁOWACKA, D. et al.: Digital technologies as a means of repression and social control. [online]. Brussels: European Parliament, Policy Department for External Relations, 2021.

obmedziť moc technologických aktérov (nie len štátu ale aj súkromných (zväčša nadnárodných) korporácií), a tým zabezpečiť, aby digitálne nástroje slúžili verejnému dobru (verejnému záujmu). Kľúčovým problémom je však disproporcía poznania a moci: zatiaľ čo štát a technologické platformy disponujú sofistikovanými nástrojmi na zber, analýzu a využívanie dát, občania a demokratické inštitúcie často zaostávajú v schopnosti tieto procesy kontrolovať. Konflikt medzi digitálnym autoritarizmom a demokratickou kontrolou sa tak prejavuje najmä v otázkach legitimacy zásahov štátu do súkromia obyvateľov.

Právne aspekty zásahu štátu do súkromia v kybernetickom priestore predstavujú komplexnú oblasť, kde sa stretáva potreba ochrany verejného záujmu s požiadavkou rešpektovania základných práv. Slovenský právny rámec poskytuje relatívne robustnú ochranu, avšak jeho aplikácia v praxi si vyžaduje dôsledný dohľad, transparentnosť a neustále aktualizovanie s ohľadom na technologický vývoj.

Vysoko aktuálnym sa stáva aj otázka tzv. digitálnej ústavy – teda súboru základných princípov, ktoré by mali upravovať vzťahy medzi jednotlivcom, štátom v kontexte technológií práve s dôrazom na prevenciu toho, aby sa digitálne nástroje, pôvodne určené na zlepšenie kvality verejného života stali nástrojom represie, exklúzie a normalizácie autoritárskych praktík. Aj z tohto dôvodu je preto nevyhnutné, aby demokratické spoločnosti neustále revidovali svoje regulačné rámce, posilňovali digitálnu gramotnosť obyvateľstva a budovali inštitúcie schopné čeliť výzvam digitálnej moci s rovnakou dôslednosťou, akou chránia základné (ústavné) princípy právneho štátu.

Súčasný výzvy a zahraničný prístup

Pre zdôraznenie aktuálnosti analyzovanej témy sa javí vhodným uviesť niekoľko praktických prípadov, v ktorých došlo k potvrdeniu nevyhnutnosti zabezpečovania bezpečnosti v rámci digitálneho prostredia štátom.

Jeden z nich sa stal v roku 2025, kedy sa Slovenská republika stala terčom koordinovaného kybernetického útoku na systém katastra nehnuteľností, čo vyvolalo diskusiu o hraniciach štátnej intervencie. Slovenská republika reagovala aktiváciou núdzových opatrení vrátane dočasného obmedzenia prístupu k niektorým digitálnym službám. Vzhľadom na skutočnosť, že (vybrané) zápisy v katastri nehnuteľností majú konštitutívny charakter (zakladajúcich vznik, zmenu alebo zánik práv a povinností), išlo o mimoriadne závažnú situáciu. Tento kybernetický (tzv. ransomvérový³⁰) útok je v súčasnosti považovaný za doposiaľ najväčší v celej histórii Slovenskej republiky. Dôsledkom tohto útoku bola (prinajmenšom) paralýza elektronických služieb katastra z čoho vyplynula nemožnosť podávania návrhov na

³⁰ Ide o typ škodlivého softvéru, ktorý zašifruje dáta na zariadení a následne od ich majiteľa požaduje výkupné za ich odblokovanie.

zmeny v listoch vlastníctva. Slovenská republika zareagovala zvolaním bezpečnostnej rady, uzatvorením služieb katastra a vydaním nariadenia o nezapínaní technických zariadení prepojených na kataster nehnuteľností. Nasledovalo vyšetrovanie Úradu boja proti organizovanej kriminalite v spolupráci s Národným centrom kybernetickej bezpečnosti SK-CERT ale aj etických heckerov. Ukázalo sa, že Slovenská republika nedisponuje centrálnymi zálohami poškodených údajov a začala sa rekonštrukcia údajov z fyzickej (tzv. papierovej) formy listov vlastníctva. Výsledky vyšetrovania ukázali, že stopa vedie do zahraničia, pričom s vysokou pravdepodobnosťou išlo o organizovanú kybernetickú kriminálnu skupinu.

Za ďalší mimoriadne znepokojujúci útok vo virtuálnom prostredí možno označiť kybernetické hrozby cielené na zdravotnícke zariadenia. Podľa dostupných štatistických údajov došlo v roku 2024 k nárastu kybernetických incidentov smerujúcich na zdravotnícke zariadenia o 135 % v porovnaní s predošlým obdobím³¹. Tieto útoky okrem iného zahŕňali aj tzv. phishingové kampane, ktoré sa snažili získať citlivé údaje pacientov a narušiť chod nemocníc.

Konkrétne možno poukázať na incident nemocnice v Žiline, ktorý sa stal v roku 2024, kedy bol zaznamenaný pokus o prienik do systému elektronických zdravotných záznamov. Tento útok bol však včas odhalený, vďaka čomu nedošlo k poškodeniu alebo strate dát. Situácia však spôsobila dočasné obmedzenie niektorých digitálnych služieb a tým aj k obmedzeniu poskytovania zdravotnej starostlivosti.

Vyššie uvedené situácie predstavujú iba zlomok hrozieb, ktoré predstavujú praktické výzvy pre štát vo virtuálnom priestore pričom možno spoľahlivo tvrdiť, že iba poukazujú na potrebu kreácie jasného ústavného rámca pre zásahy do tzv. digitálnych práv občanov (nie len) v krízových situáciách.

Vo vzťahu k zahraničnému prístupu k riešenej problematike možno uviesť, že regulácia kybernetického priestoru a ochrana verejného záujmu v digitálnom prostredí sa v jednotlivých štátoch líši v závislosti od ústavného systému, technologickej vyspelosti, ale aj politickej kultúry.³²

V rámci komparatívnej analýzy možno identifikovať v zásade tri základné modely: centralizovaný (autoritatívny) prístup, decentralizovaný (demokratický) prístup a kombinované (hybridné formy) regulácie.³³

Z hľadiska invazívnosti štátu do „digitálnych práv občanov“ možno odkázať na Čínsku ľudovú republiku, ktorá udržiava kybernetický priestor pod prísnu štátnu kontrolou, pričom koncept tzv. „kybernetickej suverenity“ legitimizuje zásahy štátu do

³¹ K uvedenému pozri: [Kybernetické útoky na Slovensku rastú: Rekordný nárast incidentov v štáte aj zdravotníctve | oPeniazoch.sk](#)

³² K uvedenému pozri analýzu: SLOVAK BUSINESS AGENCY. 2025. *Regulácia v oblasti kybernetickej bezpečnosti v EÚ a SR*. Bratislava: Slovak Business Agency.

³³ Pozri bližšie: DEIBERT, R.: 2013. *Distributed Security as Cyber Strategy: Outlining a Novel Approach to Cyber Security Governance*. In: *Strategic Studies Quarterly*, vol. 7, no. 1, pp. 21–35.

digitálneho prostredia vrátane cenzúry, sledovania a obmedzovania prístupu k informáciám. Tento model je charakteristický vysokou mierou tzv. vertikálnej koncentrácie rozhodovacej právomoci.³⁴

Členské štáty Európskej únie presadzujú regulačný rámec založený na ochrane základných práv, transparentnosti a participatívnom rozhodovaní. Príkladom je legislatíva v oblasti digitálnych služieb (Digital Services Act³⁵) a digitálnych trhov (Digital Markets Act³⁶), ktoré zavádzajú mechanizmy demokratickej kontroly nad digitálnymi platformami, čím zabezpečujú bezpečnosť používateľov v digitálnom priestore.³⁷

Nemožno nespomenúť ani tzv. pluralitný prístup, ktorý je uplatňovaný v Spojených štátoch amerických, pričom pre tento sú charakteristické fragmentované štátne zásahy. Uvedené je spôsobené absenciou jednotného federálneho orgánu pre komplexnú reguláciu digitálneho prostredia, dominanciou technologických korporácií ale aj tendenciou Spojených štátov amerických k reaktívnosti (pomerné často sa vyskytujúcich) kybernetických bezpečnostných incidentov.³⁸

Aj táto stručná komparácia naznačuje, že slovenský model sa nachádza v štádiu skorého formovania, pričom čelí prirodzeným výzvam spojeným s definovaním rozsahu štátnej intervencie, zabezpečením demokratickej legitimacy zásahov a ochranou (nie len) digitálnych práv občanov.

Záver

Konkluzívne možno skonštatovať, že moderné hrozby si vyžadujú moderné spôsoby ich riešenia a presne tak, ako sa tieto hrozby vyvíjajú v čase, je nevyhnutné, aby sa vyvíjala aj (ústavno)právna reflexia na ne.

Ak chce štát naďalej zabezpečovať svoju elementárnu funkciu (vyplývajúcu z teórie spoločenskej zmluvy³⁹), ktorou je garancia ochrany širokej škály ústavných základných práv a slobôd vlastných občanov, musí mať v prípade potreby za týmto

³⁴ Bližšie pozri: HUNG, H. T.: Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. *Journal of Computational Social Science*, 2025, vol. 8, article no. 24.

³⁵ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu digitálnych služieb a o zmene smernice 2000/31/ES (Akt o digitálnych službách).

³⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 z 14. septembra 2022 o súťaživých a spravodlivých trhoch v digitálnom sektore a o zmene smerníc (Akt o digitálnych trhoch).

³⁷ Pozri bližšie: CAUFFMAN, C., GOANTA, C.: A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 2021, vol. 12, no. 4, pp. 758–774.

³⁸ NEWMAN, A., FARRELL, H.: Weaponized Interdependence: How Global Economic Networks Shape State Coercion. In: *International Security*, 2022, vol. 44, no. 1, pp. 42–79.

³⁹ Teóriou spoločenskej zmluvy chápeme elementárne teoretickoprávne východisko „dobrovoľnej dohody medzi občanmi a štátom“, v ktorej sa občania zhodli na odovzdaní moci o rozhodovaní zásadných otázkach chodu štátu svojim zástupcom – reprezentantom a teda štátnej moci ako takej.

účelom k dispozícii rázne a dostatočne efektívne (právne) nástroje efektivitou prispôsobené virtuálnemu prostrediu.

Štát je povinný nielen nezasahovať do základných práv, ale aj aktívne zabezpečovať ich ochranu. V kontexte virtuálneho priestoru sa tento pozitívny záväzok premieňa do povinnosti štátu vytvárať efektívne právne, technické a organizačné mechanizmy na ochranu pred kybernetickými hrozbami, ktoré môžu ohroziť súkromie, slobodu prejavu či integritu jednotlivca. Na strane druhej, štát by mal byť považovaný za digitálne zvrchovaný subjekt, ktorý má nielen právo, ale aj povinnosť regulovať, chrániť a spravovať „digitálne územie“ – teda dátové toky, infraštruktúru, kybernetické identity a algoritmické prostredie, ktoré ovplyvňuje jeho obyvateľov. Práve tento koncept by mohol viesť k novému typu digitálneho občianstva, kde štát garantuje kybernetické práva a bezpečnosť ako súčasť ústavného rámca. Transformáciou štátu na „kybernetického garanta“ by tak vznikol hybridný model verejno-súkromnej bezpečnostnej zodpovednosti. Tento model by mohol byť zakotvený napríklad v podobe digitálneho bezpečnostného konzorcia, ktoré by malo právne záväzné povinnosti voči občanom, podobne ako verejnoprávne inštitúcie. Po načrtnutí zodpovednosti štátu a jeho postavenia v stále sa vyvíjajúcom virtuálnom prostredí možno predkladaný príspevok epilogicky zakončiť výstižným (a pravdivým) výrokom, podľa ktorého *má moc Janusovskú podobu, je utlačovateľom i integrátorom zároveň*.⁴⁰

Zoznam použitej literatúry

1. ANDRAŠKO, Jozef, MESARČÍK, Matúš, SOKOL, Pavol: *Právo kybernetickej bezpečnosti*. 1. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. 186 s. ISBN 978-80-7160-632-1. Dostupné online: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/E-KNIHY/Andrasko_Mesarcik_Sokol_-_Pravo_kybernetickej_bezpecnosti_ucebnica.pdf.
2. BAYER, Judith, STARK, Alexander: Digital sovereignty and the regulation of online platforms in the EU. Internet Policy Review [online]. 2020, 9(4), 1–20. ISSN 2197-6775. Dostupné z: <https://policyreview.info/articles/analysis/digital-sovereignty-and-regulation-online-platforms-eu>.
3. BREZULA, Ján: Aspekty kybernetickej bezpečnosti na Slovensku a vo svete. Krízový manažment. Žilina: Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, 2017, roč. 16, č. 2, s. 83–88. ISSN 1336-0019.

⁴⁰ HOLLÄNDER, P.: Základy všeobecné štátovedy, Plzeň: Aleš Čeněk, 2009, s. 62, citované podľa: HODÁS, M.: Historický vývoj ľudských práv a ústavného štátu (a niektoré súčasné výzvy), Bratislava, História ľudských práv, o. z., 2006, s. 283.

4. CARR, Madeline: Public–private partnerships in national cyber-security strategies. *International Affairs* [online]. 2016, 92(1), 43–62. ISSN 0020-5850. Dostupné online: <https://academic.oup.com/ia/article/92/1/43/2326750>.
5. CAUFFMAN, Caroline, GOANTA, Catalina: A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 2021, vol. 12, no. 4, pp. 758–774. ISSN 1867-299X.
6. DEIBERT, Ronald: The road to digital unfreedom: The rise of the surveillance state. *Journal of Democracy* [online]. 2019, 30(1), 20–34. ISSN 1045-5736. Dostupné online: <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom/>.
7. DEIBERT, Ronald: *Distributed Security as Cyber Strategy: Outlining a Novel Approach to Cyber Security Governance*. In: *Strategic Studies Quarterly*, 2013, vol. 7, no. 1, pp. 21–35. ISSN 1936-1815. Dostupné online: <https://www.airuniversity.af.edu/SSQ/>.
8. DOBROVODSKÝ, Róbert, HARGAŠOVÁ, Lucia, HOLDOŠ, Juraj a kol.: *Národná koncepcia ochrany detí v digitálnom priestore* [online]. Bratislava: Ministerstvo práce, sociálnych vecí a rodiny SR, 2021. Dostupné na: <https://nks.gov.sk/wp-content/uploads/2025/SM/narodna-koncepcia-ochrany-deti-v-digitálnom-priestore-1.pdf>.
9. FELDSTEIN, Steven: Digital Authoritarianism: AI Surveillance and the Threat to Human Rights. *Journal of Democracy*, 2020, roč. 31, č. 1, s. 40–53. ISSN 1045-5736.
10. GERA, Matej, HUSOVEC, Martin, SZILVA, Štefan, ZABUŽKOVÁ, Petra: *Digitálna verejná správa a ľudské práva*. Bratislava: European Information Society Institute, 2015. ISBN 978-80-971307-3-2 (tlač), ISBN 978-80-971307-4-9 (PDF). Dostupné online: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/PIKT1/D_VSLP_final.pdf.
11. GŁOWACKA, Dorota et al.: Digital technologies as a means of repression and social control. [online]. Brussels: European Parliament, Policy Department for External Relations, 2021. Dostupné online: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_S_TU\(2021\)653636_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_S_TU(2021)653636_EN.pdf).
12. HUNG, Ho Ting: Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. *Journal of Computational Social Science*, 2025, vol. 8, article no. 24. ISSN 2432-2725. DOI: 10.1007/s42001-024-00346-8

13. HOBBS, Thomas: *Leviathan, or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil*. London : Andrew Crooke, 1651. ISBN 978-1-4209-2985-11.
14. HODÁS, Milan: *Historický vývoj ľudských práv a ústavného štátu (a niektoré súčasné výzvy)*, Bratislava, *História ľudských práv*, o. z., 2006, 429 s.
15. HODÁS, Milan, ŽIDEK, Dávid: Niektoré právne aspekty inteligentnej mobility. In: *Právo a bezpečnosť*, 01/2022, AMBIS vysoká škola, a. s. s. 7-27. Dostupné online: <https://5322ff71c9.clvaw-cdnwnd.com/5e1f67eaeafa2406e3efeefd75ef8b58/200000067-1a0b01a0b2/PaB%201-2022-0.pdf?ph=5322ff71c9>.
16. HOLLÄNDER, Pavel: *Základy všeobecné státovédy*, Plzeň: Aleš Čeněk, 2009, 368 s.
17. KASPERSKI, Maciej: Cybersecurity as a public good: The role of the state in securing cyberspace. *Journal of Cyber Policy* [online]. 2021, 6(2), 254–272. ISSN 2373-8871. Dostupné online: <https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1934235>.
18. KONEČNÝ, Stanislav: Verejný záujem: Príspevok k teórii a praxi verejnej politiky. *Právny obzor*, 105(2), 97–112. ISSN 0032-6984.
19. KUČERA, Tomáš: Ontologický status kybernetického priestoru: filozofické aspekty digitálnej reality. In: *Filozofia*. Bratislava: Ústav filozofie SAV, roč. 75, č. 3, 2020, s. 195–210. ISSN 0046-385X.
20. LOVEČEK, Tomáš: Nové legislatívne bezpečnostné požiadavky na ochranu kritickej infraštruktúry. *Bezpečnosť v praxi* [online]. Bratislava: Fórum bezpečnostných profesionálov, 2025. Dostupné na internete: <https://www.bezpecnostvpraxi.sk/aktuality/nove-legislativne-bezpecnostne-poziadavky-na-ochranu-kritickej-infrastruktury-aktbvp.htm>.
21. NEWMAN, Abraham, FARRELL, Henry: Weaponized Interdependence: How Global Economic Networks Shape State Coercion. In: *International Security*, 2022, vol. 44, no. 1, pp. 42–79. ISSN 0162-2889. DOI: 10.1162/isec_a_00351
22. PÍRY, Martin: Verejný záujem ako neurčitý právny pojem v správnom práve. In: *Justičná revue*, roč. 69, č. 11, s. 1205-1215.
23. RANGL, Jakub: Povaha práva v teórii a praxi. *Právny obzor*, roč. 103, č. 4, 2020, s. 290–305.
24. SLOVAK BUSINESS AGENCY. 2025. *Regulácia v oblasti kybernetickej bezpečnosti v EÚ a SR*. Bratislava: Slovak Business Agency. ISBN 978-80-89186-XX-X.
25. TEKELI, Jozef: Verejný záujem ako právna kategória v ústavnom systéme Slovenskej republiky. In: *Právny obzor*, roč. 104, č. 4/2020, s. 289-305.
26. TEUBNER, Gunther: Reflexive Law in the Context of Regulatory Reform. In: *Regulatory Reform and Reflexive Regulation: Beyond Command and Control*. Oxford: Oxford University Press, 2023.

27. TURČAN, Ciprian: Úvod do teórií spoločenskej zmluvy. Nitra : Univerzita Konštantína Filozofa v Nitre, 2022. ISBN 978-80-558-1854-2.
28. VALUCH, Jozef: *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava: Wolters Kluwer SR, s.r.o., 2020. 160 s. ISBN 978-80-571-0154-3. Dostupné online: <https://obchod.wolterskluwer.sk/sk/kyberneticke-hrozby-v-kontexte-medzinarodneho-prava-a-medzinarodnej-bezpecnosti.p4519.html>.
29. VAN SCHEWICK, Barbara: Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like. *Stanford Law Review*, 2013, roč. 67, č. 1, s. 1–166. ISSN 0038-9765.
30. WEINBERGER, Ota: *Inštitucionalizmus: Nová teória konania, práva a demokracie*. Bratislava: Kalligram, 2010. ISBN 978-80-8101-361-4
31. ZÁBAVSKÁ, Dominika: Reflexívna regulácia v kontexte právneho rámca 3D biotlače. In: *Zborník príspevkov z konferencie Právo – technológie – spoločnosť 2024*. Bratislava: Právnická fakulta UK, 2024, s. 45–58. ISBN 978-80-7160-123-4. Dostupné online: https://dspace.uniba.sk/bitstream/handle/123456789/225/BPF_2024_pdv.pdf?sequence=1.

Kontaktné údaje

Mgr. Dávid Židek
zidek14@uniba.sk
Katedra ústavného práva
Univerzita Komenského v Bratislave
Právnická fakulta

UMELÁ INTELIGENCIA A ĽUDSKÉ PRÁVA. JE EURÓPA LEGISLATÍVNE PRIPRAVENÁ NA TECHNOLOGICKÚ REVOLÚCIU?

ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS. IS EUROPE LEGISLATIVELY PREPARED FOR THE TECHNOLOGICAL REVOLUTION?

Martin Búran¹

Abstrakt: Príspevok je venovaný možnému vplyvu umelej inteligencie na oblasť ochrany ľudských práv, s osobitným dôrazom na európsky právny kontext. V prvých častiach príspevku autor na praktických príkladoch poukazuje na riziká, ktoré vnáša umelá inteligencia do oblasti práva na súkromie, práva na život a do požiadavky zákazu diskriminácie. Tento vplyv je hodnotený ako taký, ktorý predstavuje významné riziko a ktorému je nutné ex ante predchádzať. V nadväznosti na uvedené autor kriticky rozoberá kľúčové ľudskoprávne aspekty nadnárodnej európskej legislatívy, ktorá má ľudské práva pred umelou inteligenciou chrániť a načrtnutým vplyvom predchádzať – a to tak na úrovni Európskej únie (tzv. akt o umelej inteligencii), ako i na úrovni Rady Európy (tzv. Rámcový dohovor o umelej inteligencii). Primárne sa teda autor zaoberá otázkou, či predmetná legislatíva na úrovni Európskej únie a Rady Európy dokáže ľudské práva efektívne ochrániť. Bez ohľadu na tempo digitálneho pokroku sú totiž tieto organizácie (a ich členské štáty) za ochranu ľudských práv zodpovedné.

Kľúčové slová: umelá inteligencia; ľudské práva; Európska únia; Rada Európy

Abstract: This paper is devoted to the possible impact of artificial intelligence on the protection of human rights, with a particular focus on the European legal context. In the first parts of the article, the author uses practical examples to highlight the risks that artificial intelligence poses to the right to privacy, the right to life, and the requirement to prohibit discrimination. This impact is assessed as posing a significant risk and must be prevented ex ante. Following on from the above, the author critically examines the key human rights aspects of supranational European legislation, which is intended to protect human

¹ Katedra ústavného práva, Právnická fakulta Univerzity Komenského v Bratislave.

rights from artificial intelligence and prevent the outlined impact – both at the level of the European Union (the so-called EU Artificial Intelligence Act) and at the level of the Council of Europe (the Framework Convention on Artificial Intelligence). The author primarily addresses the question of whether the legislation in question at the level of the European Union and the Council of Europe can effectively protect human rights. Regardless of the pace of digital progress, these organizations (and their member states) are responsible for protecting human rights.

Key words: artificial intelligence; human rights; European Union; Council of Europe

Úvod

Obvykle platí pri zavádzaní nejakých nových technológií, systémov etc. fráza, že sa (technológie) „pomaly stávajú súčasťou našich životov“. Pri umelej inteligencii (ďalej aj „AI“) je to inak. Nie však tým, že by sa AI súčasťou našich životov nestávala. Čo neplatí je tvrdenie, že je jej integrácia „pomalá“. V bežnom živote sa rozmach AI viditeľne prejavuje v jej veľkých jazykových modeloch (napr. ChatGPT), založených na báze neurónových sietí,² schopných strojovo sa „učiť“ kopírovaním fungovania mozgu. Jazykové modely sú okrem ich globálnej dostupnosti pre masu čoraz častejšie zapájané do rozhodovacích procesov, či už na úrovni súkromnej, ale aj verejnej sféry. Existujúce druhy AI nie sú jazykovým modelom vyčerpané, na úvodnú ilustráciu to však postačuje.

Efekt umelej inteligencie na ľudskú spoločnosť je dvojsečný. Na jednej strane totiž AI uľahčuje spoločenské fungovanie (napríklad postupným nahrádzaním jednoduchej administratívy, ktorú doposiaľ vykonávali ľudské bytosti), na druhej strane je pre spoločnosť ohrozením. Ohrozením nielen jej „tradičného“ nastavenia,³ ale aj ohrozením ochrany základných práv (ekonomické a sociologické aspekty na účely tohto príspevku vynímame). (Aj) z tohto dôvodu môžeme v súčasnosti sledovať počiatky⁴ komplexnej právnej regulácie zo strany nadnárodných inštitúcií, ktoré sú pre slovenský právny priestor relevantné.⁵

To, že umelá inteligencia do tejto oblasti s určitosťou zasiahne (zasahuje), si uvedomuje aj Rada Európy. *Steering Committee for Human Rights (CDDH)*, resp.

² SARRION, E.: How Does ChatGPT Work?. In: Exploring the Power of ChatGPT. Berkeley, CA: Apress, 2023, s. 9–16.

³ Úvodzovky používame na zdôraznenie toho, že hoc sa nám môže javiť súčasný spôsob spoločenského fungovania ako tradičný, nie vo všetkých ohľadoch to platí (napr. vývoj po roku 1918/1945/1989 dobové fungovanie spoločnosti značne zmenil).

⁴ Počiatky z dôvodu, že regulácia AI bude z povahy veci veľmi dynamická.

⁵ Menovite Európska únia, Rada Európy.

Riadiaci výbor pre ľudské práva zriadil tzv. Pracovnú skupinu pre ľudské práva a umelú inteligenciu (CDDH-IA), ktorej cieľom je komplexne spracovať ľudskoprávnu problematiku do príručky, ktorá bude slúžiť okrem iného aj pre Európsky súd pre ľudské práva (ďalej aj „ESLP“).

Autor v tomto príspevku primárne skúma riziká, ktoré môže umelá inteligencia v rámci troch vybraných základných práv priniesť. Na tento predpoklad sa v poslednej podkapitole usiluje súhrnne adaptovať aktuálne jestvujúce regulačné rámce v úvahe, či a v akej miere je možné negatívne efekty AI na základné práva odvrátiť. To všetko s dôrazom na zodpovedanie kľúčovej otázky, či je Európa – v rozsahu Európskej únie ako regulačného lídra⁶ a Rady Európy – voči týmto rizikám imúnna, alebo ak nie, či je istú obranyschopnosť po ľudskoprávnej stránke možné v dohľadnej dobe predpokladať. Na tomto mieste je ešte potrebné uviesť niekoľko poznámok k metodike tohto príspevku.

1. Pri klasifikácii vybraných základných práv, z hľadiska pozície v právnom akte, vychádza autor z Európskeho dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „EDLP“).

2. Výber základných práv, ktoré sú v texte rozvíjané, vychádza (okrem vlastných úvah) z dokumentov už zmienenej pracovnej skupiny Rady Európy a z inšpirácie poznatkami zahraničných akademikov.

3. Vplyv AI na ľudské práva nie je v tejto chvíli možné demonštrovať formou skutočných prípadov, ktoré boli súdmi rozhodnuté. Dôsledná analýza caselaw (ani ESLP,⁷ ani SDEÚ, ani národných súdov⁸) spojených s AI nie je v čase písania tohto príspevku možná – s výnimkou pár rozhodnutí⁹ sa súdy zatiaľ AI priamo nevenujú.¹⁰ Sú však autori, ktorí sa o analýzu rozhodovacej činnosti smerom k AI na základe obdobných princípov usilujú i tak. Pre úplnosť na tento prístup odkazujeme,¹¹ no

⁶ Obdobný pojem používajú aj autori MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 65.

⁷ Pozri napr. s. 9 z Judicial Seminar 2025 – Background Document: Protecting human rights in a world of Artificial Intelligence, algorithms and big data, dostupné tu: <https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng>. Ako je viditeľné, ESLP zatiaľ neprejednával prípady, ktoré by uvedenú problematiku rozoberali.

⁸ Odkazujeme na dotazník obsahujúci dáta zozbierané zo strany Rady Európy od jej členských štátov, dostupný tu: <https://rm.coe.int/steering-committee-for-human-rights-drafting-group-on-human-rights-and/488010e7c5>.

⁹ Pozri napr. tu: <https://www.havelpartners.blog/prvni-rozsudek-o-ai-generovanych-dilech-v-cr-kde-konci-mechanicke-uzivani-a-zacina-lidska-kreativita>.

¹⁰ Čo však neznamená, že počet nebude narastať. Napr. tu: <https://www.stephensonharwood.com/insights/cjeu-to-rule-on-ai-and-copyright-in-a-landmark-case-against-google>.

¹¹ Napr. SZAPPANYOS, Melinda: Artificial Intelligence: Is the European Court of Human Rights Prepared?. In: Acta Humana – Human Rights Publication, Roč. 11, č. 1 (2023),. osobitne s. 96-104.

nepovažujeme ho za úplne správny. Nejde totiž o nič, čo by predtým už množstvom autorov rozoberané nebolo. Analogická aplikácia tradičných princípov na nové situácie je síce pevne zakorenená, umelá inteligencia však z povahy veci vylučuje uplatnenie viacerých zaužívaných schém.

AI ako kybernetická a ľudskoprávna hrozba

Národné centrum kybernetickej bezpečnosti Spojeného kráľovstva (*National Cyber Security Centre*) vydalo v máji 2025 *Report* ohľadom vplyvu umelej inteligencie na kybernetické hrozby. Spojené kráľovstvo považuje za takmer isté (pravdepodobnosť nad 95 %), že AI bude do roku 2027 zapojená do kybernetických útokov na kritickú infraštruktúru a s rovnakou mierou pravdepodobnosti upozorňuje, že prípadná implementácia AI do nosných sieťových systémov Spojeného kráľovstva výrazne zvyšuje priestor, ktorý môže byť na útoky využitý. Nástroje AI (aj tie, ktoré mali systémové zraniteľnosti odhaľovať) na páchanie kybernetickej kriminality zneužívajú útočníci už dnes. Hoc plne využívať AI potenciál na kybernetické útoky dokážu v súčasnosti len „*vysoko schopní štátni aktéri s prístupom k potrebným investíciám, kvalitným údajom a odborným znalostiam*“¹², na útoky bývajú (zo strany menej technologicky vyspelých útočníkov) zneužitie aj open-source nástroje.¹³ Obdobne upozorňujú na zneužívanie AI na páchanie kybernetickej kriminality aj iní autori.¹⁴ Aj tu sa teda ukazuje dvojsečnosť pozície AI. Táto správa sa primárne týka krajiny, ktorá ju vydala, bolo by však iluzórne myslieť si, že dáta ostatných krajín by sa líšili, keby boli spracované a verejne prístupné.

Kybernetickej bezpečnosti sa ale tento príspevok nevenuje, primárne totiž nejde o právnu oblasť. Uvedené autor použil len na ilustráciu jedného z pohľadov na umelú inteligenciu, ktorý v tomto príspevku ponúka. A to vnímania AI nielen ako príležitosti dosiahnuť nepoznaný pokrok, ktorej sa treba okamžite chopiť, ale aj ako hrozby. Hrozby nielen kybernetickej, ale aj ľudskoprávnej. Na ňu nemožno zabúdať. Technologický pokrok bez dôslednej ochrany ľudských práv by totiž nebol skutočným pokrokom. To, že riziko smerom k ľudským právam je veľké, rozoberáme na riadkoch nižšie.

¹² Pozn.: voľný preklad autora.

¹³ Bližšie NCSC: Impact of AI on the cyber threat – now to 2027 (Národné centrum kyberbezpečnosti Spojeného kráľovstva), dostupné tu: <https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027>.

¹⁴ MESARČÍK – GYURÁSZ, ref. 6, s. 184-185.

Nediskriminácia a rovnosť

Zákaz diskriminácie¹⁵ a rovnosť môžu byť (a aj bývajú) systémami umelej inteligencie narúšané. Rada Európy upriamuje pozornosť na riziko spojené so stereotypmi.¹⁶ Keďže systémy AI pracujú (zjednodušene) na báze kopírovania správania ľudského mozgu a spracúvajú enormné množstvo dát, stereotypom (ktorých je plný internet) sa nevyhnú. Ako príklad je možné uviesť akúkoľvek etnickú menšinu, ktorej existencia nie je dominantnou časťou nejakého národa dobre prijatá. Človek z takejto menšiny sa hlási do zamestnania, pošle životopis. V životopise je uvedená fotka a adresa. Spoločnosť, ktorá výberové konanie organizuje, na spracúvanie životopisov použije systém umelej inteligencie, ktorý má zostaviť poradovník uchádzačov. Všetci prihlásení uchádzači majú približne rovnaký vek, dosiahnutú úroveň vzdelania, aj vyplnené osobnostné predpoklady. Uchádzač X má však adresu zhodnú s oblasťou, kde je podľa verejne dostupných registrov značný výskyt pre časť populácie problematickej etnickej menšiny, farba pleti po analýze fotografie ukáže pravdepodobnú zhodu. Čo urobí AI, ktorá má objektívne zoradiť všetkých uchádzačov? Možno sa bez ďalšieho spoliehať na to, že aj bez výslovného príkazu danej spoločnosti (zohľadniť etnikum) sa AI rozhodne daného uchádzača zaradiť na posledné miesto, v dôsledku čoho nemusí byť na pohovor pozvaný? Diskriminačných dôvodov môže byť, samozrejme, viac (vek, sexuálna orientácia, pohlavie, etc.), riziko diskriminácie nie je iluzórne. Napriek tomu, že na úrovni Rady Európy nemá zákaz diskriminácie stanovený EDLP a jeho dodatkovými protokolmi aplikovateľnosť na čisto súkromnoprávne vzťahy (kam spadá aj načrtnuté uchádzanie o zamestnanie), jeho porušenie môže nastať aj v rovine zlyhania štátu konať aktívne, v rámci pozitívneho záväzku zabezpečiť ochranu pred diskrimináciou.¹⁷ Na úrovni EÚ je ochrana pred diskrimináciou vo vyššej kvalite – Súdny dvor EÚ prisúdil čl. 21 (1) Charty základných práv Európskej únie horizontálny priamy účinok.¹⁸ Nezhľadnenie rizík umelej inteligencie teda môže spôsobiť porušenie zákazu diskriminácie na oboch úrovniach nadnárodnej ochrany.

¹⁵ Porovnaj napr. čl. 14 Európskeho dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „EDLP“), či čl. 1 Protokolu č. 12 k EDLP.

¹⁶ Porovnaj s. 16 Council of Europe – Steering Committee for Human Rights Drafting Group on Human Rights and AI (CDDH-IA): Handbook on Human Rights and Artificial Intelligence, dostupné na: <https://rm.coe.int/steering-committee-for-human-rights-drafting-group-on-human-rights-and/1680b4coca>.

¹⁷ Napríklad v prípade, ak existuje jasná medzera v právnej úprave z hľadiska ochrany pred diskrimináciou. Porovnaj napr. § 25-27 Explanatory Report to the Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, dostupné tu: <https://rm.coe.int/09000016800cce48>.

¹⁸ Pre bližšie informácie pozri napr. BOBEK, Michal – BŘÍZA, Petr – HUBKOVÁ, Pavlína. 6.2 Horizontální přímý účinek Listiny EU. In: BOBEK, Michal – BŘÍZA, Petr – HUBKOVÁ, Pavlína. Vnitrostátní aplikace práva Evropské unie. 2. vydání. Praha: C. H. Beck, 2022, s. 284.

Príkladov je však viac, diskriminácia sa netýka výlučne pracovnoprávnej oblasti. Môže ísť napr. o prístup k zdravotnej starostlivosti (na základe AI zostavovaných poradovníkov), vzdelaniu, či k iným službám poskytovaným štátom. AI algoritmy zlyhali už v minulosti,¹⁹ diskriminácia je tu možná pod rúškom objektivity na základe získaných dát.

Právo na súkromie

V spojení s umelou inteligenciou možno právo na súkromie (hoc nie výlučne) zúžiť²⁰ na ochranu dát/osobných údajov, práve to je totiž v súčasnosti podľa názoru autora najviac aktuálne. Ak na právo na súkromie nazeráme tradičným pohľadom (vybudovaným na poznatkoch nemeckého ústavného súdu), možno každé neoprávnené spracovanie osobných údajov označiť za porušenie práva na súkromie – rovnako, ako by každé neoprávnené použitie fyzického majetku bolo porušením vlastníckeho práva.²¹

Pri tradičnom prístupe sa teda používa systém akejsi skladačky. „*Napríklad, ak je zaregistrované moje meno, evidenčné číslo vozidla alebo telefónne číslo, považuje sa to za porušenie; ak sú uložené v databáze, považuje sa to za ďalšie porušenie; a ak sú kombinované s inými osobnými údajmi, ako sú údaje o polohe, považuje sa to za ďalšie porušenie.*“²² Povedané inak, v súlade s právom je taký postup, pri ktorom je konkrétne použitie a spracovanie osobných údajov ich vlastníkovi vopred známe predtým, než udelí súhlas – každé použitie osobných údajov by malo byť odôvodnené. V zásade nebýva veľký problém určiť zodpovedný subjekt za protiprávny postup. Pri AI to ale nie je také jednoduché. Osobných údajov, ku ktorým má umelá inteligencia prístup, je mnoho. A pri jej prípadnej integrácii do administratívnych systémov ich bude ešte viac.

Na prvý pohľad nie až tak viditeľným problémom tu podľa nášho názoru nie je otázka zabezpečenia, šifrovania alebo spôsobu uchovávania osobných dát – aj keď aj aj tieto

¹⁹ Trefný je príklad vyhľadávača Google, ktorého mechanizmy rozpoznávania obrázku popisovali ľudia čiernej pleti ako gorily, alebo pri nich ukazovali sexuálne explicitný materiál. Viac o tom píše KAMBLE, R.M.: Artificial intelligence and human rights. In: Uniform Law Review, Roč. 29, č. 1 (2024), Oxford: Oxford University Press, s. 81.

²⁰ Uvedomujeme si, že právo na súkromie je ako také veľmi široké a dôslednejšej analýze jeho pre AI relevantných aspektov by mohol byť venovaný samostatný príspevok.

²¹ POSCHER, Ralf: Artificial Intelligence and the Right to Data Protection. In: VOENEKY, Silja – KELLMEYER, Philipp – MUELLER, Olaf – BURGARD, Wolfram (eds.): The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2022, s. 281–282.

²² Ibid. s. 282. Pozn.: voľný preklad autora.

(oprávnene) často vystupujú často do popredia.²³ Možno tu identifikovať dva iné zásadné problémy, ktoré spolu neodmysliteľne súvisia: 1. rýchlosť a schopnosť spracovať obrovské množstvo informácií a 2. (ne)transparentnosť.

Aj napriek tomu, že sami tvorcovia AI často deklarujú, ako sú dáta využívané len v súlade s právnym rámcom a o spracúvaní osobných údajov informujú, o realite nemusia vedieť ani oni sami. Niektorí autori uvedený problém označujú za tzv. *black box issue*, teda za problém čiernej skrinky. Vrátiac sa k vyššie načrtnutej skladačke, pri „samoučiacej sa“ AI býva problémom odhaliť, ako prišlo k zneužitiu dát, resp. k dátovému úniku. Napríklad pri používaní chatbota je v zásade nemožné zistiť, ktoré konkrétne osobné údaje (častočasť poskytnuté samotným užívateľom) umelá inteligencia použije, porovná, či inak (v rámci procesu sebazdokonaľovania) spracuje.²⁴ Pri súkromí by sme mohli ísť omnoho ďalej – napríklad do prakticky neobmedzených možností (pri dostatočnom počte zariadení) diaľkovej biometrickej identifikácie osôb v reálnom čase, ktoré by mohli zneužívať štátne zložky. Ostávame však v jednoduchšej rovine, ktorá demonštruje existenciu ohrozenia aj pri na prvý pohľad neinvazívnej činnosti, obvyčajnej komunikácii s virtuálnym asistentom. Ponúka sa tu hneď niekoľko otázok. Dá sa úniku zabrániť? A čo sa dá následne robiť, ak už raz nastane – je možné prinavrátiť pôvodný stav a zo samoučiaceho sa modelu tieto dáta jednoducho vymazať? A voči komu vyvodiť zodpovednosť, ak tieto údaje prejdú cez viacero jazykových modelov?

Uvedené otázky budú v budúcnosti podľa názoru autora ešte zásadnejšie – a to sa ani nemusíme zamýšľať nad istou formou subjektivity, ktorá by bola v budúcnosti AI legislatívne udelená a ktorá by otázku zodpovednosti redefinovala.²⁵ V súčasnosti sme len v úvode toho, čo masovo dostupné AI systémy dokážu. A už teraz im ľudia, zdá sa, dôverujú viac, než by to bolo podľa názoru autora vhodné – napríklad na komunikáciu o dôverných (intímnych) informáciách, kde sú voči chatbotom kvôli (na prvý pohľad) zaručenej anonymite otvorenejší, než pri ľudskom partnerovi.²⁶

²³ Napríklad z dôvodu, že komerčne dostupnú umelú inteligencia vyvíjajú prevažne súkromné spoločnosti. Porovnaj napr. bod 51 (s. 18) Council of Europe – Steering Committee for Human Rights Drafting Group on Human Rights and AI (CDDH-IA): Handbook on Human Rights and Artificial Intelligence, ref. 16.

²⁴ POSCHER, ref. 21, s. 283.

²⁵ Hoc viacerí autori prijímajú uvedené (osobitnú formu právnej subjektivity pre AI) pro futuro ako automatické. Vid' napr.: KSIEŻAK, Paweł – WOJTCZAK, Sylwia: Artificial Intelligence and Legal Subjectivity. In: Toward a Conceptual Network for the Private Law of Artificial Intelligence. Law, Governance and Technology Series, vol. 51. Cham: Springer, 2023, s. 13–35.

²⁶ Pre viac info pozri strany 286–290 CROES, Emmelyn A. J. – ANTHEUNIS, Marjolijn L. – VAN DER LEE, Chris – DE WIT, Jan M. S.: Digital Confessions: The Willingness to Disclose Intimate Information to a Chatbot and its Impact on Emotional Well-Being. In: Interacting with Computers, Roč. 36, č. 5 (2024), s. 279–292. Oxford: Oxford University Press.

Právo na život

Už dlhší čas je zrejmé, že EDĽP vo svojom čl. 2 (1) nechráni život človeka len negatívne, teda formou zákazu. Podobne, ako je tomu pri iných právach a slobodách, má štát aj pri článku 2 EDĽP povinnosť konať aktívne – teda „*prijat' primerané opatrenia na ochranu života osôb, ktoré sa nachádzajú v jeho jurisdikcii.*“²⁷ ESĽP následne skúma, či štát vykonal všetko, čo bolo od neho možné očakávať na to, aby bol život osoby dôvodne ohrozený.²⁸ Uvedené nie je pre právnu obec novinkou, v zásade platí, že sa tento pozitívny prístup aplikuje pri akejkolvek činnosti, pri ktorej existuje ohrozenie práva na život.²⁹ Ako to však ale súvisí s AI?

Odpoveď môžeme rozdeliť do dvoch rovín.³⁰ Optimistický scenár a pesimistický scenár. Pri optimistickom je pravdepodobné, že AI bude schopná výrazne skvalitniť ochranu ľudského života – napríklad cez vopred vytrénované jazykové modely (ako príklad autor uvádza klinickú liečbu onkologických ochorení).³¹ Pesimistický scenár možno ilustrovať na príklade idealizácie samovrážd, ktoré sú pomocou AI internetových algoritmov na sociálnej sieti TikTok mladým ľuďom cítiacim sa osamelo podsúvané.³² Uvedené je veľkým problémom. AI totiž dokáže vytvoriť istú podobu digitálnej charakteristiky tej-ktorej osobnosti, aj keď táto osoba nemusí svoje

²⁷ Pozn. voľný preklad autora § 36 rozsudku ESĽP vo veci L.C.B. v. The United Kingdom.

²⁸ Ibid.

²⁹ KRATOCHVÍL, Jan: Kapitola XI [Právo na život (čl. 2 EÚĽP)]. In: KMEC, Jiří – KOSAŘ, David – KRATOCHVÍL, Jan – BOBEK, Michal: Evropská úmluva o lidských právech. Praha: C. H. Beck, 2012, s. 362. Nejde však len o činnosti, ktoré vykonáva konkrétny jednotlivec – pozitívny záväzok štátu sa chápe v uvedenom značne širšie.

³⁰ To by bolo limitovane možné aj pri predošlých zmienených ľudských právach. Autor to však v predošlom texte nerobí z dôvodu, že možné benefity AI nie sú v daných oblastiach podľa jeho názoru tak významné, ako možné riziká. Napríklad pri práve na súkromie sa dá využívanie AI (povedzme chatbotov) chápať ako výsledok autonómneho rozhodnutia, teda naplnenie jednej zložky práva na súkromie. Nie je však niečím, čoho používanie by v súčasnosti naplňalo pozitívny záväzok štátu. Pri (ne)diskriminácii by to, hypoteticky, možné bolo. Systém vie byť vo všeobecnosti objektívnejší, ako človek. Problémom je, že to vie byť aj naopak, ako je ilustrované v predošlom texte. Pri práve na život sú benefity AI neprehliadnuteľné a ako také sú predmetom intenzívneho medicínskeho skúmania.

³¹ Kde sa očakáva, že chatboty budú schopné pomáhať pri personalizovaných možnostiach liečby, hľadani korelácií medzi rôznymi pacientmi (resp. ich zdravotným stavom) a pri výbere liekov. Bližšie pozri MURMU, Ankita – GYÖRFFY, Balázs: Artificial intelligence methods available for cancer research. In: Frontiers of Medicine, Roč. 18, č. 5 (2024), s. 790.

³² Podľa v júli 2025 publikovaného výskumu, ktorého metódou bolo na základe vpísania kľúčového slova „osamelý“ (*lonely*) do vyhľadávača danej sociálnej siete zistiť obsah, ktorý sa zobrazuje, vyšlo, že v prípade 4,9 % videí, ktoré internetový (umelou inteligenciou ovládaný) algoritmus ponúka, ide o idealizáciu samovraždy. Idealizácia sebaopoškodzovania, porúch potravy a ďalších psychických porúch bola prítomná taktiež v nezanedbateľnej vzorke obsahu. Pre viac info HARRIES, Bethan – ZENONE, Marco – HARTWELL, Greg: Feeling lonely in the online crowd: what TikTok tells us about young people and loneliness. In: Health Promotion International, Roč. 40, č. 4 (2025). Oxford: Oxford University Press, osobitne s. 3-4.

pocity nikomu zdieľať (napr. pomocou analýzy histórie vyhľadávania, či používaniu trackerov – „sledovačov“ internetového pohybu medzi stránkami na internete).³³ Sú známe prípady,³⁴ kedy chatboty údajne navádzali ľudí na spáchanie samovraždy – v niektorých prípadoch, žiaľ, úspešne.³⁵ Rovnako nemožno opomenúť ani výzvy chatbotov adresované užívateľom na zabitie iných osôb.³⁶ Opäť sa ponúka otázka zodpovednosti, odpoveď na ktorú v tejto chvíli nepoznáme, keďže na rozhodnutie v prelomovom prípade³⁷ sa ešte čaká. Isté je len to, že aj v oblasti ochrany ľudského života je pri používaní AI potrebná významná miera opatrnosti.

Zvlášť, keď prebieha práca na AI nástrojoch zameraných na predikciu samovražedného správania. Uvedené vyvoláva, aj ak by AI nástroje fungovali stopercentne (čo sa pri riadkoch vyššie nejaví), oprávnené obavy s nakladaním s takýmito dátami o zdravotnom stave – čiže so súkromím, rozoberanom v predošlej časti.³⁸ Na záver tejto časti je však potrebné skonštatovať, že zásahy AI do práva na život nie sú len sci-fi, ako by sa to na prvý pohľad mohlo javiť. K otázke zodpovednosti (alebo pričítateľnosti) však možno ešte jednu poznámku. Pri práve na život sa ešte viac, než pri iných ukazuje, že zodpovednosť je až sekundárna otázka. Stratený život

³³ Uvedené profilačné praktiky (vrátane zberu citlivých informácií) sú bežnou súčasťou AI rozšírení pre internetové prehliadače, čo potvrdil výskum zverejnený na webových stránkach *Cornell University* (osobitne relevantné sú s. 12-15). VEKARIA, Yash et al.: Big Help or Big Brother? Auditing Tracking, Profiling, and Personalization in Generative AI Assistants.

³⁴ Napr. GUO, Eileen: An AI chatbot told a user how to kill himself—but the company doesn't want to "censor" it. MIT Technology Review, 6. februára 2025, dostupné tu: <https://www.technologyreview.com/2025/02/06/1111077/nomi-ai-chatbot-told-user-to-kill-himself/>.

³⁵ PAYNE, Kate: An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges. AP News, 26. október 2024, dostupné tu: <https://apnews.com/article/chatbot-ai-lawsuit-suicide-teen-artificial-intelligence-9d48adc572100822fdb3c90d1456bdo>. Spoločnosti Alphabet (Google) a Character.AI medzičasom v uvedenom prípade čelia žalobe. Americká sudkyňa okresného súdu Anne Conway zatiaľ odmietla ich tvrdenia, že výstupy chatbota sú chránené slobodu prejavu, resp., že sú vôbec prejavom. Pozri napr. BRITTAIN, Blake: Google, AI firm must face lawsuit filed by a mother over suicide of son, US court says. Reuters, 21. máj 2025, dostupné tu: <https://www.reuters.com/sustainability/boards-policy-regulation/google-ai-firm-must-face-lawsuit-filed-by-mother-over-suicide-son-us-court-says-2025-05-21/>.

³⁶ Pozri napr. situáciu, o ktorej píše GERKEN, Tom: Chatbot 'encouraged teen to kill parents over screen time limit'. BBC News, 11. december 2024, dostupné tu: <https://www.bbc.com/news/articles/cd605e48q1vo>, kedy AI podsúvala chlapcovi možnosť zabiť svojich rodičov ako adekvátnu reakciu za časové obmedzenie používania smartfónu.

³⁷ Ref. 35.

³⁸ Ak by k daným údajom dostal prístup štát – napríklad skrz v budúcnosti možné preventívne psychické prehliadky (a povedzme osoba X by bola vyhodnotená umelou inteligenciou pri psychologickom teste ako riziková z pohľadu potenciálneho spáchania samovraždy), existujú názory, počet samovrážd by to, paradoxne, mohlo zvýšiť. Bližšie pozri MARKS, Mason: Artificial Intelligence-Based Suicide. In: Yale Journal of Law & Technology, roč. 21, Special Issue 98, dostupné tu: <https://yolt.org/artificial-intelligence-based-suicide>, s. 113.

majetková kompenzácia prinavrátiť nedokáže. Regulácia by na uvedené mala pamätať. Je to tak však aj v skutočnosti?

Čo na to Európa?

Najviac relevantné sú v tejto chvíli dva právne akty na dvoch rozdielnych úrovniach. Na úrovni Európskej únie je ním nariadenie Európskeho parlamentu a rady (EÚ) 2024/1689 (ďalej len „Akt o AI“);³⁹ Rada Európy prijala Rámcový dohovor Rady Európy o umelej inteligencii (ďalej len „Dohovor o AI“).⁴⁰ Oba dokumenty sú vzájomne kompatibilné, čo potvrdila aj Európska únia tým, že sa vo vzťahu k Dohovoru o AI stala jeho signatárom. Je však potrebné dodať, že Dohovor o AI ešte v čase písania tohto príspevku nenadobudol účinnosť – stane sa tak v zmysle jeho čl. 30 (3) po uplynutí 3 mesiacov odo dňa, kedy ho ratifikujú piati signatári (z nich aspoň tri členské štáty Rady Európy). Do dnešného dňa Dohovor o AI neratifikoval ani jeden subjekt.⁴¹ Vo vzťahu k Aktu o AI je taktiež potrebné zdôrazniť, že je posunutá uplatniteľnosť časti jeho ustanovení na august 2026, resp. časti na august 2027.⁴² V tomto príspevku sa však, so zúžením na rozoberané ľudské práva, venujeme obom právnym aktom v ich úplnej podobe – najskôr regulácii na úrovni EÚ, následne na úrovni Rady Európy.

Akt o AI predstavuje podľa slov EÚ prvú komplexnú reguláciu AI vo svete.⁴³ Vo vzťahu k ľudskoprávnej oblasti však tvrdenie o komplexnosti nie je na mieste (a to ani vtedy, ak berieme v úvahu jeho v súčasnosti ešte neuplatňované ustanovenia). Na jednej strane síce predmetný dokument (veľmi správne) obsahuje v čl. 5 zoznam tzv. (absolútne) zakázaných praktík,⁴⁴ či kategorizuje systémy AI podľa miery rizika, čomu následne prispôsobuje miestami prísnu reguláciu, ktorá je primárne orientovaná na tzv. vysokorizikové systémy.⁴⁵ Je potrebné dodať, že aj keď ide v ich

³⁹ Dostupné tu: <http://data.europa.eu/eli/reg/2024/1689/oj>.

⁴⁰ Dostupné tu: <https://rm.coe.int/1680a0fae3c>.

⁴¹ Pozri tu: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.

⁴² Vid' čl. 113 Aktu o AI.

⁴³ Slová sú prebraté zo stránky Európskeho parlamentu, dostupné tu: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.

⁴⁴ Ide pomyselné hranicu, ktorá nesmie byť žiadnym systémom, na ktoré sa nariadenie vzťahuje, prekročená. Napríklad je zakázané využívanie podprahových techník [čl. 5 (1) písm. a)], zraniteľnosti fyzickej osoby [čl. 5 (1) písm. b)], diskriminačná klasifikácia osôb [čl. 5 (1) písm. c)], biometrická kategorizácia [čl. 5 (1) písm. g)], až na výnimky biometrická identifikácia v reálnom čase [čl. 5 (1) písm. h)], či iné.

⁴⁵ Pomenovanie zvyšných kategórií je implicitné – napr. MESARČÍK – GYURÁSZ, ref. 6 na s. 73 – uvádzajú systémy obsahujúce praktiky uvedené pod čl. 5 ako systémy neprijateľného rizika (teda

prípade „len“ o vysoké a nie o neprijateľné riziko (ako je to pri čl. 5), rizikové oblasti sú veľmi citlivé (vzdelávanie, zamestnanosť, biometria, etc.).⁴⁶ Tieto systémy preto právo EÚ prikazuje dizajnovať tak, aby bolo možné počas obdobia používania vykonávať nad ich činnosťou ľudský dohľad,⁴⁷ či dokonca „v akejkoľvek konkrétnej situácii rozhodnúť, že sa vysokorizikový systém AI nepoužije alebo sa výstup vysokorizikového systému AI inak nezohľadní, potlačí alebo zvráti.“⁴⁸ Uvedené by teoreticky⁴⁹ dokázalo pokryť škálu nami načrtnutých najviac zásadných ľudskoprávných rizík rozoberaných v predošlých častiach textu. Na druhej strane, ľudskoprávne organizácie (napr. Amnesty International) upozorňujú na viacero nedôsledností, s ktorými nová regulácia prichádza, predovšetkým:

1. Akt o AI (článok 27) síce obsahuje povinnosť nasadzujúceho subjektu⁵⁰ vykonať posúdenie vplyvu na základné práva v prípade vysokorizikových systémov AI, otáznou je efektivita uvedeného procesu. Toto posúdenie zahŕňa viacero aktivít (napr. definovanie konkrétnych rizík ujmy voči fyzickým osobám a opatrení, ktoré sa v prípade ich naplnenia majú aplikovať), žiaden subjekt tieto riziká neoveruje z hľadiska ich prijateľnosti. Rovnako tak nie je stanovená povinnosť týmto ľudskoprávnym rizikám predchádzať.⁵¹ Posúdenie vplyvu na základné práva sa preto môže javiť ako formálne.
2. Existujú rozdiely v registračnej povinnosti medzi súkromným a verejným sektorom⁵² – napr. nasadzujúci subjekt vysokorizikového systému AI zo súkromného sektora nie je, na rozdiel od náprotivku z verejného sektora, povinný registrovať sa v databáze, do ktorej sa evidujú napríklad posúdenia vplyvov na ľudské práva.⁵³ Ako je však v predošlých častiach textu uvedené,

obdobne ako preambula daného aktu označuje predmetné praktiky za neprijateľné), „pod“ vysokorizikovými sú systémy s nízkym/žiadnym rizikom, ktorých regulácia je veľmi obmedzená. Sú dve metódy, pomocou ktorých možno AI systém kategorizovať ako vysokorizikový, pre tento príspevok nie je uvedené podstatné detailnejšie rozoberať. V prípade záujmu pozri čl. 6 ods. 1-3, ods. 2 v spojení s prílohou III; pre väčšie porozumenie s. 76-85 MESARČÍK – GYURÁSZ, ref. 6

⁴⁶ Kompletný výpočet je v prílohe III.

⁴⁷ Čl. 14 Aktu o AI.

⁴⁸ Čl. 14 (4) písm. d) Aktu o AI.

⁴⁹ Teoretické je to z dvoch dôvodov. 1. – žiadna regulácia nie je účinná na 100%; 2. – regulácia je vo svojich častiach nedôsledná, ako uvádzame nižšie. Teoreticky by však k načrtnutej diskriminácii dochádzať nemalo, rovnako ani k ohrozeniu života, obe tieto praktiky spadajú totiž, ako vyššie uvádzame, pod absolútne zakázané.

⁵⁰ K pojmu pozri čl. 3 (4) Aktu o AI.

⁵¹ AMNESTY INTERNATIONAL: EU's AI Act fails to set gold standard for human rights, dostupné tu: <https://www.amnesty.eu/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf>, s. 3.

⁵² Ibid., s. 2. Amnesty International upozorňuje aj na viac problémov, ktoré v tomto článku nerozoberáme.

⁵³ Porovnaj čl. 49 (3) v spojení s čl. 71 Aktu o AI.

v súkromnom sektore sú ľudskoprávne riziká AI taktiež značné a tento rozdiel (medzi verejným a súkromným sektorom) vníma preto autor *in concreto* ako neopodstatnený.

Oba tieto body v nás vyvolávajú, a to napriek vo všeobecnosti ocenení snahe únijných regulátorov, pochybnosti, do akej miery bude takto (ne)dôsledný regulačný rámec postačovať. Na „odsúdenie“ efektívnosti daného predpisu je síce ešte priskoro, máme ale obavy, či takto nastavená ochrana ľudských práv dokáže v praxi prekročiť tieň občasnej formálnosti.

Dohovor o AI by mal byť, na rozdiel od aktu z dielne EÚ, primárne orientovaný na ľudské práva. V porovnaní s Aktom o AI je tvorený inou filozofiou, mierne inšpirovaný štýlom EDLP. Dohovor je (aj vzhľadom na rámcový charakter) stručnejší, v dôsledku čoho je častokrát (aj napriek snahe o konkrétne vymedzenie vybraných oblastí ľudských práv, ktoré majú štáty osobitne chrániť) až priveľmi všeobecný.⁵⁴ Na všeobecnosti rámcového dohovoru nemusí byť nič zlé – otázne je, či to však v tak dynamickej oblasti nie je kontraproduktívne. Ochrane ľudských práv pred negatívnym efektom AI podľa nášho názoru nepomôže akási obdoba formálnej deklarácie bez reálnych kontúr. Dohovor o AI v súčasnosti (odhliadnuc od toho, že ešte nenadobudol účinnosť), inak hodnotiť podľa nášho názoru ani nemožno.

Záver

Stephen Hawking pri otvorení *Leverhulme Centre for the Future of Intelligence* povedal: „Úspech pri tvorbe umelej inteligencie by mohol byť najväčšou udalosťou v histórii našej civilizácie, ale mohol by byť aj úspechom posledným – pokiaľ sa nenaučíme, ako sa vyhnúť (jej) rizikám.“⁵⁵ Riziká spojené s ľudskými právami sú veľké, efektívnosť regulácie je otázna. Na definitívne zodpovedanie otázky, či je Európa na umelú inteligenciu legislatívne pripravená, treba ešte nejaký čas počkať – až sa efekt regulácie naplno dostaví. Minimálne na úrovni EÚ sú riziká prípadných pokút dostatočne vysoké na predpoklad, že nedostatočná výška sankcií nebude dôvodom regulačnej neefektivity, ak by aj neefektívnosť nastala.⁵⁶ Určenie subjektu, voči ktorému bude v konečnom bode zodpovednosť vyvedená, však nebude tak jednoduché. Jedno je však isté už teraz. Z pohľadu ochrany ľudských práv mohla byť

⁵⁴ Porovnaj napr. znenie čl. 10 Dohovoru o AI, ktorý patrí medzi jeho obsažnejšie články.

⁵⁵ “The best or worst thing to happen to humanity” - Stephen Hawking launches Centre for the Future of Intelligence, dostupné tu: <https://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of>. Pozn.: voľný preklad autora.

⁵⁶ Článok 99 Aktu o AI. – za isté porušenia až do výšky 7% celosvetového ročného obratu, alebo do 35 000 000 Eur podľa toho, ktorá suma je vyššia.

Európa⁵⁷ pripravená ešte lepšie. I tak je však otázne, akou cestou sa vydať. Nedôsledná regulácia „nahráva“ technologickým gigantom, teda súkromnému sektoru, príliš prísna (autoritatívno-arbitrárna) spôsobuje, v prípade nedostatočnej verejnej participácie, demokratický deficit.⁵⁸ To všetko je v protiklade so spoločným dobrom, v oboch prípadoch sa totiž sledujú záujmy len jednej skupiny, nie dobro spoločnosti ako takej. Nech je to akokoľvek, dynamika vývoja AI neposkytuje možnosť na nedôslednosť, prípadné pochybenia sa budú naprávať ťažko. A klásť si v závere otázku, kto bude za prípadné zlyhania zodpovedný – či AI; spoločnosť, ktorá ju vytvorila; štáty; etc. – nebude to najdôležitejšie.

Zoznam použitej literatúry

1. BOBEK, Michal – BŘÍZA, Petr – HUBKOVÁ, Pavlína. 6.2 Horizontální přímý účinek Listiny EU. In: BOBEK, Michal – BŘÍZA, Petr – HUBKOVÁ, Pavlína. Vnitrostátní aplikace práva Evropské unie. 2. vydání. Praha: C. H. Beck, 2022, s. 282-290. ISBN 978-80-7400-896-2.
2. COECKELBERGH, Mark: Artificial intelligence, the common good, and the democratic deficit in AI governance. In: AI and Ethics, roč. 5, č. 2 (2025), s. 1491–1497. <https://doi.org/10.1007/s43681-024-00492-9>.
3. CROES, Emmelyn A. J. – ANTHEUNIS, Marjolijn L. – VAN DER LEE, Chris – DE WIT, Jan M. S.: Digital Confessions: The Willingness to Disclose Intimate Information to a Chatbot and its Impact on Emotional Well-Being. In: Interacting with Computers, Roč. 36, č. 5 (2024), s. 279–292. Oxford: Oxford University Press. <https://doi.org/10.1093/iwc/iwae016>.
4. HARRIES, Bethan – ZENONE, Marco – HARTWELL, Greg: Feeling lonely in the online crowd: what TikTok tells us about young people and loneliness. In: Health Promotion International, Roč. 40, č. 4 (2025). Oxford: Oxford University Press. <https://doi.org/10.1093/heapro/daaf094>.
5. KAMBLE, R.M.: Artificial intelligence and human rights. In: Uniform Law Review, Roč. 29, č. 1 (2024), Oxford: Oxford University Press, s. 77-86. <https://doi.org/10.1093/ulr/unae020>.
6. KRATOCHVÍL, Jan: Kapitola XI [Právo na život (čl. 2 EÚLP)]. In: KMEC, Jiří – KOSAŘ, David – KRATOCHVÍL, Jan – BOBEK, Michal: Evropská úmluva o lidských právech. Praha: C. H. Beck, 2012, s. 345 – 396. ISBN 978-80-7400-365-3.
7. KSIĘŻAK, Paweł – WOJTCZAK, Sylwia: Artificial Intelligence and Legal Subjectivity. In: Toward a Conceptual Network for the Private Law of Artificial

⁵⁷ To platí aj pre EÚ, o to viac však pre Radu Európy, aj keď sa nezanedbateľný počet ich členských štátov prelína.

⁵⁸ COECKELBERGH, Mark: Artificial intelligence, the common good, and the democratic deficit in AI governance. In: AI and Ethics, roč. 5, č. 2 (2025), s. 1491–1497, s. 5.

Intelligence. Law, Governance and Technology Series, vol. 51. Cham: Springer, 2023, s. 13–35. https://doi.org/10.1007/978-3-031-19447-4_2.

8. MARKS, Mason: Artificial Intelligence-Based Suicide. In: Yale Journal of Law & Technology, roč. 21, Special Issue 98, s. 98–121. <https://yjolt.org/artificial-intelligence-based-suicide>.
9. MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 244 s. ISBN: 978-80-7160-715-1
10. MURMU, Ankita – GYÖRFFY, Balázs: Artificial intelligence methods available for cancer research. In: Frontiers of Medicine, Roč. 18, č. 5 (2024), s. 778–797. <https://doi.org/10.1007/s11684-024-1085-3>.
11. POSCHER, Ralf: Artificial Intelligence and the Right to Data Protection. In: VOENEKY, Silja – KELLMEYER, Philipp – MUELLER, Olaf – BURGARD, Wolfram (eds.): The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2022, s. 281–289. <https://doi.org/10.1017/9781009207898.022>.
12. SARRION, E.: How Does ChatGPT Work?. In: Exploring the Power of ChatGPT. Berkeley, CA: Apress, 2023, s. 9–16. https://doi.org/10.1007/978-1-4842-9529-8_2.
13. SZAPPANYOS, Melinda: Artificial Intelligence: Is the European Court of Human Rights Prepared?. In: Acta Humana – Human Rights Publication, Roč. 11, č. 1 (2023), s. 93–110. <https://doi.org/10.32566/ah.2023.1.6>.
14. VEKARIA, Yash et al.: Big Help or Big Brother? Auditing Tracking, Profiling, and Personalization in Generative AI Assistants. <https://doi.org/10.48550/arXiv.2503.16586>.

Kontaktné údaje

Mgr. Martin Búran

martin.buran@flaw.uniba.sk

Katedra ústavného práva

Právnická fakulta Univerzity Komenského v Bratislave

MEDZINÁRODNOPRÁVNE ASPEKTY VYUŽÍVANIA TECHNOLÓGIÍ PRI KONTROLE A OCHRANE BIODIVERZITY¹

INTERNATIONAL LEGAL ASPECTS OF THE USE OF TECHNOLOGIES IN BIODIVERSITY MONITORING AND PROTECTION

Petra Paľuchová²

Abstrakt: Príspevok sa zameriava na prepojenie ochrany voľne žijúcich živočíchov s modernými technológiami a umelou inteligenciou. Cieľom je preskúmať, do akej miery môžu technologické a digitálne nástroje posilniť existujúce medzinárodnoprávne nástroje pri regulácii obchodu s ohrozenými druhmi a prispieť k efektívnejšiemu dodržiavaniu záväzkov štátov vyplývajúcich z Dohovoru o biologickej diverzite, ako aj Dohovoru o medzinárodnom obchode s ohrozenými druhmi voľne žijúcich živočíchov a rastlín. Z metodologického hľadiska využíva príspevok metódu analýzy právnych textov a relevantnej vedeckej literatúry, komplementárne je pritom využívaná aj komparatívna a interpretačná metóda. Osobitná pozornosť je v rámci príspevku venovaná využívaniu moderných technológií pri monitorovaní populácií, odhaľovaní nelegálnych aktivít a zlepšovaní kontrolných mechanizmov. V závere príspevok poukazuje na limity súčasného systému a identifikujú prínos technológií ako doplnku k existujúcej medzinárodnoprávnej regulácii. Príspevok v neposlednom rade rozoberá otázku právnej zodpovednosti subjektov v prípade škôd spôsobených technológiami, v kontexte čoho poukazuje na nejednoznačnosť existujúcich pravidiel v medzinárodnej aj vnútroštátnej rovine. Príspevok prináša vedecký prínos v podobe systematizácie diskusie o úlohe technológií v ochrane biodiverzity a praktický prínos v identifikácii odporúčaní pre efektívnejšie využívanie moderných technológií pri presadzovaní medzinárodných environmentálnych záväzkov.

¹ Predkladaný príspevok bol spracovaný s podporou projektu č. UK/1285/2025 s názvom *Ochrana zvierat nástrojmi medzinárodného práva*.

² Katedra medzinárodného práva a medzinárodných vzťahov, Právnická fakulta, Univerzita Komenského v Bratislave

Kľúčové slová: ochrana zvierat, voľne žijúce druhy, CITES, biodiverzita, nové technológie

Abstract: The paper examines the relationship between wildlife protection and the use of modern technologies and artificial intelligence. Its aim is to explore how technological and digital tools can strengthen existing international legal instruments regulating trade in endangered species and support compliance with states' obligations under the Convention on Biological Diversity and the Convention on International Trade in Endangered Species of Wild Fauna and Flora. Methodologically, the paper applies legal text analysis and relevant scientific literature, complemented by comparative and interpretative methods. Special attention is given to the role of technologies in population monitoring, detection of illegal activities, and the improvement of control mechanisms. The paper highlights the limitations of the current system and identifies the contribution of technologies as a supplement to existing international legal regulation. It further discusses the issue of legal responsibility for damage caused by technologies, stressing the ambiguity of current rules at both international and national levels. The scientific contribution lies in the systematization of the debate on the role of technologies in biodiversity protection, while the practical relevance rests in identifying recommendations for more effective use of modern technologies in enforcing international environmental commitments.

Key words: animal protection, wild species, CITES, biodiversity, new technologies

Úvod

Ochrana životného prostredia patrí k najdiskutovanejším a najvýraznejším témam súčasnosti. Otázky udržateľného rozvoja, klimatickej zmeny a straty biodiverzity sa stali predmetom pozornosti laickej verejnosti a politických stratégií, čo ich posúva medzi aktuálne témy súčasnosti. Strata biodiverzity patrí k najvážnejším globálnym hrozbám 21. storočia. Podľa Správy IPBES³ je ohrozených (na pokraji vyhynutia v

³ IPBES značí tzv. Medzivládnu platformu pre biodiverzitu a ekosystémové služby (z angl. The Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services), ktorá je nezávislým medzivládnym orgánom s cieľom posilniť prepojenie medzi vedou a politikou v oblasti biodiverzity. Hoci nie je orgánom Organizácie Spojených národov, Program OSN pre životné prostredie poskytuje IPBES sekretariátne služby. Predmetná správa je prvá komplexná svojho druhu a odvoláva sa na ňu aj samotná Organizácia Spojených národov. K tomu bližšie v: UNITED NATIONS. UN Report: Nature's Dangerous Decline 'Unprecedented'; Species Extinction Rates 'Accelerating',

priebehu niekoľkých desaťročí) až jeden milión druhov. Azda ešte dôležitejšia je skutočnosť, že otázky environmentálnej ochrany, resp. ochrany biodiverzity sú nemenej centrom odbornej diskusie, nevynímajúc právnu vedu. Práve prostredníctvom medzinárodného práva štáty koordinujú svoje povinnosti a prijímajú záväzky smerujúce o. i. k ochrane prírodného dedičstva. Pri pohľade na udalosti posledných desaťročí ale možno pozorovať, že tradičné kontrolné mechanizmy dodržiavania záväzkov nie sú postačujúce.

Nelegálny obchod s voľne žijúcimi živočíchmi sa posledné roky zaradil medzi najvýnosnejšie formy organizovaného zločinu.⁴ UNODC uvádza, že nelegálny obchod postihuje približne 4 000 druhov a prebieha v desiatkach štátov.⁵ Takýto nelegálny trh so slonovinou, exotickými vtákmi či morským bohatstvom pritom nepredstavuje výlučne environmentálny problém, ale je aj problémom bezpečnostným.⁶

Na tento problém pritom reagovalo medzinárodné spoločenstvo prijatím viacerých mnohostranných zmlúv, najmä Dohovoru o biologickej diverzite (1992) (ďalej aj len ako „**CBD**“)⁷ a Dohovoru o medzinárodnom obchode s ohrozenými druhmi voľne žijúcich živočíchov a rastlín (1973)⁸ (ďalej aj len ako „**CITES**“). CBD možno vnímať ako rámcový dohovor, ktorého cieľom je zastaviť úbytok biodiverzity. CITES bola uzatvorená s cieľom regulovať medzinárodný obchod s voľne žijúcimi živočíchmi a rastlinami, aby sa zabezpečilo, že tento obchod nebude mať negatívny vplyv na voľne žijúce populácie rastlín a živočíchov, ktoré sú predmetom obchodu.⁹

Napriek existencii uvedených medzinárodnoprávných nástrojov sa v praxi potvrdzuje, že boj s nelegálnym obchodom a efektívna ochrana biodiverzity zostávajú mimoriadne náročnou úlohou. Za posledné roky sa preto do popredia dostáva aj otázka, akým spôsobom môže byť ochrana voľne žijúcich druhov posilnená pomocou využitia moderných technológií, ktoré sú schopné precíznejšieho monitorovania, odhaľovania nelegálnych aktivít a vyhodnocovania zozbieraných údajov. Ochrana biodiverzity je tak spojená s technologickým rozvojom. Na tom základe ale vyvstávajú niektoré právne otázky. CITES a CBD ukladajú povinnosti

2025. [online]. Dostupné na internete dňa 28.09.2025: <https://www.un.org/sustainabledevelopment/blog/2019/05/nature-decline-unprecedented-report/>.

⁴ MOORE, Kimberly C.: The Case for the Legal Protection of Animals. Humanity's Shared Destiny with the Animal Kingdom, 2023. s. 89.

⁵ UNODC, World Wildlife Crime Report 2024: Trafficking in Protected Species (Vienna: United Nations publications, 2024). [online]. Dostupné na internete dňa 28.09.2025: https://www.unodc.org/documents/data-and-analysis/wildlife/2024/Wildlife2024_Final.pdf. s. 22, 61.

⁶ *Ibid.* s. 92.

⁷ Dohovor o biologickej diverzite (Convention on Biological Diversity) 1760 UNTS 79.

⁸ Dohovor o medzinárodnom obchode s ohrozenými druhmi voľne žijúcich živočíchov a rastlín (Convention on International Trade in Endangered Species of Wild Fauna and Flora) 993 UNTS 243.

⁹ WIJNSTEKERS, Willem: The Evolution of CITES - 9th edition, 2011. s. 32.

výlučne štátom, technológie nevyhnutné na ich realizáciu spravujú a ovládajú prevažne súkromné spoločnosti či výskumné inštitúcie. Naskytá sa tak otázka zodpovednosti za škodu spôsobenú využívaním týchto technológií. Predkladaný príspevok sa preto sústreďuje na analýzu prierezových otázok a identifikáciu výziev v rámci využívania technológií a ochrany biodiverzity.

Medzinárodnoprávny režim ochrany biodiverzity

Biologická rozmanitosť je pre spoločnosť, resp. ľudstvo ako také, životne dôležitá. Z ekonomického a sociálneho hľadiska predstavuje základ širokého spektra ekosystémových služieb, od ktorých závisí nielen ľudský blahobyť, ale aj samotný rozvoj spoločnosti.¹⁰ Hoci vedecká diskusia o presnom vzťahu medzi biodiverzitou a poskytovaním ekosystémových služieb nie je úplne jednoznačná,¹¹ možno povedať, že konsenzus sa zakladá minimálne na skutočnosti, že zachovanie biodiverzity je podmienkou udržateľného fungovania spoločnosti.

Sohľadom na to sa ochrana biodiverzity dostala do centra pozornosti medzinárodného práva a stala sa predmetom mnohostranných zmlúv. Možno spomenúť dva základné právne nástroje, ktoré vznikli od druhej polovice 20. storočia, a síce už spomínaný CITES a CBD. Spoločne tieto predstavujú jadro medzinárodného režimu ochrany biodiverzity, každý však s odlišným zameraním.

Dohovor o biologickej diverzite a jeho limity

Stejskal tvrdí, že CBD možno s niekoľkými výhradami vnímať ako kodifikáciu právnej úpravy starostlivosti o biologickú rozmanitosť,¹² pričom ale ide o rámcový dohovor, ktorý stanovuje základné ciele a princípy v oblasti ochrany biodiverzity, zatiaľ čo záväzky a mechanizmy ich napĺňania sa rozpracúvajú prostredníctvom jeho protokolov, resp. dodatkov.¹³

CBD hneď vo svojom čl. 1 ustanovuje záväzok zmluvných strán zastaviť a zvrátiť úbytok biodiverzity. Cieľmi tohto dohovoru sú v jeho zmysle zachovanie biologickej diverzity, trvalo udržateľné využívanie jej zložiek a spravodlivé a rovnocenné rozdeľovanie prínosov vyplývajúcich z využívania genetických zdrojov, a to aj

¹⁰ STEJSKAL, Vojtěch: Právní prostředky ochrany biologické rozmanitosti. In: České právo životního prostředí, Č. 29 (2011), s. 7. K tomu bližšie aj v: SECRETARIAT OF THE CONVENTION ON BIOLOGICAL DIVERSITY. Global Biodiversity Outlook 3. Montréal, 2010. ISBN 92-9225-220-8. [online]. Dostupné na internete dňa 28.09.2025: <http://www.cbd.int/GB03>. s. 23.

¹¹ PLEŠNÍK, Jan: Ekosystémové služby nejsou anonymní: Význam organismů pro fungování ekosystémů. In: Ochrana přírody, Roč. 67, č. 5 (2012), s. 24.

¹² STEJSKAL, Vojtěch: Úvod do právní úpravy ochrany přírody a péče o biologickou rozmanitost, 2006. s. 46.

¹³ KLEMM, Cyrille de – SHINE, Clare: Biological Diversity Conservation and the Law: Legal Mechanisms for Conserving Species and Ecosystems, 1993. s. 24.

prostredníctvom primeraného prístupu ku genetickým zdrojom a primeraného prenosu príslušných technológií, s prihliadnutím na všetky práva k týmto zdrojom a technológiám, ako aj prostredníctvom primeraného financovania.¹⁴

Ako ale upozorňujú autori Ekardt, Günther, Hagemann a i., tieto ciele nemožno vnímať striktne *len* ako politické vyhlásenia, ale prostredníctvom systematickej a teleologickej interpretácie ich možno považovať za právne záväzné povinnosti zmluvných strán, a to aj napriek tomu, že formulácia viacerých ustanovení dohovoru obsahuje vyjadrenia ako „*as far as possible*“ alebo „*as appropriate*“.¹⁵ Argumentujú okrem iného aj čl. 31 ods. 1 Viedenského dohovoru o zmluvnom práve, ktorý zaväzuje štáty konať, vykladať zmluvy dobromyseľne, v súlade s obvyklým významom a s prihliadnutím na predmet a účel zmluvy.¹⁶

Napriek zmienenej záväznosti jeho ustanovení a normatívnej povahe cieľov, ktoré stanovuje, praktické skúsenosti uplatňovania tohto dohovoru ukazujú, že toto uplatňovanie je zväčša obmedzené. V dôsledku vo všeobecnej rovine formulovaných povinností je v konečnom dôsledku štátom umožnené uchýliť sa k voľnejšiemu výkladu a *praktická záväznosť* dohovoru je tak oslabená.

Ďalším nedostatkom je monitorovanie dodržiavania tohto dohovoru. CBD neobsahuje silný kontrolný mechanizmus. V rámci CBD funguje mechanizmus podávania správ, kedy štáty predkladajú vlastné národné správy. Na rozdiel od Kartagenského¹⁷ či Nagojského protokolu,¹⁸ ktoré disponujú vlastnými komisiami poverenými kontrolou ich dodržiavania, samotný CBD takýto nástroj nemá.¹⁹ Konferencia zmluvných strán nehodnotí individuálne správy predkladané štátmi, ale vychádza iba zo zozbieraného materiálu, ktorý pripravuje sekretariát.²⁰ Súčasné hodnotenia sa pritom sústreďujú najmä na formálnu stránku, a teda či bola správa

¹⁴ CBD, čl. 1.

¹⁵ EKARDT, Felix et al.: Legally binding and ambitious biodiversity protection under the CBD, the global biodiversity framework, and human rights law. In: Environmental Sciences Europe, Vol. 35, N. 80 (2023). s. 7. <https://doi.org/10.1186/s12302-023-00786-5>

¹⁶ Vyhláška ministra zahraničných vecí č. 15/1988 Zb. o Viedenskom dohovore o zmluvnom práve.

¹⁷ Kartagenský protokol o biologickej bezpečnosti, 2226 UNTS 208, UN Doc. UNEP/CBD/ExCOP/1/3.

¹⁸ Nagojský protokol o prístupe ku genetickým zdrojom a spravodlivom a rovnocennom využívaní prínosov vyplývajúcich z ich využívania, 3008 UNTS 3.

¹⁹ MORGERA, Elisa – TSIUOMANI, Elsa: Yesterday, Today, and Tomorrow: Looking Afresh at the CBD. In: Yearbook of International Environmental Law, Vol. 21, N. 1 (2010), s. 31. <https://doi.org/10.1093/yiel/yv003>

²⁰ XIANG, YIBIN – MEEHAN, Sandra: Financial Cooperation, Rio Conventions and Common Concerns. In: Review of European Community and International Environmental Law, Vol. 14, N. 3 (2005), s. 218.

predložená a aké kvantitatívne údaje obsahuje, nie na kvalitatívne posúdenie obsahu a reálneho plnenia záväzkov. CBD má tak v tomto smere zásadnú slabinu.²¹

Takéto nedostatky sa prirodzene premietli aj do výsledkov, kedy sa nepodarilo úplne splniť žiaden z dvadsiatich cieľov (tzv. Aichi Targets)²² prijatých na obdobie 2010-2020.²³ Rovnako aj Správa IPBES konštatuje, že napriek existencii záväzných medzinárodnoprávných pravidiel je približne jeden milión druhov v súčasnosti tak či onak ohrozený vyhynutím.²⁴

Vyššie v texte naznačené závery týkajúce sa obmedzeného plnenia záväzkov vyplývajúcich z CBD však nie sú osobitne prekvapivé či výnimočné. Uvedené je celkom typické pre mnohé rámcové zmluvy v medzinárodnom práve životného prostredia, ktoré často fungujú skôr ako politické smerovanie než ako efektívne vymáhateľné pravidlá správania sa pre ich zmluvné strany. Možno povedať, že medzinárodné environmentálne právo sa často vo veľkej miere spolieha na postupné prijímanie protokolov a doplňujúcich mechanizmov. Aj v oblasti, ktorá je predmetom tohto článku sa preto už v 70. rokoch objavila potreba reakcie na konkrétnejšiu *hrozbu* v podobe nekontrolovaného obchodu s ohrozenými druhmi.²⁵ Nástrojom prijatým na reguláciu tejto oblasti sa stal CITES. Zatiaľ čo CBD sleduje širšie ciele zachovania a udržateľného využívania biologickej rozmanitosti, CITES reguluje najmä obchod s exemplármi ohrozených druhov.

²¹ KOH, Niak – ITUARTE-LIMA, Claudia – HAHN, Thomas: Mind the Compliance Gap: How Insights from International Human Rights Mechanisms Can Help to Implement the Convention on Biological Diversity. In: Transnational Environmental Law, Vol. 11, č. 1 (2022), s. 14. doi:10.1017/S2047102521000169

²² Tzv. Aichi Targets predstavujú súbor dvadsiatich globálnych cieľov prijatých v roku 2010 ako súčasť Strategického plánu pre biodiverzitu 2011-2020. Sú dôkazom úsilia medzinárodného spoločenstva zastaviť stratu biodiverzity. Pokrývali témy od zníženia tlakov na biodiverzitu, cez zachovanie ekosystémov a druhov, až po spravodlivé rozdeľovanie prínosov z genetických zdrojov. K tomu pozri: CONVENTION ON BIOLOGICAL DIVERSITY. Strategic Plan for Biodiversity 2011-2020, including Aichi Biodiversity Targets, 2020. [online]. Dostupné na internete dňa 28.09.2025: <https://www.cbd.int/sp/targets>.

²³ SECRETARIAT OF THE CONVENTION ON BIOLOGICAL DIVERSITY. Global Biodiversity Outlook 5. Summary for Policy Makers. Montréal, 2020. ISBN 9789292256883. [online]. Dostupné na internete dňa 28.09.2025: <https://www.cbd.int/gbo/gbo5/publication/gbo-5-spm-en.pdf>. s. 14-16.

²⁴ IPBES. The global assessment report on biodiversity and ecosystem services. Summary for Policy Makers. Bonn, 2019. [online]. Dostupné na internete dňa 28.09.2025: https://files.ipbes.net/ipbes-web-prod-public-files/inline/files/ipbes_global_assessment_report_summary_for_policymakers.pdf. s. 12.

²⁵ DAHAL, Sagar – HEINEN, Joel T.: A History of the Convention on International Trade in Endangered Species of Wild Fauna and Flora Implementation in Nepal. In: Diversity, Vol. 17, N. 5 (2025), s. 312. <https://doi.org/10.3390/d17050312> Pozri tiež: WIJNSTEKERS, Willem: The Evolution of CITES - 11th edition, 2018. s. 33.

Úskalia Dohovoru o medzinárodnom obchode s ohrozenými druhmi

CITES sa stal jedným z najúspešnejších medzinárodných nástrojov v oblasti ochrany prírody. V súčasnosti má vyše 180 zmluvných strán a zahŕňa približne 40 000 druhov rastlín a živočíchov. Tento dohovor za cieľ zabezpečiť, aby obchod s exemplármi chránených druhov prebiehal len v takej miere a za takých podmienok, aby nebolo ohrozené ich prežitie v prírode.²⁶ Nástrojom či mechanizmom uplatňujúcim sa pri napĺňaní cieľa je tak systém povolení, resp. certifikátov, ktoré štátne orgány musia vydávať alebo kontrolovať pri dovoze, vývoze či reexporte druhov zaradených do jeho príloh, podľa rozdielneho režimu obchodu v zmysle týchto príloh. Režim obchodovania funguje od úplného zákazu pri najohrozenejších druhoch až po regulovaný obchod pod podmienkou sledovania jeho vplyvov na populáciu. Možno ale povedať, že efektívnosť tohto systému je ale taktiež častokrát nedostatočná.

Osobitne zaujímavý pohľad na aplikačné problémy spojené s mechanizmami zavedenými CITES poskytuje štúdia autorov Smith a kol. z roku 2011, ktorá sa sústreďuje na vedecké hodnotenia, ktoré sú podľa CITES nevyhnutným predpokladom pre vydanie exportného povolenia k druhom zaradeným do Prílohy II, t. j. k tým, pri ktorých je obchod povolený iba za predpokladu, že neohrozí ich populácie v prírode. Títo autori sa zameriavajú na to, ako sa v praxi posudzuje vplyv medzinárodného obchodu na druhy zaradené do príloh CITES. Za uvádzania konkrétnych príkladov poukazujú pritom na to, že prax štátov je veľmi rozdielna a že vo veľkej miere naráža na nedostatok či nekonzistentnosť biologických dát, čoho výsledkom je nejednotné zhodnotenie rizika obchodu s takýmito druhmi a v konečnom dôsledku aj samotné oslabenie plnenia záväzkov plynúcich pre zmluvné strany z tohto dohovoru.²⁷

Rola moderných technológií pri ochrane biodiverzity

Limity existujúceho systému otvárajú však dvere pre iné možnosti, ktoré môžu v danej oblasti výrazne pomôcť a ktoré vedú v neposlednom rade tiež posilniť schopnosť štátov dodržiavať svoje záväzky.

V posledných desaťročiach možno len ťažko nájsť oblasť, ktorú by technologický vývoj obíšiel. Moderné technológie sa v mnohých aspektoch ukazujú ako užitočný

²⁶ Uvedený cieľ vyplýva už z jeho článku II. Predmetný článok delí druhy do troch kategórií zhrnutých v jednotlivých prílohách I až III (ods. 1 až 3 čl. II CITES), ktoré stanovujú rozdielny režim obchodu podľa stupňa ohrozenia jednotlivých druhov, pričom ods. 4 tohto článku stanovuje zmluvným stranám možnosť povoliť obchod s exemplármi druhov uvedených v prílohách iba vtedy, ak to bude v súlade s ustanoveniami s CITES. K tomu bližšie v: CITES, čl. II ods. 1 až 4.

²⁷ SMITH, Matthew et al.: Assessing the impacts of international trade on CITES-listed species: Current practices and opportunities for scientific research. In: *Biological Conservation*, Vol. 144, N. 1 (2011), s. 82 – 91. <https://doi.org/10.1016/j.biocon.2010.10.018>

pomocník aj v oblasti ochrany prírody. Na dôkaz slúži penzum situácií, kedy tieto dokázali preklenúť nedostatky tradičných mechanizmov a vniesť do praxe prvky presnosti a efektivity. Kedysi namáhavé terénne sčítavanie druhov a vizuálna kontrola je dnes v mnohom dopĺňaná alebo priamo nahrádzaná technickými, resp. digitálnymi riešeniami. Technológie prirodzene umožňujú získavať dáta v rozsahu a kvalite, ktoré boli kedysi nedosiahnuteľné. Prinášajú tiež možnosti reagovať na hrozby rýchlejšie a adresnejšie. Ich využívanie je tak v súčasnosti súčasťou monitorovania druhov, odhaľovania nelegálnych aktivít alebo aj kontroly medzinárodného obchodu ako kľúčového doplnku samotného CITES. Príklady z praxe rovnako ukazujú, že moderné technológie sú využiteľné aj v tejto oblasti ba dokonca ju zásadným spôsobom ovplyvňujú. *In concreto* možno uviesť aspoň niekoľko najvýraznejších príkladov.

Využívanie dronov a bezpilotných lietadiel je pozorovateľné pri monitorovaní nosorožcov v južnej Afrike či pri sčítavaní vtáčích kolónií v arktických oblastiach. Využitie modernej technológie zadováži presnejšie dáta a zároveň minimalizuje riziko rušenia zvierat v porovnaní s klasickými pozemnými metódami.²⁸ Ďalším príkladom sú satelitné systémy využívané na sledovanie pytlactva a odhaľovanie nelegálnej ťažby dreva.²⁹ Nemožno nespomenúť aj významný pokrok, ktorý priniesli genetické databázy a metóda DNA barcodingu. Táto metóda umožňuje identifikáciu druhov aj v kritických prípadoch, kedy by kontrola zlyhala. Typickým príkladom je odhaľovanie podvodov pri obchode s rybami a morskými plodmi.³⁰

Z istého uhla je azda ešte prekvapivejší posun, ktorý v tejto oblasti priniesla umelá inteligencia a strojové učenie. Algoritmy vedia totiž s vysokou presnosťou identifikovať ponuky ohrozených druhov na online platformách³¹ a odhaliť vzorce v

²⁸ ANDERSON, Karen – GONZALEZ, Felipe – GASTON, Kevin J.: Drones in ecology: ten years back and forth. In: *BioScience*, Vol. 75, N. 8 (2025), s. 664 – 680. <https://doi.org/10.1093/biosci/biafo69> Pozri tiež štúdiu: HUA, Martin A. et al.: Protecting endangered megafauna through AI analysis of drone images in a low-connectivity setting: a case study from Namibia. In: *PeerJ*, Vol. 10:e13779. <https://doi.org/10.7717/peerj.13779>

²⁹ TURNER, Woody et al.: Free and open-access satellite data are key to biodiversity conservation. In: *Biological Conservation*, Vol. 182, (2015), s. 173 – 176. <https://doi.org/10.1016/j.biocon.2014.11.048> Autori vo svojom článku pritom zdôrazňujú, že satelitná technológia zvyšuje naše chápanie globálnych zmien biodiverzity a zabezpečenie dostupnosti takýchto údajov sú pre výskumníkov a ochrancov prírody nevyhnutné na efektívne využívanie prírodných zdrojov.

³⁰ FILONZI, Laura et al.: Molecular Barcoding: A Tool to Guarantee Correct Seafood Labelling and Quality and Preserve the Conservation of Endangered Species. In: *Foods*, Vol. 12, N. 12 (2023). <https://doi.org/10.3390/foods12122420>

³¹ KUMAR, Sharan Kumar Jaya Agni Sathiesh: Detection of illegal wildlife trade using machine learning. In: *AIP Conference Proceedings*, Vol. 2790, N. 1 (2023). <https://doi.org/10.1063/5.0153664>

nelegálnom obchode s pangolínmi.³² V súčasnosti prekvitá nelegálny obchod s voľne žijúcimi živočíchmi a rastlinami na platformách elektronického obchodu, „dark webe“ a sociálnych sieťach. Obzvlášť znepokojujúca je skutočnosť, že k uvedeným miestam má jednoduchý prístup vysoký počet používateľov. Autori pod vedením E. Di Minina sa ale v tejto súvislosti domnievajú, že algoritmy strojového učenia vedia slúžiť ako vhodný nástroj prevencie, resp. minimalizovania takéhoto obchodu.³³ V neposlednom rade možno zmeniť využitie robotických a autonómnych systémov, ktoré sa dokážu dostať aj do pre človeka ťažko preniknuteľného prostredia a priniesť tak skutočne cenné dáta napríklad o stave populácií.³⁴

Medzinárodnoprávne výzvy využívania technológií pri ochrane biodiverzity

Otázka využívania moderných technológií v ochrane biodiverzity je nevyhnutne aj otázkou právnou.

V prvom rade je treba zdôrazniť, že vychádzajúc z podstaty medzinárodného práva verejného a vyššie analyzovaných dohovorov ako jeho prameňov, základné záväzky podľa CBD a CITES sú adresované výlučne štátom. Štát je teda subjektom, ktorý nesie primárnu zodpovednosť za dodržiavanie dohovorov.³⁵

Pri pohľade do aplikačnej praxe v danej oblasti možno ale naraziť na možné problémy či výzvy. Je totiž zrejmé, že kľúčové potrebné a vyššie zmienené technológie, či už v podobe satelitných systémov, algoritmov umelej inteligencie či genetických databázy, sú vyvíjané, vlastnené a v neposlednom rade spravované súkromnými subjektmi, ako napríklad technologickými spoločnosťami, výskumnými ústavmi alebo aj mimovládnyimi organizáciami. Tento v stručnosti zhrnutý problém vyvoláva niekoľko otázok, ktoré sú zastrešené pod otáznikom toho, do akej miery by malo byť právo s ohľadom na tak rýchly technologický vývoj (aj v environmentálnej oblasti) schopné reflektovať úlohu neštátnych aktérov. Vo vedeckej literatúre, nemenej z oblasti medzinárodného práva životného prostredia, už niekoľko rokov prebiehajú diskusie o tom, či a do akej miery možno adaptovať medzištátne záväzky tak, aby vznikli aj pre súkromné subjekty. Morgera poukazuje na skutočnosť, že medzinárodné právo tradične adresuje povinnosti štátom, no v praxi zásadnú rolu

³² CARDOSO, Anna Sofia et al.: Detecting wildlife trafficking in images from online platforms : A test case using deep learning with pangolin images. In: Biological Conservation, Vol. 279 (2023). <https://doi.org/10.1016/j.biocon.2023.109905>

³³ DI MININ, Enrico: Machine learning for tracking illegal wildlife trade on social media. In: Nature Ecology & Evolution, Vol. 2 (2018), s. 406–407. <https://doi.org/10.1038/s41559-018-0466-x>

³⁴ DAVIES, Zoe G. et al.: Robotics and Autonomous Systems for Environmental Sustainability, 2023. s. 6-8.

³⁵ Medzinárodné právo životného prostredia ako mnohé iné pododvetvia medzinárodného práva sú systémom zameraným na štát. K tomu pozri: SVÁK, Ján - MAREČEK, Lukáš: *Medzinárodné právo verejné a úvod do verejného medzinárodného práva*, 2024. s. 825.

zohrávajú aj súkromné spoločnosti. Možno súhlasiť že súčasné medzinárodné právo nedisponuje efektívnymi nástrojmi na reguláciu správania neštátnych aktérov, ktorých konanie má environmentálne dopady.³⁶ Tieto závery je pritom možno použiť aj v oblasti ochrany biodiverzity prostredníctvom technológií, kde štáty nesú právne záväzky, no už dnes potrebné *know-how* ovládajú prevažne súkromné osoby.

V tejto súvislosti osobitnou a možno kľúčovou otázkou je otázka zodpovednosti. Možno si predstaviť situáciu, kedy dron používaný na monitoring naruší prirodzené správanie zvierat alebo algoritmus AI nesprávne vyhodnotí dáta a dôjde k prehliadnutiu pytliackej aktivity, v dôsledku čoho dôjde k strate druhov, prípadne množstvo iných prirodzene neželaných situácií, pri ktorých sa naskytá príznačná právna otázka: kto nesie zodpovednosť?

V predmetnej oblasti je ale azda mimoriadne problematická. O to viac pri uvedomení si, že jednoznačné riešenie zatiaľ absentuje nielen na medzinárodnej úrovni, ale aj na úrovni vnútroštátnej. Právne poriadky dodnes zápasia s tým, ako uchopiť škody spôsobené modernými technológiami, a to ako v režime súkromnoprávnej, tak verejnoprávnej zodpovednosti.³⁷ Obdobná dilema je tak prirodzene premietnutá aj do medzinárodného práva, kde tradičný režim zodpovednosti štátov vychádza z pričítateľnosti konania štátu v zmysle Návrhu článkov o zodpovednosti štátov za medzinárodne protiprávne správanie z roku 2001.³⁸ Pričítateľnosť konania súkromnej spoločnosti, ktorá prevádzkuje monitoring alebo poskytuje technické riešenie štátu je ale prinajmenšom otázna, poťažmo problematická.

Záver

Aj keď súčasný medzinárodnoprávny režim ochrany biodiverzity, reprezentovaný v kontexte tohto príspevku najmä CBD a CITES, síce vytvoril základné piliere medzinárodnoprávnej regulácie v tejto oblasti, jeho efektivita je limitovaná, a to najmä rámcovou a vágne formulovanou povahou záväzkov, ako aj obmedzenými mechanizmami kontroly. Ako významný nástroj na preklenutie týchto problémov sa v praxi ukazujú moderné technológie. Ich využívanie avšak otvára škálu právnych otázok. Možno konštatovať, že otázky spojené so zodpovednosťou pri využívaní moderných technológií v ochrane biodiverzity zatiaľ nemožno uspokojivo zodpovedať. Existujúca medzinárodnoprávna úprava pochopiteľne nebola koncipovaná s ohľadom na rýchlo rastúcu digitalizáciu. Z uvedeného dôvodu poskytujú len čiastočné riešenia. Avšak už samotná identifikácia a pomenovanie

³⁶ MORGERA, Elisa: *Corporate Environmental Accountability in International Law*, 2020. s. 38.

³⁷ K tomu pozri: MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: *Právo a umelá inteligencia*, 2024. s. 116 – 134.

³⁸ Draft articles on responsibility of States for international wrongful acts, Report of the International Law Commission, Yearbook of the International Law Commission: 2001, vol. II, (A/56/10).

problémov, ktoré rozvoj technológií vyvoláva, predstavuje prvý krok k ich neskoršiemu uchopeniu. Nemožno spochybniť, že moderné technológie predstavujú dôležitý príspevok k záväzkom podľa CITES či CBD, nakoľko, ako je rozoberané vyššie, umožňujú efektívnejší monitoring, kontrolu a odhaľovanie nelegálnych aktivít, čím v konečnom dôsledku zvyšujú šance na dodržiavanie medzinárodných záväzkov. Príspevok tak poukázal na potrebu uvažovať o tom, ako môže medzinárodné právo flexibilnejšie reagovať na technologický rozvoj v oblasti ochrany biodiverzity a posilniť schopnosť existujúcich režimov dosahovať svoje ciele.

Zoznam použitej literatúry

1. ANDERSON, Karen – GONZALEZ, Felipe – GASTON, Kevin J.: Drones in ecology: ten years back and forth. In: *BioScience*, Vol. 75, N. 8 (2025), s. 664 – 680. <https://doi.org/10.1093/biosci/biaf069>
2. CARDOSO, Anna Sofia et al.: Detecting wildlife trafficking in images from online platforms : A test case using deep learning with pangolin images. In: *Biological Conservation*, Vol. 279 (2023). <https://doi.org/10.1016/j.biocon.2023.109905>
3. CONVENTION ON BIOLOGICAL DIVERSITY. Strategic Plan for Biodiversity 2011-2020, including Aichi Biodiversity Targets, 2020. [online]. Dostupné na internete dňa 28.09.2025: <https://www.cbd.int/sp/targets>.
4. DAHAL, Sagar – HEINEN, Joel T.: A History of the Convention on International Trade in Endangered Species of Wild Fauna and Flora Implementation in Nepal. In: *Diversity*, Vol. 17, N. 5 (2025), s. 312. <https://doi.org/10.3390/d17050312>
5. DAVIES, Zoe G. et al.: Robotics and Autonomous Systems for Environmental Sustainability. UK-RAS, 2023. 24 s. ISSN 2398-4422. doi: 10.31256/WP2023.4
6. DI MININ, Enrico: Machine learning for tracking illegal wildlife trade on social media. In: *Nature Ecology & Evolution*, Vol. 2 (2018), s. 406– 407. <https://doi.org/10.1038/s41559-018-0466-x>
7. Dohovor o biologickej diverzite (Convention on Biological Diversity) 1760 UNTS 79.
8. Dohovor o medzinárodnom obchode s ohrozenými druhmi voľne žijúcich živočíchov a rastlín (Convention on International Trade in Endangered Species of Wild Fauna and Flora) 993 UNTS 243.
9. Draft articles on responsibility of States for international wrongful acts, Report of the International Law Commission, Yearbook of the International Law Commission: 2001, vol. II, (A/56/10).
10. EKARDT, Felix et al.: Legally binding and ambitious biodiversity protection under the CBD, the global biodiversity framework, and human rights law. In: *Environmental Sciences Europe*, Vol. 35, N. 80 (2023). <https://doi.org/10.1186/s12302-023-00786-5>

11. FILONZI, Laura et al.: Molecular Barcoding: A Tool to Guarantee Correct Seafood Labelling and Quality and Preserve the Conservation of Endangered Species. In: *Foods*, Vol. 12, N. 12 (2023). <https://doi.org/10.3390/foods12122420>
12. HUA, Martin A. et al.: Protecting endangered megafauna through AI analysis of drone images in a low-connectivity setting: a case study from Namibia. In: *PeerJ*, Vol. 10:e13779. <https://doi.org/10.7717/peerj.13779>
13. IPBES. The global assessment report on biodiversity and ecosystem services. Summary for Policy Makers. Bonn, 2019. [online]. Dostupné na internete dňa 28.09.2025: https://files.ipbes.net/ipbes-web-prod-public-files/inline/files/ipbes_global_assessment_report_summary_for_policymakers.pdf.
14. Kartagenský protokol o biologickej bezpečnosti, 2226 UNTS 208, UN Doc. UNEP/CBD/ExCOP/1/3.
15. KLEMM, Cyrille de – SHINE, Clare: *Biological Diversity Conservation and the Law: Legal Mechanisms for Conserving Species and Ecosystems*. Gland: IUCN, 1993. 292 s. ISBN 2-8317-0192-9.
16. KOH, Niak – ITUARTE-LIMA, Claudia – HAHN, Thomas: Mind the Compliance Gap: How Insights from International Human Rights Mechanisms Can Help to Implement the Convention on Biological Diversity. In: *Transnational Environmental Law*, Vol. 11, č. 1 (2022), s. 39 – 67. doi:10.1017/S2047102521000169
17. KUMAR, Sharan Kumar Jaya Agni Sathiesh: Detection of illegal wildlife trade using machine learning. In: *AIP Conference Proceedings*, Vol. 2790, N. 1 (2023). <https://doi.org/10.1063/5.0153664>
18. MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: *Právo a umelá inteligencia*. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 244 s. ISBN 978-80-7160-715-1.
19. MOORE, Kimberly C.: *The Case for the Legal Protection of Animals. Humanity's Shared Destiny with the Animal Kingdom*. Cham: Palgrave Macmillan, 2023. 334 s. ISBN 978-3-031-46064-7.
20. MORGERA, Elisa – TSIOUMANI, Elsa: Yesterday, Today, and Tomorrow: Looking Afresh at the CBD. In: *Yearbook of International Environmental Law*, Vol. 21, N. 1 (2010), s. 3 – 40. <https://doi.org/10.1093/yiel/yvr003>
21. MORGERA, Elisa: *Corporate Environmental Accountability in International Law*. 2nd edition. Oxford: OUP, 2020. 318 s. ISBN 978-0-19-873804-6.
22. Nagojský protokol o prístupe ku genetickým zdrojom a spravodlivom a rovnocennom využívaní prínosov vyplývajúcich z ich využívania, 3008 UNTS 3.
23. PLESNÍK, Jan: Ekosystémové služby nejsou anonymní: Význam organismů pro fungování ekosystémů. In: *Ochrana přírody*, Roč. 67, č. 5 (2012), s. 21 – 25.

24. SECRETARIAT OF THE CONVENTION ON BIOLOGICAL DIVERSITY. Global Biodiversity Outlook 3. Montréal, 2010. ISBN 92-9225-220-8. [online]. Dostupné na internete dňa 28.09.2025: <http://www.cbd.int/GBO3>.
25. SECRETARIAT OF THE CONVENTION ON BIOLOGICAL DIVERSITY. Global Biodiversity Outlook 5. Summary for Policy Makers. Montréal, 2020. ISBN 9789292256883. [online]. Dostupné na internete dňa 28.09.2025: <https://www.cbd.int/gbo/gbo5/publication/gbo-5-spm-en.pdf>.
26. SMITH, Matthew et al.: Assessing the impacts of international trade on CITES-listed species: Current practices and opportunities for scientific research. In: Biological Conservation, Vol. 144, N. 1 (2011), s. 82 – 91. <https://doi.org/10.1016/j.biocon.2010.10.018>
27. STEJSKAL, Vojtěch: Právni prostředky ochrany biologické rozmanitosti. In: České právo životního prostředí, Č. 29 (2011), s. 6–12.
28. STEJSKAL, Vojtěch: Úvod do právní úpravy ochrany přírody a péče o biologickou rozmanitost. Praha: Linde, 2006. 591 s. ISBN 80-720-1609-1.
29. SVÁK, Ján - MAREČEK, Lukáš: Medzinárodné právo verejné a úvod do verejného medzinárodného práva. Bratislava: Wolters Kluwer, 2024. 972 s. ISBN 978-80-571-0704-0.
30. TURNER, Woody et al.: Free and open-access satellite data are key to biodiversity conservation. In: Biological Conservation, Vol. 182, (2015), s. 173 – 176. <https://doi.org/10.1016/j.biocon.2014.11.048>
31. UNITED NATIONS. UN Report: Nature's Dangerous Decline 'Unprecedented'; Species Extinction Rates 'Accelerating', 2025. [online]. Dostupné na internete dňa 28.09.2025: <https://www.un.org/sustainabledevelopment/blog/2019/05/nature-decline-unprecedented-report/>.
32. UNODC. World Wildlife Crime Report 2024: Trafficking in Protected Species (Vienna: United Nations publications, 2024). [online]. Dostupné na internete dňa 28.09.2025: https://www.unodc.org/documents/data-and-analysis/wildlife/2024/Wildlife2024_Final.pdf.
33. Vyhláška ministra zahraničných vecí č. 15/1988 Zb. o Viedenskom dohovore o zmluvnom práve.
34. WIJNSTEKERS, Willem: The Evolution of CITES - 11th edition. Budakeszi: International Council for Game and Wildlife Conservation, 2018. 1022 s.
35. WIJNSTEKERS, Willem: The Evolution of CITES - 9th edition. Budakeszi: International Council for Game and Wildlife Conservationk, 2011. 937 s. ISBN 978-963-88778-4-0.
36. XIANG, YIBIN – MEEHAN, Sandra: Financial Cooperation, Rio Conventions and Common Concerns. In: Review of European Community and International Environmental Law, Vol. 14, N. 3 (2005), s. 212 – 224.

Kontaktné údaje

Mgr. Petra Paluchová

petra.paluchova@flaw.uniba.sk

Katedra medzinárodného práva a medzinárodných vzťahov

Univerzita Komenského v Bratislave

Právnická fakulta

Sekcia správneho práva
Využívanie umelej inteligencie pri rozhodovaní vo
verejnej správe

NIEKOĽKO ÚVAH O VYUŽÍVANÍ UMELEJ INTELIGENCIE V ROZHODOVACÍCH PROCESOCH VO VEREJNEJ SPRÁVE¹

SEVERAL CONSIDERATIONS ON THE USE OF ARTIFICIAL INTELLIGENCE IN DECISION-MAKING PROCESSES IN PUBLIC ADMINISTRATION

Marián Vrabko²

Abstrakt: Článok pojednáva o základných pojmoch vo verejnej správe a ich právnej regulácii u nás. Ďalej autor poukazuje na právnu reguláciu pri rozhodovacích procesoch, ktorá je urobená na úrovni Európskej únie. Veľkou časťou príspevku sú špecifické inštitúty správneho práva a verejnej správy, ktoré bude nevyhnutné upravovať pre potreby využívania umelej inteligencie v rozhodovacích procesoch vo verejnej správe vrátane nových foriem činnosti verejnej správy.

Kľúčové slová: Verejná správa, rozhodovacie procesy vo verejnej správe, správna úvaha, právne pohyblivé pojmy, umelá inteligencia, formy činnosti verejnej správy, verejný poriadok.

Abstract: The article deals with basic concepts in public administration and their legal regulation in our country. Furthermore, the author points out legal regulation in decision-making processes, which is made at the European Union level. A large part of the paper is the specific institutes of administrative law and public administration, which will be necessary to regulate the needs of the use of artificial intelligence in decision -making processes in public administration, including new forms of public administration activities.

Key words: Public administration, decision -making processes in public administration, Correct consideration, legal moving concepts, Artificial intelligence, forms of public administration activity, public order

¹ Článok je podporovaný grantom APVV-24-0543: Energetická hospodárnosť budov v SR, zlepšenie energetického a právneho rámca vo svetle nových požiadaviek EÚ.

² Univerzita Komenského v Bratislave, Právnická fakulta.

Úvod

V úvode nebudeme polemizovať do akej miery je vhodné či nevhodné využívať umelú inteligenciu v rozhodovacích procesoch vo verejnej správe. Faktom ostáva, že vývoj v spoločnosti nás naučil, že ju budeme využívať, či sa nám to páči alebo nie. Dôležité je, aby jej právna regulácia bola ustanovená tak, aby nám umelá inteligencia slúžila, a aby zohľadňovala práve tie špecifiká správneho práva, ktoré je vhodné alebo žiadúce využiť pri aplikácii administratívnoprávnych noriem.

Pojem umelá inteligencia nie je pojem právny, ale technický. Z tohto dôvodu je vhodné, aby sme vedeli čo je jeho obsahom a prečo sa tak rýchlo rozvíja. Prof. Bieliková z STU hovorí prečo umelá inteligencia tak dobre funguje. Uvádza, že jej úspech stojí na troch pilieroch:

- prvým je obrovské množstvo dát,
- druhým je zásadný posun v algoritmoch od symbolickej ku subsymbolickej umelej inteligencii,
- tretím je ľudský talent³.

Z týchto technologických údajov je zrejmé, že sa im musíme venovať aj v práve a zabezpečiť ich právnu reguláciu.

Pre jednoznačné pochopenie problematiky je nevyhnutné uskutočniť analýzu právnej úpravy v podmienkach Slovenska a súčasne aj Európskej únie, ktorej sme členom. Na národnej úrovni je nevyhnutné sledovať rozhodovacie procesy s ich špecifikami v našej verejnej správe.

Súčasný právny stav

Začal by som s charakteristikou obsahu niekoľkých pojmov, ktoré traktujem v príspevku. **Základným pojmom je verejná správa.** V súlade s národnými predpismi môžeme konštatovať, že obsah tohto pojmu je ustálený a podobný úijnnému vymedzeniu. Ide o štruktúru, ktorá má obsahovú i formálnu stránku alebo inak uvedené dynamickú a statickú stránku. Statickú stránku predstavuje štruktúra orgánov a dynamickú okrem iných aj rozhodovacia činnosť. Pri štruktúre orgánov ide o nenáhodné usporiadanie dopredu ustanovených prvkov a ich špecifické vzťahy a druhy orgánov. Rozhodovaciu činnosť predstavuje výber z ponúkaných možností foriem činnosti.

Základný právny rámec statickej stránky verejnej správy tvorí ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení ústavných zákonov, ktorá v čl. 46 uvádza pojem verejná správa, ale nevymedzuje ho. V čl. 64 uvádza, že „základom územnej samosprávy je obec. Územnú samosprávu tvorí obec a samosprávny kraj“⁴.

³ Denník N, sobota, 18. 10. 2025. s. 15.

⁴ VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava: C.H.Beck, 2025, s. 2 a n.

Tieto a nasledujúce ustanovenia, sú vykonávané a konkretizované v zákonoch, ktorými sú najmä :

- z. č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov,
- z. č. 302/2001 Z. z. o samospráve vyšších územných celkov (zákon o samosprávnych krajoch) v znení neskorších predpisov,
- z. č. 221/1996 o územnom a správnom usporiadaní Slovenskej republiky v znení neskorších predpisov,
- z. č. 281/1997 Z. z. o vojenských obvodoch a zákon, ktorým sa mení zákon NR SR č. 222/1996 Z. z. o organizácii miestnej štátnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- z. č. 305/2003 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej správy a o zmene a doplnení niektorých zákonov (zákon o e- Governmente),
- z. č. 18/2017 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých údajov a mnoho ďalších zákonov.

Druhou stranou mince pojmu verejná správa je rozhodovanie a pojem rozhodovacie procesy, alebo inak dynamická stránka. V duchu nižšie uvedených zákonov môžeme konštatovať, že rozhodovacie procesy predstavujú nenáhodný výber z viacerých alternatív, ktoré prechádzajú právne ustanovenými fázami.⁵

Základný národný právny rámec výberu vhodných procesov tvorí ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení ústavných zákonov, ktorá v čl. 108 uvádza, „že Vláda Slovenskej republiky je vrcholným orgánom výkonnej moci“ z čoho vyplýva, že v štruktúre orgánov štátnej správy stojí najvyššie a pod ňou stojí celá štruktúra orgánov štátnej správy, od ústredných a ostatných ústredných orgánov štátnej správy, až po miestne orgány štátnej správy s ich subordináciou, v ktorej prebiehajú rozhodovacie procesy. Rozhodovacie procesy prebiehajú aj v štruktúre samosprávy. Vykonávacie predpisy, k týmto ustanoveniam sú najmä:

- z. č. 71/1976 Zb. o správnom konaní (správny poriadok), v znení neskorších predpisov,
- z. č. 162/2015 Z. z. správny súdny poriadok (SSP), v znení neskorších predpisov a osobitné zákony, ktorými sú regulované jednotlivé druhy konaní.

V podmienkach UK reguluje využívanie AI Smernica rektora UK č. 2/2024 o používaní nástrojov umelej inteligencie na Univerzite Komenského v Bratislave. Z uvedenej Smernice rektora UK vyberám konkrétne ustanovenie čl. II a nasl. z ktorého vyplýva: „používať nástroje UI (umelá inteligencia) na priame vypracovanie celých textov, formulovanie záverov a akýchkoľvek tvrdení, ktoré majú byť výsledkom samotnej práce, môže byť akademickým podvodom“. Odporúčané spôsoby citovania sú uvedené v prílohe. Je to vážna výstraha pre akademickú samosprávu, ktorú musíme sledovať a zohľadňovať aj vo vzťahu k študentom.

⁵ VRABKO, M. a kol.: Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C.H. Beck, 2019, s. 7 a n.

Právna regulácia využívania umelej inteligencie AI (ei: ai:) nemá zatiaľ osobitný národný právny rámec. Jej únijský právny rámec je v súlade s našou Ústavou najmä čl. 1, čl. 2, čl. 7, ako aj ďalšími článkami Ústavy vymedzený v únijskom akte o umelej inteligencii. Všeobecnú charakteristiku sme prevzali z charakteristiky Európskej Únie (EÚ), ktorá uvádza, že ide o súbor technológií, ktoré dokážu vykonávať úlohy, ktoré si zvyčajne vyžadujú ľudskú inteligenciu, ktorá spočíva v: učení sa, rozpoznávaní vzorcov, spracovávaní prirodzeného jazyka a rozhodovanie.

Pre úplnosť je potrebné pripomenúť, že sa pripravuje aj národný rámec pre využívanie AI v podobe zákona „O organizácii štátnej správy v oblasti umelej inteligencie“.

Využívanie AI v našich podmienkach som prevzal od Chat gpt a je nasledovné:

1 Automatizácia rutinných úkonov – spracovanie žiadostí a administratívnych procesov

2 Podpora rozhodovania – analýzy dát, predikatívne modelovanie, odporúčacie systémy

3 interakcia s občanmi – chaty digitálne asistentky, personalizované služby.⁶

Ide o tri základné okruhy ktorým sa budeme v budúcnosti venovať.

Právny rámec na nadnárodnej úrovni, ako som už uviedol, je akt EÚ, ktorým je:

Akt o umelej inteligencii (Artificial Intelligence Act), ktorý bol prijatý v roku 2024.

Je to nariadenie Európskeho parlamentu, ktoré je platné od 1. septembra 2024 a jeho ustanovenia majú vstúpiť do účinnosti postupne v priebehu nasledujúcich 6 až 36 mesiacov. Akt ako celok by mal nadobudnúť účinnosť 1. augusta 2026.

Tento Akt o AI klasifikuje systémy AI podľa rizikovosti nasledovne: minimálne, obmedzené, vysoké a nepripustné riziko. Ustanovuje teda štyri úrovne rizík, ktorým zodpovedajú rôzne pravidlá užívania. Osobitne sú ustanovené špecifické požiadavky na systémy AI s vysokým rizikom, ktoré sa môžu využívať aj vo verejnej správe napr. v oblasti migrácie, justície alebo sociálneho zabezpečenia. Tu bude nevyhnutné v počiatočných využívať určené vopred ustanovené formy činnosti, tak aby zohľadňovali mieru rizika.

Pre využitie vo verejnej správe sú zaujímavé systémy s vysokou mierou rizika, tieto však môžu mať negatívny dopad na základné práva alebo bezpečnosť a sú rozdelené do dvoch kategórií. Pre chod verejnej správy je osobitne zaujímavá druhá kategória, kde je osem oblastí, ktoré musia byť registrované v databáze EÚ. Bližšie sa tejto problematike venuje európsky Akt o umelej inteligencii.

V našich podmienkach to budú najmä nasledujúce činnosti, ktorým sa pri využívaní umelej inteligencie pri rozhodovacích procesoch vo verejnej správa budeme musieť osobitne venovať:

Rozhodovacie procesy

⁶ ChatGPT. OpenAI, 20 Sept. 2025, chat.openai.com. Transcript of conversation with the author. Videné 20.09 2025.

Poskytovanie služieb občanom
Prediktívne analýzy a plánovanie
Administratívna činnosť.

Výhodami užívania týchto činností bude: rýchlosť, efektívnosť, objektivita, nekorupčnosť.

Samozrejme, že tento projekt má aj nevýhody, ktorými sú: hrozba diskriminácie, nedostatočná kontrola, problémy s marginalizovanými skupinami, existencia správnej úvahy, existencia právne pohyblivých pojmov, alebo inak nazývaných právne neurčitých pojmov a ďalšie skutočnosti, ktoré uvediem neskôr.

Okrem regulácie rizík je pre verejnú správu v súlade s naším vymedzením samotného pojmu verejná správa dôležité aj vymedzenie štruktúry orgánov, ktoré sa jej na úrovni EÚ budú venovať. Ide o:

- Úrad pre AI zriadený v rámci Európskej Komisie na presadzovanie spoločných pravidiel v celej EÚ
- Vedecký panel nezávislých odborníkov na podporu činností v oblasti presadzovania práv
- Rada pre AI so zástupcami členských štátov s cieľom riadiť a pomáhať Komisii a členským štátom pri jednotnom a účinnom uplatňovaní Aktu AI
- Poradné fórum pre zainteresované na poskytovanie technických odborných znalostí pre AI a Komisií.

Z pohľadu realizácie a aplikácie správneho práva bude nevyhnutné hovoriť o dvoch veľkých skupinách okruhov pojmov. Prvú budú tvoriť pojmy, ktorých obsah bude jednoznačne vymedzený, bez možnosti AI zasahovať do ich podstaty. Druhú veľkú skupinu budú tvoriť pojmy, ktoré fyzické osoby pri aplikácii právnych predpisov bežne využívajú, no ich obsah nie je jednoznačne vymedzený, hranice zákonnosti pri ich aplikácii nie sú dané alebo sú vágne. Tieto hranice môže AI v aplikačnom procese využiť, ale aj zneužiť, a to až tak, že sa obsah stane nekontrolovateľný. Aby sme predišli problémom budeme sa musieť opäť vrátiť ku klasifikácii foriem činnosti, na právne dovolené a právne prikázané, prípadne právne zakázané.

Problémové inštitúty správneho práv vo verejnej správe

Dovoľte mi niekoľko slov k tej druhej skupine pojmov, ide o tie ktorých obsah nie je jednoznačne vymedzený, ale verejná správa ich bežne používa. **Jedným z prvých je správna úvaha.** Správna úvaha (správne uváženie) je inštitút, ktorý je ozdobou verejnej správy a správne orgány ho za ustanovených podmienok môžu využívať vo svojej činnosti. Verejná správa využíva správne uváženie zvyčajne tam, kde chce obmedziť tvrdosť zákona, odstrániť alebo posunúť v rámci možností bariéry v konaní, či umožniť subjektom, ktoré rozhodujú, alebo účastníkom konania, viac zohľadniť miestnu situáciu z pohľadu vecného, časového miestneho aj personálneho. Správna

úvaha však musí mať presne ustanovené hranice, alebo inak ustanovené medze zákona za ktoré sa nesmie nikdy dostať. A to platí aj pre AI, lebo čo AI urobí v medziach zákona, bude zákonné konanie či rozhodnutie, a naopak ak pôjde za hranice zákona, AI urobí nezákonný krok či vydá nezákonné rozhodnutie. Tu bude väčší priestor pre odstránenie ľudského vplyvu, ale naopak bude tu väčšie riziko neukontrolovania AI.⁷ To ale neznamená, že sa nevyhneme využívaniu správnej úvahy pri tvorbe rozhodnutí AI. To využívanie musí však byť zákonné, primerané, náležité a vhodné.

Osobitnú skupinu tvoria právne pohyblivé alebo právne neurčité pojmy. V úvode tejto úvahy je potrebné uviesť, že právne pohyblivé alebo právne neurčité pojmy nepredstavujú svojou podstatou správne uváženie. Aj právne pohyblivé pojmy pripúšťajú zvažovanie príslušných orgánov vo veciach časových, funkčných či personálnych. Na rozdiel od správneho uváženia nemajú však zákonom či podzákonným predpisom fixne ustanovené hranice či medze zákona, za ktoré subjekt, ktorý rozhoduje nemôže ísť. Klasickým príkladom takého pojmu je pojem **verejný záujem**. Aj obsah tohto pojmu je zvyčajne časovo, funkčne, či personálne determinovaný. Orgán, ktorý rozhoduje má však vždy povinnosť zvážiť okolnosti, ktoré budú ovplyvňovať jeho konanie či rozhodnutie, nemá však striktne ustanovené hranice za ktoré nemôže ísť. Jeho povinnosťou je však zohľadňovať **verejný záujem**, ktorý je časovo, miestne i vecne premenný. Obsah tohto pojmu máme zvyčajne v každom zákone vymedzený osobitne pre potreby tohto zákona, ale máme aj ústavný zákon č. 357/2004 o ochrane verejného záujmu pri výkone funkcií verejných funkcionárov, kde je jednoznačne uvedené čo je verejný záujem. Podľa tohto zákona je verejný záujem taký záujem, ktorý prináša majetkový prospech alebo iný prospech všetkým, alebo mnohým občanom. S ohľadom na to, že ide o ústavný zákon vyplýva z neho, že žiadny neústavný „obyčajný zákon“ by nemal ísť nad rámec tohto vymedzenia. Vyplýva to z ponímania sily formálnych prameňov práva, kde Ústava a ústavné zákony majú najväčšiu právnu silu.

Pri využití AI je tu opäť hrozba diskriminácie, svojvoľného konania, vydania nenáležitého rozhodnutia alebo takého, ktoré vôbec nezohľadní verejný záujem, ktorého obsah sa v priebehu konania modifikoval, prípadne úplne zmenil. Tu musíme dať pozor, aby sme zákony prirodzeného výberu nenahrádzali inteligentným plánovaním a nevytvárali umelé neovládateľné monštrá. Tak ako nás na to upozorňuje historik Harari.⁸

⁷ O tom, že je to možné svedčí film Simulátor, ktorý odvysielala Slovenská televízia. V uvedenom filme sa objavuje „Oddelenie pre vynucovanie poslušnosti umelej inteligencie“, čo signalizuje, že táto hrozba tu je, lebo simulátor získal toľko autonómie, že sa dokázal nekontrolovane zapájať do života spoločnosti aj jednotlivcov.

⁸ Yuval Noah Harari: Sapiens stručná história ľudstva. s. 382.

Ďalším zásadným pojmom a aj inštrumentom vo verejnej správe sú rozhodovacie procesy vo verejnej správe so svojimi štádiami a charakteristickými črtami. Rozhodovacích procesov vo verejnej správe je veľa, a preto je aj množstvo kritérií na ich delenie. My v prvom rade vydelíme tie rozhodovacie procesy, ktoré nie sú právom regulované. Vychádzame z ďalších možných delení, že právom regulované môžu byť štátnosprávne a samosprávne.⁹ Potom nám vychádza, že AI sa môže venovať obom druhom rozhodovacích procesov za predpokladu, že budú právom regulované. Právna regulácia predpokladá úpravu metód a najmä foriem činnosti verejnej správy. Otázne ostáva či AI dovoľíme v tých rozhodovacích procesoch vo verejnej správe využívať aj právne doktríny. Napr. neznalosť práva neospravedlňuje za súčasnej znalosti, že marginalizované skupiny obyvateľstva nemajú prístup k AI a ak aj majú, tak ju niekedy odmietajú.

Podstatnou otázkou ostáva do akej miery bude AI využívať judikatúru súdov. Je veľmi pravdepodobné, s ohľadom na ich európsky charakter, že ak bude dbať o to, aby pri judikatúre súdov, najmä z EÚ, ale nielen tých, bolo uvedené, že daný judikát súdu je pre AI záväzný. Podstatou judikátu je, že ide o nové rozhodnutie v danej veci a z dôvodu novosti sa stáva záväzným pre ostatných. Ďalej musíme jednoznačne uviesť či AI bude môcť v danej veci aj zohľadňovať miestne podmienky, alebo len kopírovať smerodajný judikát.

S týmto problémom úzko opäť súvisí aj skutočnosť aké formy činnosti bude AI vydávať, lebo formy činnosti podľa Správneho poriadku nie sú identické s tými, ktoré pozná Správny súdny poriadok, a tým je ohrozený kontrolný mechanizmus vo verejnej správe prostredníctvom správnych súdov. Ide napríklad o opatrenie, ktoré je podľa Správneho súdneho poriadku (ďalej len SPP) pripodobňované k rozhodnutiu v správnom konaní, čo správny poriadok nepozná. Naopak SSP nepozná toľko foriem činnosti ako Správny poriadok.

Osobitným problémom bude rozhodovanie vo vzťahu k marginalizovaným skupinám ľudí, alebo bezdomovcom, keď niektorí z nich nemajú možnosť pracovať s AI alebo záujem, alebo ju ignorujú, žiaľ objavujú sa aj takí, ktorí nevedia čítať. Stáva sa, že najmä územná samospráva v bagatelných veciach radšej nevydáva záporné rozhodnutia, ako by mala získať do svojho rozpočtu dlžníkov, ktorí svoj dlh nikdy neuhradia, a tak územná samospráva radšej nezaťažuje svoj rozpočet nevymožiteľnými finančnými pohľadávkami.

Z pohľadu foriem činnosti bude nevyhnutné definitívne oddeliť obsah pojmov princípy v práve ako vedúce ideí, ktoré sa dotýkajú práva ako celku od procesných zásad v konaní, ktoré sa budú využívať pri rozhodovacích procesoch vo verejnej správe. Procesné zásady bude nevyhnutné vnímať ako základné interpretačné pravidlá vo verejnej správe.

⁹ TÓTHOVÁ, K.: Rozhodovacie procesy v štátnej správe, Bratislava. Vydavateľstvo Obzor, s. 56.

Špecifickým problémom je delba práva na súkromné a verejné, ktorá je v rôznych krajinách EÚ rôzna. S ohľadom na úijnú a národnú judikatúru sa AI bude musieť viac zaujímať spolu s nami o tzv. odvetvové delenie práva a nezohľadňovať delenie práva na súkromné a verejné. Máme na mysli delenie práva napr. na zdravotnícke právo, pozemkové právo, právo v energetike a pod. Toto nové delenie práva obsahuje v sebe prvky súkromného a verejného práva, ktoré zmiešava. Veď si len predstavme porovnanie správneho trestania napr. v Poľsku a u nás. V Poľsku prerokúvajú priestupky súdy a u nás ide o verejnoprávne delikty, ktoré prejednávajú orgány štátnej správy a územnej samosprávy, za istých okolností pri prenesenom výkone štátnej správy to môžu robiť aj fyzické alebo právnické osoby. Pri porovnávaní práva budeme ďalej pokračovať a uvedieme opäť príklad z Poľska, kde súdy môžu za niektoré druhy priestupkov uložiť aj trest odňatia slobody. U nás orgány verejnej správy vo verejnoprávnom konaní nie.

Uplatňovanie zodpovednosti pri rozhodovacích procesoch vo verejnej správe bude vyžadovať dlhodobé riešenia. Napríklad AI rozhodne zákonne, ale nesprávne v rozpore so zdravým rozumom, ako bolo uvedené v jednom z judikátov Najvyššieho súdu SR, ktorý preskúmaval rozhodnutie verejnej správy. Sudcovia Najvyššieho súdu SR, teraz by to bol Najvyšší správny súd, rozhodli rozhodnutie verejnej správy zrušiť, konštatovali, že boli porušené právne predpisy, verejná správa zle uplatnila správnu úvahu a navyše rozhodnutie odporovalo zdravému rozumu. Výška pokuty za spáchaný priestupok na železničnej stanici bola pre dvoch dôchodcov, manželov, likvidačná. Zároveň odporučili dôchodcom uplatniť si náhradu vzniknutej škody v občianskom súdnom konaní. Otázka v našom prípade by znela, ak by rozhodla AI, kto uhradí škodu a ako sa bude postupovať.

Jedným z ďalších problémom Slovenska pri zodpovednostných vzťahoch bude prenesený výkon štátnej správy na obce či fyzické alebo právnické osoby. Slovensko je rurálna krajina s veľkým počtom malých sídiel, čo v praxi znamená, že štát nebude mať možnosť zabezpečiť rovnaký výkon správy vo všetkých sídlach. Niektoré obce však nesúhlasia s preneseným výkonom, a to napriek tomu, že originálny výkon nie sú schopné realizovať napr. z personálnych dôvodov. Napr. nedostatok kvalifikovaných pracovníkov.

Zo všetkými vyššie uvedenými problémami úzko súvisí špecifický problém správneho práva, ktorým je veľký počet podzákonných predpisov, ktorí podľa vyjadrenia funkčne starších kolegov neustále stúpa.

Záver

AI v rozhodovacích procesoch sa za ustanovených podmienok môže stať dobrým pomocníkom, ale pri nekontrolovanom procese zlým pánom tak, ako to poznáme v prípade ohňa. Pre zvládnutie tohto procesu bude nevyhnutné akceptovať úijnú

legislatívu, ale v našich podmienkach prijať aj národnú legislatívu, ktorá zohľadní naše národné špecifiká. Národná legislatíva samozrejme nemôže ísť nad rámec únijnej ani smerovať proti nej. V národnej legislatíve, ktorá bude regulovať využívanie AI, musíme dôsledne plniť nasledovné úlohy:

Bude nevyhnutné ustanoviť orgány, ktoré sa tejto problematike budú venovať na celoštátnej úrovni.

Rozlišovať zákony a podzákonné predpisy, pri podzákonných predpisoch bude nevyhnutné znížiť ich počet, najmä v tých prípadoch keď podzákonné predpisy nebudú mať celoštátnu pôsobnosť. Vytvoriť algoritmy postupov orgánov verejnej správy pri tých formách činnosti, ktoré budú jednoznačne zadefinované. S tým úzko súvisí nové rozlišovanie foriem činnosti vo verejnej správe na dovolené, prikázané a zakázané.

Vo vzťahu k marginalizovaným a vylúčeným skupinám bude nevyhnutné začať vzdelávanie z ohľadom na to, že jeho výsledky sa nedostavia v tom volebnom období keď sa s nimi začalo, ale až oveľa neskôr.

Bude nevyhnutné si uvedomiť, že použitie AI v konaní nie je novým konaním, ale ide len o novú formu činnosti.

Pri využívaní AI bude nevyhnutné ustanoviť nové algoritmy pri rozhodovacích procesoch, najmä v tých prípadoch, kde bude správne uváženie a právne pohyblivé pojmy

Pri analýze zodpovednostných vzťahov, ktoré vzniknú pri používaní AI vo verejnej správe, bude potrebné jednoznačne ustanoviť pozíciu AI v týchto vzťahoch a jej následnú zodpovednosť pri porušení právnych predpisov z jej strany.

Zoznam použitej literatúry

1. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2113, (EÚ), 2018/858 (EÚ), 2018/1139 a (EÚ) 2019/ 2144 a smernice 2014/90/EÚ (EÚ), 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).
2. Kódex dobrej verejnej správy, príloha nezáväzného odporúčania CM/Rec (2007) z Výboru ministrov členských štátov Rady Európy z 20. júna 2007 o dobrej verejnej správ.
3. Nariadenie Európskeho parlamentu a rady (EÚ) č. 2016/679 z apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov).
4. Smernica rektora UK č. 2/2024 o používaní nástrojov umelej inteligencie na Univerzite Komenského v Bratislave.

5. ANDRAŠKO, J. a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha. Wolters Kluwer ČR, 2022, 380 s.
6. HARARI Noah Yuval: Sapiens stručná história ľudstva: Aktuell, 2018, s. 424.
7. VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 3. vydanie. Bratislava: C.H.Beck, 2025, 344 s.
8. VRABKO, M. a kol.: Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C.H.Beck, 2019, 204 s.
9. TÓTHOVÁ, K.: Rozhodovacie procesy v štátnej správe. Bratislava, Vydavateľstvo Obzor, 1989, 120 s.
10. ČUPKA, M.: Skutočné otázky o AI sú sociálneho charakteru. Forbs, október 2025 s. 182-186.
11. FARKAŠ, I.: Potrebujeme trénovať myseľ. Forbs, október 2025 s. 198-200.
12. BIELIKOVÁ, M. – Denník N: Jej úspech stojí na troch pilieroch, s. 15, 18. 10. 2025.

Kontaktné údaje

prof. JUDr. Marián Vrabko, CSc.

marian.vrabko@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Katedra správneho a environmentálneho práva

PRÁVNE ASPEKTY AKTOV DSA A AIA VO VZŤAHU K ROZHODOVANIU VO VEREJNEJ SPRÁVE¹

LEGAL ASPECTS OF DSA AND AIA ACTS IN RELATION TO DECISION-MAKING IN PUBLIC ADMINISTRATION

Anton Martvoň²

Abstrakt: V rámci práva Európskej únie na pôde Európskeho parlamentu boli prijaté Akt o digitálnych službách (tzv. „Akt DSA“) a Akt o umelej inteligencii (tzv. „Akt AIA“), ktoré majú priamy dopad aj na verejnú správu v Slovenskej republike, no zároveň si vyžadujú ešte dôslednú národnú implementáciu - najmä v oblasti určovania orgánov dohľadu a ukladania sankcií. Predmetom môjho vedeckého príspevku je poukázanie na priame i nepriame právne aspekty a na obsah Aktov DSA a AIA vo vzťahu k verejnej správe, ako aj na ich prípadné možné dopady na rozhodovanie, či na používanie umelej inteligencie v rámci verejnej správy v Slovenskej republike. Taktiež v rámci záveru môjho vedeckého príspevku poukazujem na základné atribúty automatizovaného rozhodovania vo verejnej správe za využitia umelej inteligencie tzv. „AI“ v prípade, ak by systémy umelej inteligencie predsa len mali mať možnosť rozhodovať a robiť automatizované správne úkony, vrátane automatizovaného vydávania správnych aktov vo verejnej správe v Slovenskej republike.

Kľúčové slová: správne právo, verejná správa, AI, umelá inteligencia, digitálne služby, e-Government

Abstract: Within the framework of European Union law, the European Parliament adopted the Digital Services Act (the so-called "DSA Act") and the Artificial Intelligence Act (the so-called "AIA Act"), which also have a direct impact on public administration in the Slovak Republic, but at the same time still require consistent national implementation - especially in the area of determining supervisory authorities and imposing sanctions. The subject of my scientific contribution is to point out the direct and indirect legal aspects and the content of the DSA and AIA Acts in relation to public administration, as well

¹ Príspevok bol spracovaný v rámci grantu APVV evidenčné č. APVV-24-0146 s názvom „Právne a aplikačné aspekty aktu DSA na fungovanie orgánov štátnej správy v online prostredí“ udeleného Agentúrou na podporu výskumu a vývoja (APVV)

² Katedra správneho a environmentálneho práva Právnickej fakulty UK v Bratislave

as their possible possible impacts on decision-making or the use of artificial intelligence within public administration in the Slovak Republic. Also, as part of the conclusion of my scientific contribution, I point out the basic attributes of automated decision-making in public administration using artificial intelligence, the so-called "AI", in the event that artificial intelligence systems should nevertheless be able to make decisions and perform automated administrative acts, including the automated issuance of administrative acts in public administration in the Slovak Republic.

Key words: administrative law, public administration, AI, artificial intelligence, digital services, e-Government

Úvod

V rámci práva Európskej únie na pôde Európskeho parlamentu boli prijaté *Akt o digitálnych službách* (ďalej len „Akt DSA“) a *Akt o umelej inteligencii* (ďalej len „Akt AIA“), ktoré majú priamy dopad aj na verejnú správu v Slovenskej republike, no zároveň si vyžadujú ešte dôslednú národnú implementáciu - najmä v oblasti určovania orgánov dohľadu a ukladania sankcií. Predmetom môjho vedeckého príspevku je poukázanie na priame i nepriame právne aspekty a na obsah Aktov DSA a AIA vo vzťahu k verejnej správe, ako aj na ich prípadné možné dopady na rozhodovanie, či na používanie umelej inteligencie v rámci verejnej správy v SR, pokiaľ by bola daná systémom umelej inteligencie (ďalej len „AI“) zákonná možnosť rozhodovať a robiť automatizované správne úkony, vrátane automatizovaného vydávania správnych aktov vo verejnej správe v Slovenskej republike.

Akt o umelej inteligencii, (tzv. „Akt AIA“)

Dňa 21.04.2021 Európska komisia navrhla Akt AIA, dňa 21.05.2024 ho Rada EÚ schválila a Európsky parlament ho schválil ako *Nariadenie Európskeho parlamentu a Rady číslo 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie* a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (**tzv. akt o umelej inteligencii**)³, pričom ako akt účinnosť nadobudol dňa 01.08.2024, no členské štáty majú povinnosť začať implementovať ním stanovené opatrenia až od 01.08.2026. Akt AIA si dovoľím charakterizovať ako prvé nariadenie, resp. právny predpis na svete regulujúci umelú inteligenciu ako globálna norma.⁴ Jeho cieľom je zabezpečiť, aby

³<https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

⁴<https://www.consilium.europa.eu/sk/policies/artificial-intelligence/> (odkaz platný k 28.09.2025)

boli systémy umelej inteligencie (ďalej ak ako „AI“) bezpečné, etické a dôveryhodné, ako aj aby sa systémy AI vyvíjali a používali zodpovedne.

Upravuje jednotné pravidlá pre vývoj a využívanie AI technológií v Európskej únii. Akt AIA sa zameriava na identifikáciu a reguláciu AI systémov podľa ich rizikovosti a stanovuje povinnosti pre poskytovateľov, distribútorov a používateľov AI systémov. Právny rámec sa vzťahuje na verejné aj súkromné subjekty v Európskej únii (ďalej aj ako „EÚ“) aj mimo nej, pokiaľ bude systém umelej inteligencie uvedený na trh EÚ alebo ak bude mať jeho používanie vplyv na bežných ľudí nachádzajúcich sa v EÚ.⁵ V Akte AIA obsiahnutými a so zakotvenými pravidlami sa poskytovateľom technológií umelej inteligencie a umelú inteligenciu nasadzujúcim subjektom ukladajú povinnosti na tomto úseku, plus sa upravuje ním povoľovanie systémov umelej inteligencie na jednotnom trhu EÚ, ako aj riešia sa ním riziká spojené s umelou inteligenciou, ako je skreslenie, diskriminácia subjektov a nedostatky v oblasti zodpovednosti, pričom sa týmto Aktom AIA podporuje aj inovácia a zavádzanie umelej inteligencie do reálnej praxe. Presadzuje aj pravidlá pre modely umelej inteligencie na všeobecné účely.⁶

Umelá inteligencia tzv. „AI“ je definovaná v Akte AIA ako rýchlo sa rozvíjajúca skupina technológií, ktorá prispieva k širokému spektru hospodárskych, environmentálnych a spoločenských prínosov vo všetkých odvetviach a spoločenských činnostiach.⁷

Ďalej je potrebné uviesť, že „systém AI“ je v Akte AIA definovaný ako strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, ako aj zo spôsobu generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie.⁸ Pojem „strojový“ sa vzťahuje na skutočnosť, že systémy AI fungujú práve na strojoch.⁹

V Akte AIA sa upravuje riziko spojené s konkrétnym používaním umelej inteligencie, pričom sa v ňom toto spomenuté riziko kategorizuje na **štyri úrovne rizika** používania AI a na v rámci nich z toho vyplývajúce stanovenia rôznych im zodpovedajúcich pravidiel a obmedzení¹⁰ (i pre subjekty verejnej správy, ktoré by

⁵<https://www.uvo.gov.sk/aktualne-temy/aktualita/nariadenie-o-umelej-inteligencii> (cit. 2025-09-28)

⁶ <https://digital-strategy.ec.europa.eu/en/policies/ai-office> (cit. 2025-09-28)

⁷ Bod 4) recitálu (resp. Preambuly) Aktu AIA

⁸ Článok 3 Aktu AIA

⁹<https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

¹⁰<https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

využívali umelú inteligenciu pri ich rozhodovaní vo verejnej správe¹¹). Ide o nasledovné úrovne rizika:

- a) **Minimálne alebo žiadne riziko** - Väčšina systémov umelej inteligencie nepredstavuje riziká. Hry alebo protispamové filtre poháňané umelou inteligenciou sa môžu voľne používať. Akt AIA ich **nereguluje** a nemá na ne žiadny vplyv.
- b) **Obmedzené riziko** - Na systémy umelej inteligencie, ktoré predstavujú len obmedzené riziko (ako sú napríklad četovacie roboty alebo systémy AI, ktoré tvoria obsah) sa budú vzťahovať povinnosti transparentnosti, ako je informovanie používateľov, že ich obsah bol vytvorený priamo umelou inteligenciou, aby mohli prijímať informované rozhodnutia o ich ďalšom používaní.
- c) **Vysoké riziko** - Vysokorizikové systémy umelej inteligencie, ako sú systémy používané pri diagnostike chorôb, pri autonómnom vedení vozidla a pri biometrickej identifikácii jednotlivcov zapojených do trestnej činnosti alebo vyšetrovaných v tomto kontexte, musia spĺňať prísne požiadavky a povinnosti na získanie prístupu na trh Európskej únie. Patrí medzi ne prísne testovanie, transparentnosť a ľudský dohľad.
- d) **Neprijateľné riziko** - Ide o používanie systémov umelej inteligencie, ktoré ohrozujú bezpečnosť, ľudské práva alebo živobytie ľudí, a preto sú v tomto prípade **v EÚ zakázané**. Patrí sem kognitívna manipulácia správania sa ľudí¹² a hlavne zraniteľných skupín obyvateľstva (napr. deti, seniori), prediktívne vykonávanie policajných funkcií, rozpoznávanie emócií na pracovisku a vo vzdelávacích inštitúciách alebo sociálne hodnotenie.¹³ Zakazuje sa aj používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejných priestoroch bez splnenia prísnych podmienok (napr. na úseku GDPR), ako je rozpoznávanie tváre orgánmi presadzovania práva vo verejných priestoroch¹⁴, až na niekoľko obmedzených výnimiek (napr. pri imigrácii alebo pri ochrane štátnych hraníc).

¹¹ VRABKO, Marián a kol.: Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C.H. Beck, 2018, s. 3 a nasl.

¹² Bližšie pozri: SLACK, Gordy: What DALL-E Reveals About Human Creativity, zverejnené dňa 17.01.2023. Stanford University, Human-Centered Artificial Intelligence, Arts and Humanities, Neuro and Cognitive Science, Dostupné online na: <https://hai.stanford.edu/news/what-dall-e-reveals-about-human-creativity> (cit. 2025-09-28)

¹³ MESARČÍK, Matúš: Zakázané praktiky. In: ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022, s. 334 a nasl.

¹⁴ <https://slowakei.ahk.de/sk/newsletter-recht-steuern/ausgabe-1-25/novy-akt-o-umelej-inteligencii> (cit. 2025-09-28)

Negatívne vymedzenie pôsobnosti Aktu AIA

Akt AIA sa nevzťahuje na systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské a obranné účely, na účely národnej bezpečnosti, a na produkty v rámci právnych aktov výslovne vymenovaných v čl. 2 ods. 2 Aktu AIA, ako napr. Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008. o bezpečnostnej ochrane civilného letectva alebo nariadenia Európskeho parlamentu a Rady týkajúce sa typového schvaľovania motorových vozidiel a ich prípojných vozidiel, či ich motorov. Tento Akt AIA ako nariadenie sa tiež neuplatňuje na systémy alebo modely AI vrátane ich výstupov, ktoré sú osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja.¹⁵

Pozitívne vymedzenie pôsobnosti Aktu AIA pri rozhodovaní vo verejnej správe

Je potrebné uviesť, že ak systém umelej inteligencie nespadá pod osobitnú reguláciu, tak potom kľúčová Príloha III Aktu AIA obsahuje oblasti, na ktoré sa Akt AIA vzťahuje. Ide o nasledovné oblasti:

- biometrická identifikácia a kategorizácia FO vrátane rozpoznávania ich emócií;
- riadenie a prevádzka kritickej infraštruktúry, energetiky, cestnej premávky, dopravy, logistiky alebo pri dodávkach vody, plynu, tepla alebo elektriny;
- vzdelávanie a odborná príprava;
- problematika ochrany predmetov práv duševného vlastníctva, tzn. ochrany práv autorov a pôvodcov týchto predmetov z pohľadu transparentnosti použitia týchto predmetov pri trénovaní systémov umelej inteligencie;¹⁶
- prístup k súkromným a k verejným službám a k dávkam, vrátane posudzovania nárokov na ne, či na účely odhaľovania finančných podvodov;
- hodnotenie a klasifikácie tiesňových volaní FO alebo na vysielanie záchranných služieb prvej reakcie vrátane zo strany polície, hasičov a zdravotníckej pomoci alebo na stanovovanie priority ich vysielania, ako aj pokiaľ ide o systémy triedenia pacientov v rámci pohotovostnej zdravotnej starostlivosti;
- zamestnanosť, riadenie zamestnancov a prístup k samostatnej zárobkovej činnosti, ako aj umiestňovanie cielených inzerátov na pracovné miesta, analýza a filtrovanie žiadostí o zamestnanie a hodnotenie uchádzačov o zamestnanie;
- migrácia, azyl a riadenie kontroly hraníc;
- presadzovanie práva (na posudzovanie rizika, že či sa fyzická osoba stane obeťou trestných činov, na podporu orgánov a ich metód presadzovania práva ako

¹⁵<https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

¹⁶ DAŇKO, Martin: Prienik umelej inteligencie a práva duševného vlastníctva: výzvy a očakávania. In: Zborník Bratislavské právnické fórum 2024 s názvom „Právo a technológie v 21. storočí optikou európskeho práva. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 99

polygrafy alebo podobné nástroje, či na hodnotenie spoľahlivosti dôkazov v priebehu vyšetrovania alebo stíhania trestných činov);

- výkon spravodlivosti a demokratické procesy (ide o systémy AI, ktoré má používať justičný orgán pri skúmaní a interpretácii skutkových okolností a práva a pri uplatňovaní práva na konkrétny súbor skutkových okolností alebo ktoré sa majú používať obdobným spôsobom pri alternatívnom riešení sporov, ako aj systémy AI určené na ovplyvňovanie výsledku volieb, referenda alebo volebného správania fyzických osôb pri hlasovaní vo voľbách alebo v referende, vrátane nástrojov používaných na organizovanie, optimalizáciu alebo tvorbu štruktúry politických kampaní z administratívneho a logistického hľadiska);
- v oblasti zdravotnej starostlivosti, poľnohospodárstva a bezpečnosti potravín;
- médií, športu (napr. AI monitoring vstupu na štadióny) a kultúry;
- efektívneho využívania zdrojov a energie, monitorovania životného prostredia, zachovania a obnovy biodiverzity a ekosystémov a zmierňovania zmeny klímy a adaptácie na ňu.¹⁷

Základné atribúty automatizovaného rozhodovania vo verejnej správe za pomoci AI zakotvené v Akte AIA, sú nasledovné:

- transparentnosť v podobe povedomia, vysvetliteľnosti a dosledovateľnosti rozhodnutí vydaných za po moci AI¹⁸,
- aktuálnosť a bezpečnosť informácií, ako aj odbornosť nahratých podkladov, či databáz právnych argumentov v systéme AI pre automatizované rozhodovanie vo verejnej správe,
- dôvera v podobe rešpektovania súkromia, ľudského dohľadu nad AI, či štátneho a nezávislého dohľadu,
- a spravodlivosť automatizovaného rozhodovania vo verejnej správe v podobe zákazu diskriminácie, či prílišného spoliehania sa verejného sektora na technológie AI, pričom musí dochádzať k minimalizácii skreslení pri automatizovanom rozhodovaní, či musí byť k dispozícii právo namietat' zmenu vydaného rozhodnutia účastníkom konania alebo oprávnenie na vykonanie zmeny takéhoto automatizovane vydaného rozhodnutia zo strany orgánu verejnej správy.

Subjekty automatizovaného rozhodovania vo verejnej správe podľa Aktu AIA

Subjekty automatizovaného rozhodovania umelej inteligencie vo verejnej správe zakotvené priamo Aktom AIA¹⁹ sú nasledovné:

¹⁷ Bližšie pozri: Príloha III Aktu AIA

¹⁸ ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022, s. 341 a nasl.

¹⁹ Článok 64 a nasl. Aktu AIA

- 1.) Úrad pre umelú inteligenciu (Úrad pre AI)
- 2.) Európska rada pre umelú inteligenciu (Rada pre AI)
- 3.) Poradné fórum pre poskytovanie technicko-odborných znalostí a poradenstva Rade pre AI a EK
- 4.) Vedecký panel nezávislých expertov
- 5.) Vnútroštátne príslušné orgány a jednotlivé kontaktné miesta – každý štát EÚ musí zriadiť aspoň
 - a) jeden notifikujúci orgán a
 - b) jeden orgán dohľadu nad trhom pre účely Aktu AIA a na účely kontroly systémov umelej inteligencie.²⁰

Identifikované možné nedostatky automatizovaného rozhodovania za využitia umelej inteligencie vo verejnej správe v kontexte Aktu AIA, sú nasledovné :

- a) Požiadavka zabezpečenia kybernetickej bezpečnosti a ochrany vysokorizikových AI je iba všeobecne formulovaná, nie je definovaná jej úroveň a preto rozhodovanie vo verejnej správe môže byť narušené a paralyzované útokmi z vonku.
- b) Ľudský dohľad nad systémami AI je vyžadovaný aspoň dvoma FO okrem systémov AI využívaných na účely presadzovania práva, migrácie, kontroly hraníc alebo azylu. Práve v týchto vyňatých oblastiach si myslím, že je práveže nutne potrebný dohľad aspoň dvoma FO, ak nie i viacerými.
- c) V Akte AIA sú zakotvené rôzne neprimerané výnimky pre mikropodniky²¹, čím získavajú pri prípadnom zneužití AI neprimeranú ochranu pred sankciami zo strany správnych orgánov.
- d) Výnimky v rámci negatívneho vymedzenia pôsobnosti Aktu AIA, ktoré by bolo potrebné zrušiť a subsumovať pod Akt AIA.
- e) Posúdenie vplyvu na základné práva v prípade vysokorizikových systémov AI je síce zakotvené v čl. 27 Aktu AIA, no iba pre prvé použitie systému AI, na ktoré sa potom tento systém nasadzujúci subjekt môže odvolávať, pričom tam absentuje zo strany verejnej správy povinnosť vykonávať priebežné alebo následné kontrolné posúdenie vplyvu na ľudské práva počas používania daného systému AI.
- f) Akt AIA síce rieši požiadavky na odbornosť a nezávislosť notifikovaných orgánov a notifikovaných osôb od systémov AI nasadzujúcich subjektov, ale iba v rovine právnických osôb ako zodpovedných subjektov. Nevenuje pozornosť a nestanovuje žiadne konkrétne požiadavky na nezávislosť, či na možný konflikt záujmov voči umelej inteligencii nasadzujúcim subjektom pre jednotlivých zamestnancov notifikovaných orgánov verejnej správy a notifikovaných osôb

²⁰<https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

²¹ Článok 63 Aktu AIA

vykonávajúcich priamo kontrolu zhody systémov AI alebo ich certifikácie v praxi. A ani nezakotvuje riešenie ich predpojatosti.

Akt o digitálnych službách (tzv. „Akt DSA“)

Ide o Nariadenie (EÚ) č. 2022/2065 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES prijaté dňa 19.10.2022²² a uplatňuje sa v Európskej únii od 17.02.2024.

Akt DSA sa zameriava cez rozhodovanie správnych orgánov na vytvorenie bezpečnejšieho online prostredia pre spotrebiteľov a spoločnosti v Európskej únii (EÚ) so súborom pravidiel na tieto účely:

- účinnejšie chrániť spotrebiteľov, maloleté osoby a ich základné práva²³,
- vymedziť jednoznačné povinnosti online platforiem a sociálnych médií, vrátane poskytovania údajov výskumníkom a výskumným organizáciám,
- riešiť nezákonný obsah a výrobky, nenávistné prejavy a dezinformácie,
- dosiahnuť väčšiu transparentnosť prostredníctvom lepšieho podávania správ a dohľadu,
- podporovať inováciu, rast a konkurencieschopnosť na vnútornom trhu EÚ,
- a zriadenie Európskeho výboru pre digitálne služby.

Akt o digitálnych službách obsahuje aj osobitné pravidlá, ktoré sa vzťahujú na:

- a) *veľmi veľké online platformy* (ďalej len „VLOP“), ktoré používa viac ako 10 % zo 450 miliónov spotrebiteľov v EÚ, a
- b) *veľmi veľké online vyhľadávače* (ďalej len „VLOSE“), ktoré používa viac ako 10 % zo 450 miliónov spotrebiteľov v EÚ.

Akt o digitálnych službách (resp. Akt DSA) má podľa názoru niektorých odborníkov dokonca extrateritoriálny dosah a dopad i mimo Európskej únie cez prostredníctvom tzv. „bruselského efektu“, keďže ide o extrateritoriálne účinky prelievania Aktu DSA, ktoré sú poháňané ekonomickými stimulmi alebo de facto štandardizáciou a súkromným objednávaním.²⁴

Taktiež spomínaný akt obsahuje oprávnenie pre členské štáty určiť si jeden alebo viac príslušných orgánov zodpovedných za dohľad nad poskytovateľmi

²²<https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32022R2065&qid=1759094232555> (cit. 2025-09-28)

²³ DAŇKO, Martin – ŽÁRSKA, Petra: Vplyv aktu o digitálnych službách na duševné vlastníctvo. In: Zborník Bratislavské právnické fórum 2023 s názvom „Autonómia subjektov v 21. storočí“. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2023, s. 201

²⁴ URBAN, Jennifer – HUSOVEC, Martin: Will the DSA have the Brussels Effect? (2024) Dostupné online na: <https://verfassungsblog.de/will-the-dsa-have-the-brussels-effect/> alebo na: https://www.researchgate.net/publication/378380830_Will_the_DSA_have_the_Brussels_Effect (cit. 2025-09-28)

sprostredkovateľských služieb a uplatňovanie a presadzovanie tohto nariadenia (ďalej len „príslušné orgány“).

Akt o digitálnych službách chráni práva a záujmy všetkých zapojených strán, najmä občanov EÚ, a to prostredníctvom:

- boja proti nezákonnému obsahu na internete vrátane tovaru a služieb,
- posilnenia postavenia používateľov a občianskej spoločnosti,
- posudzovania a zmiernovania rizík, či posilnenia dohľadu a presadzovania všetkých poskytovateľov sprostredkovateľských služieb, a to s dôležitou úlohou pre nezávislých koordinátorov digitálnych služieb v každom členskom štáte EÚ a Európsky výbor pre digitálne služby – okrem toho, má Európska komisia dodatočné vyšetrovacie, kontrolné a sankčné právomoci v súvislosti s VLOP a VLOSE.

V prípade, že dôjde ku kríze, keď mimoriadne okolnosti vedú k závažnému ohrozeniu verejnej bezpečnosti alebo verejného zdravia v EÚ alebo v jej podstatných častiach, môže Európska komisia od VLOP a VLOSE vyžadovať, aby posúdili, či a ako ich služby výrazne prispievajú k tomuto závažnému ohrozeniu alebo k nemu môžu významne prispieť, aby identifikovali a uplatňovali účinné a primerané opatrenia na zmiernenie rizík (uvedené v Akte DSA) s cieľom predísť takémuto prispievaniu k ohrozeniu, odstrániť ho alebo ho obmedziť, a aby podávali Komisii správu o posudkoch a reakciu.

V závislosti od právneho systému jednotlivých členských štátov a predmetnej oblasti práva môžu vnútroštátne justičné alebo správne orgány vrátane orgánov presadzovania práva, prikázať poskytovateľom sprostredkovateľských služieb, aby konali proti jednej alebo viacerým určitým konkrétnym položkám nezákonného obsahu (s ktorým pracuje i systém AI) alebo aby im poskytli určité konkrétne informácie. Akt o digitálnych službách obsahuje aj niekoľko ustanovení, ktoré sú relevantné pre účinnosť služieb v oblasti autorských práv, odstraňovanie obsahu porušujúceho autorské práva a stíhanie porušovateľov. Tieto ustanovenia sa tiež úplne alebo čiastočne riadia judikatúrou Európskeho súdneho dvora o sprostredkovateľských službách.²⁵

Vnútroštátne právne predpisy, na základe ktorých sa takéto príkazy vydávajú, sa značne líšia a tieto príkazy sa čoraz častejšie riešia v cezhraničných situáciách. Na to, aby sa tieto príkazy, najmä v cezhraničnom kontexte, plnili účinným a efektívnym spôsobom, tak, aby dotknuté orgány verejnej moci mohli plniť svoje úlohy a poskytovatelia nepodliehali neprimeranej záťaži, a bez toho, aby boli nenáležité

²⁵ HUSOVEC, Martin: The DSA as a creator's charter? In: Journal of Intellectual Property Law & Practice, 2023, Vol. 18, No. 2, strana 72, zverejnené dňa 21.01.2023. Dostupné online na: https://www.researchgate.net/publication/367331111_The_DSA_as_a_creator's_charter, (cit. 2025-09-28)

dotknuté práva a oprávnené záujmy tretích strán, je potrebné stanoviť určité podmienky, ktoré by tieto príkazy mali spĺňať, či dopĺňujúce požiadavky týkajúce sa spracovania týchto príkazov.

Týmto Aktom o digitálnych službách, by sa preto mali harmonizovať len určité osobitné minimálne podmienky, ktoré by takéto príkazy mali spĺňať, aby poskytovatelia sprostredkovateľských služieb mali povinnosť informovať príslušné orgány o vykonaní týchto príkazov. Tento Akt o digitálnych službách ako nariadenie preto neposkytuje právny základ pre vydávanie takýchto príkazov ani nereguluje ich územnú pôsobnosť či cezhraničné presadzovanie. Uplatniteľné právo Európskej únie alebo vnútroštátne právo, na základe ktorého sa tieto príkazy vydávajú, si môže vyžadovať dodatočné podmienky, pričom by malo byť základom pre výkon príslušných príkazov. V prípade nedodržania takýchto príkazov by vydávajúcí členský štát mal mať možnosť ich vykonať priamo v súlade so svojím vnútroštátnym právom. Príslušné vnútroštátne orgány by mali mať možnosť vydávať takéto príkazy proti obsahu, ktorý sa považuje za nezákonný, alebo príkazy na poskytnutie informácií na základe práva Únie alebo vnútroštátneho práva v súlade s právom Európskej únie, predovšetkým s chartou, a adresovať ich poskytovateľom sprostredkovateľských služieb vrátane tých, ktorí sú usadení v inom členskom štáte Európskej únie.²⁶

Týmto Aktom o digitálnych službách, by však nemalo byť dotknuté právo Únie v oblasti justičnej spolupráce v občianskych alebo trestných veciach vrátane nariadenia (EÚ) č. 1215/2012 a nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach ani vnútroštátne trestné právo procesné či občianske právo procesné.

Okrem toho by sa v prípade potreby mala v Akte DSA upraviť povinnosť, aby spomenuté príkazy obsahovali odôvodnenie, v ktorom sa vysvetľuje, prečo informácie predstavujú nezákonný obsah, a to podľa uplatniteľných vnútroštátnych predpisov trestného práva procesného na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania a stíhania. Členské štáty Európskej únie, by mali zabezpečiť aj to, aby koordinátori digitálnych služieb mohli prijímať opatrenia, ktoré sú účinné pri riešení určitých obzvlášť závažných a pretrvávajúcich porušení tohto nariadenia a ktoré sú týmto porušeniam primerané. Najmä vtedy, keď tieto opatrenia môžu mať vplyv na práva a záujmy tretích strán, ako napríklad v prípadoch, keď sa obmedzí prístup k online rozhraniám, je vhodné požadovať, aby opatrenia podliehali dodatočným zárukám. Po prijatí príkazu konať proti jednej alebo viacerým konkrétnym položkám nezákonného obsahu vydaného príslušnými vnútroštátnymi justičnými alebo správnymi orgánmi na základe uplatniteľného práva Európskej únie alebo vnútroštátneho práva v súlade s právom Európskej únie poskytovatelia

²⁶<https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32022R2065&qid=1759094232555>
(cit. 2025-09-28)

sprostredkovateľských služieb bez zbytočného odkladu informujú orgán, ktorý príkaz vydal, alebo každý iný orgán uvedený v príkaze o vykonaní príkazu, pričom uvedú, či a kedy sa príkaz vykonal.²⁷

Záver

V rámci môjho vedeckého príspevku si dovoľujem na záver sformulovať nasledovné základné atribúty automatizovaného rozhodovania vo verejnej správe za využitia umelej inteligencie v Slovenskej republike:

Ako základný záver si dovoľím uviesť a myslím si, že umelá inteligencia „AI“, by sa mala využívať ako podklad, či možný zdroj pre rozhodovanie vo verejnej správe, prípadne na detekciu chýb a podvodov vo verejnej správe, no samotná umelá inteligencia, by nemala sama vykonávať nikým nekontrolované rozhodovanie vo verejnej správe, a to práve kvôli potencionálnym problémom využitia správnej úvahy v rámci jej automatizovaného rozhodovania, možného neprihliadania na špecifiká jednotlivých prípadov, správnych konaní, subjektov v špecifických konaniach (napr. združení účastníkov pozemkových úprav²⁸), či možného nesledovania verejného záujmu pri rozhodovaní vo verejnej správe zo strany umelej inteligencie.

Ak by umelá inteligencia (tzv. „AI“) vo verejnej správe predsa len mala mať možnosť robiť automatizované správne úkony, dokonca rozhodovať, či robiť automatizované vydávanie správnych aktov, tak podľa môjho názoru (pozn. autora: ovplyvneného i mnou na danú tému absolvovanou vedeckou diskusiou), je potreba:

- a) vylúčenia rizikových úkonov pri automatizovanom rozhodovaní umelej inteligencie (napr. posielanie príslušníkov polície na zásahy), potreba monitoringu lehôt a ich dodržiavania, ďalej potreba kontroly uplatňovania umelej inteligencie pri tzv. umelej AI správnej úvahe a v neposlednom rade je i potreba pre systémy umelej inteligencie zadefinovať a vymedziť tzv. verejný záujem, na ktorý má umelá inteligencia nezávisle, či obligatórne prihliadať.
- b) dôslednej transparentnosti vo verejnej správe v podobe zvyšovania povedomia, vysvetliteľnosti a dosledovateľnosti rozhodnutí vydaných za pomoci systémov umelej inteligencie.
- c) stanovenia presných limitov používania umelej inteligencie pri hodnotení dôkazov a pri rozhodovaní vo verejnej správe, vrátane určenia výslovných zákazov automatizácie a využitia umelej inteligencie na určitých úsekoch verejnej správy,

²⁷<https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32022R2065&qid=1759094232555> (cit. 2025-09-28)

²⁸ PAVLOVIČ, Maroš - SLÁMKOVÁ, Kristína: Združenia účastníkov pozemkových úprav. In: Zborník Bratislavské právnické fórum 2022 s názvom „Vlastník pozemku ako subjekt administratívno-právnych vzťahov“. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2022, s. 80.

či v určitých typoch rozhodovacích procesov²⁹ alebo správnych konaní, napr. pri rozhodovaní o opravných prostriedkoch. S tým súvisí aj otázka potreby súdneho prieskumu rozhodnutí vydaných priamo umelou inteligenciou tzv. „AI“.

- d) aktuálnosti a dôsledného zabezpečenia kybernetickej i technickej bezpečnosti informácií v systémoch umelej inteligencie a ich ochrany pred útokmi „z vonka“.
- e) kontroly odbornosti a aktuálnosti podkladov, dokumentov, či databáz právnych argumentov nahratých do systémov umelej inteligencie pre potreby automatizovaného rozhodovania vo verejnej správe³⁰, vrátane potreby nevyhnutného nastavenia pre AI využívania možných foriem činností v rámci verejnej správy, opisu algoritmov postupov a prístupov, či právnych pojmov využívaných umelou inteligenciou v rámci jej rozhodovania vo verejnej správe.
- f) dôvery v podobe zo strany AI nastaveného nediskriminačného rozhodovania, rešpektovania súkromia, základných práv a slobôd ľudí, či dôsledného dodržiavania princípu digitálnej dôstojnosti obyvateľov, ktorí musia pre AI zostať vždy subjektom a nie sa stať iba objektom jej rozhodovania.
- g) zabrániť u obyvateľov vzniku falošného pocitu z objektivity rozhodovania systémov umelej inteligencie, ako aj potreba regulácie možného vzniku živelnosti a nekritického využívania AI vo verejnej správe.
- h) ľudského dohľadu nad umelou inteligenciou, či nad jej chat-botmi, vrátane aj štátneho, či odborne nezávislého dohľadu nad systémami AI, a to za využitia prediktívnej analytiky, nakoľko dochádza k stretu práva a technológií AI, ktoré sú vždy o krok vpred pred právom (resp. pred ich právnou úpravou a ich reguláciou).
- i) nastavenia spravodlivosti automatizovaného rozhodovania umelej inteligencie vo verejnej správe za stanovenia hraníc spoliehania sa verejného sektora na technológie umelej inteligencie, pričom musí dochádzať k minimalizácii skreslení pri automatizovanom rozhodovaní AI, či musí byť k dispozícii právo namietat' zmenu vydaného rozhodnutia účastníkom konania alebo oprávnenie na vykonanie zmeny takéhoto automatizovane umelou inteligenciou vydaného rozhodnutia zo strany orgánu verejnej správy.
- j) pravidelného a povinného vzdelávania zamestnancov verejnej správy v oblasti využívania systémov umelej inteligencie, kde sa musí dávať pozor na monopolizáciu dodávateľov systémov umelej inteligencie pre verejnú správu a na nimi možnú prednastavenú predpojatosť AI (napr. negatívnu predpojatosť AI

²⁹ VRABKO, Marián a kol.: Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C.H. Beck, 2019, s. 7 a nasl.

³⁰ MÁČAJ, Ľudovít - PAVLOVIČ, Maroš: Význam elektronizácie katastra nehnuteľnosti pri identifikácii vlastníkov pozemkov s nezisteným vlastníkom. In: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov s názvom „Míľniky práva v stredoeurópskom priestore 2022“. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 65-75

v rámci diskriminácie menších, či pozitívnu predpojatosť AI v rámci uprednostňovania firiem jej dodávateľov alebo vývojárov), ako aj na nimi prípadne umožnený únik informácií cez možný vstup „na diaľku“³¹ do prostredia systémov AI cez tzv. „back door“ v systémoch AI.³²

- k) nevyhnutnosti riešenia problémov pri uplatňovaní a vyvodzovaní zodpovednosti vo verejnej správe za rozhodnutia urobené zo strany umelej inteligencie alebo za urobené správne úkony zo strany systémov umelej inteligencie, a to vrátane vyriešenia otázky regresných nárokov zo zodpovednosti za škodu spôsobenú zo strany AI pri výkone verejnej moci.

Umelá inteligencia môže byť dobrým pomocníkom pre zamestnancov vo verejnej správe, ale zároveň môže byť i nekompromisným a zlým úradníkom pri rozhodovaní vo verejnej správe, pokiaľ jej algoritmy a systémy nebudú presne nastavené a prispôsobené na špecifiká rozhodovania vo verejnej správe v Slovenskej republike.

Zoznam použitej literatúry a použitých zdrojov

1. ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022, 380 s., ISBN: 978-80-7676-547-4
2. DAŇKO, Martin: Prienik umelej inteligencie a práva duševného vlastníctva: výzvy a očakávania. In: Zborník Bratislavské právnické fórum 2024 s názvom „Právo a technológie v 21. storočí optikou európskeho práva“. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, 150 s., ISBN: 978-80-7160-728-1
3. DAŇKO, Martin – ŽÁRSKA, Petra: Vplyv aktu o digitálnych službách na duševné vlastníctvo. In: Zborník Bratislavské právnické fórum 2023 s názvom „Autonómia subjektov v 21. storočí“. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2023, 209 s., ISBN: 98-80-7160-705-2
4. HUGENHOLTZ, P.Bernt a QUINTAIS, João Pedro: 2021. Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output? IIC - International Review of Intellectual Property and Competition Law 52 (9): s. 1190–1216. Dostupné online na: <https://doi.org/10.1007/s40319-021-01115-0> (cit. 2025-09-28)

³¹ HUGENHOLTZ, P.Bernt a QUINTAIS, João Pedro: 2021. Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output? IIC - International Review of Intellectual Property and Competition Law 52 (9): s. 1190–1216. Dostupné online na: <https://doi.org/10.1007/s40319-021-01115-0> (cit. 2025-09-28)

³² LANTYER, Victor Habib: Understanding The EU AI Act: a new era in AI Regulation In Europe, zverejnené dňa 20.12.2023. Dostupné online na SSRN: <https://ssrn.com/abstract=4659892> alebo na <http://dx.doi.org/10.2139/ssrn.4659892> (cit. 2025-09-28)

5. HUSOVEC, Martin: The DSA as a creator's charter? In: Journal of Intellectual Property Law & Practice, 2023, Vol. 18, No. 2, strana 72, zverejnené dňa 21.01.2023. Dostupné online na: https://www.researchgate.net/publication/367331111_The_DSA_as_a_creator's_charter, (cit. 2025-09-28)
6. LANTYER, Victor Habib: Understanding The EU AI Act: a new era in AI Regulation In Europe, zverejnené dňa 20.12.2023. Dostupné online na SSRN: <https://ssrn.com/abstract=4659892> alebo na <http://dx.doi.org/10.2139/ssrn.4659892> (cit. 2025-09-28)
7. MÁČAJ, Ľudovít - PAVLOVIČ, Maroš: Význam elektronizácie katastra nehnuteľnosti pri identifikácii vlastníkov pozemkov s nezisteným vlastníkom. In: Zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov s názvom „Míľniky práva v stredoeurópskom priestore 2022“. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, 486 s., ISBN 978-80-7160-668-0
8. MESARČÍK, Matúš: Zakázané praktiky. In: ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022, 380 s., ISBN: 978-80-7676-547-4
9. PAVLOVIČ, Maroš - SLÁMKOVÁ, Kristína: Združenia účastníkov pozemkových úprav. In: Zborník Bratislavské právnické fórum 2022 s názvom „Vlastník pozemku ako subjekt administratívno-právnych vzťahov“. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2022, 157 s., ISBN: 978-80-7160-672-7
10. SLACK, Gordy: What DALL-E Reveals About Human Creativity, zverejnené dňa 17.01.2023. Stanford University, Human-Centered Artificial Intelligence, Arts and Humanities, Neuro and Cognitive Science. Dostupné online na: <https://hai.stanford.edu/news/what-dall-e-reveals-about-human-creativity> (cit. 2025-09-28)
11. URBAN, Jennifer – HUSOVEC, Martin: Will the DSA have the Brussels Effect?, zverejnené dňa: 21.02.2024. Dostupné online na: <https://verfassungsblog.de/will-the-dsa-have-the-brussels-effect/> a https://www.researchgate.net/publication/378380830_Will_the_DSA_have_the_Brussels_Effect (cit. 2025-09-28)
12. VRABKO, Marián a kol.: Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C.H. Beck, 2018, 344 s., ISBN: 978-80-89603-68-8
13. VRABKO, Marián a kol.: Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C.H. Beck, 2019, 232 s., ISBN: 978-80-89603-76-3
14. <https://eurlex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=sk> (cit. 2025-09-28)

15. <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32022R2065&qid=1759094232555> (cit. 2025-09-28)
16. <https://www.consilium.europa.eu/sk/policies/artificial-intelligence/> (cit. 2025-09-28)
17. <https://digital-strategy.ec.europa.eu/sk/policies/ai-office> (cit. 2025-09-28)
18. <https://www.uvo.gov.sk/aktualne-temy/aktualita/nariadenie-o-umelej-inteligencii> (cit. 2025-09-28)
19. <https://slowakei.ahk.de/sk/newsletter-recht-steuern/ausgabe-1-25/novy-akt-o-umelej-inteligencii> (cit. 2025-09-28)
20. Nariadenie Európskeho parlamentu a Rady číslo 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (tzv. akt o umelej inteligencii)
21. Nariadenie (EÚ) č. 2022/2065 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES prijaté dňa 19.10.2022

Kontaktné údaje

Mgr. Anton Martvoň, PhD.

anton.martvon@flaw.uniba.sk

Univerzita Komenského, Právnická fakulta, Katedra správneho a environmentálneho práva

ADMINISTRATIVE AND LEGAL ASPECTS OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE DECISION-MAKING PROCESS BY PUBLIC AUTHORITIES IN UKRAINE

Ivan Gabani, Yaroslav Lazur¹

Abstract. The article examines the administrative and legal aspects of the application of artificial intelligence (AI) technologies in the decision-making process by public authorities. It analyses current trends in the integration of automated systems into the activities of public administration bodies and their impact on the effectiveness, transparency, and quality of management decisions. Particular attention is paid to the legal regulation of the delegation of discretionary powers to artificial intelligence by public authorities, the issues of official liability, algorithmic transparency, and ensuring respect for citizens' rights. National and international examples of AI use in public administration are considered, including automatic processing of requests, detection of high-risk procurement, environmental monitoring, and crisis forecasting. The study substantiates the need to improve Ukraine's regulatory framework, taking into account European Union standards and the priority of human rights and freedoms. Based on the results, directions for the safe integration of AI into the activities of public authorities and mechanisms for ensuring legal certainty are proposed.

Keywords: artificial intelligence; public administration; automated decision-making; algorithmic transparency; digitalization of public administration; legal regulation.

Introduction and Problem Statement

In the current context of digitalization and transformation of public administration, artificial intelligence (AI) is becoming an important tool that can significantly enhance the effectiveness of decision-making by public authorities. At the same time, the active implementation of AI into administrative practice creates numerous legal and organisational challenges, as its use concerns not only technical aspects but also ensuring respect for citizens' rights and freedoms. There is a need for clear administrative and legal mechanisms to regulate automated decisions, covering

¹ Faculty of Law, Uzhhorod National University

issues of official accountability, algorithmic transparency, and oversight of the legality of AI systems' actions. In Ukraine, as in other countries, a comprehensive approach to the integration of AI into public administration that meets European standards and prioritises human rights and freedoms is yet to be developed. This gives rise to risks of opacity, potential discrimination, and problems of legal certainty in the automation of administrative procedures. Therefore, the relevance of the study is determined by the urgent need to develop legal mechanisms to ensure the safe and effective use of AI in public administration, combining innovative technologies with the principle of the rule of law.

Status of the Issue

Research into the administrative and legal aspects of the use of artificial intelligence (AI) in the decision-making process by public authorities is an important area of scientific inquiry in the field of public administration and administrative law. In Ukraine, this issue is particularly relevant in the context of the digitalization of public administration and the need to ensure citizens' rights and freedoms in the context of automated decision-making.

Foreign scholars have been actively analyzing the impact of AI on the efficiency, transparency, and fairness of public administration. In particular, the work of V. Straub et al., *Artificial Intelligence in Government: Concepts, Standards, and a Unified Framework* (2022)², examines conceptual approaches to the integration of AI into public administration and identifies key standards and criteria that ensure the ethical and effective use of AI in the public sector.

Scientific research on this topic is also developing in Ukraine. The article *Artificial Intelligence in Public Administration: Legal and Organisational Aspects* (2023)³ analyzes the legal basis for the implementation of AI in public administration in Ukraine, particularly in the context of ensuring human rights and prioritizing human rights and freedoms.

An important step in the legal regulation of AI in Ukraine was the development by the Ministry of Digital Transformation of Ukraine of the *Roadmap for the Regulation of Artificial Intelligence*, presented in October 2023. The document defines the main directions and principles of AI regulation in Ukraine, particularly in the field of public administration, and provides for preparing national companies for the upcoming

² Straub, V. J., Morgan, D., Bright, J., & Margetts, H. (2022). *Artificial intelligence in government: Concepts, standards, and a unified framework*. arXiv preprint arXiv:2210.17218.

³ Pushkaryova, N. (2023). Правове регулювання та потенційні ризики застосування штучного інтелекту в правоохоронній діяльності [Legal regulation and potential risks of artificial intelligence in law enforcement]. Uzhhorod: Uzhhorod National University.

legislation, similar to the European AI Act, as well as ensuring the protection of citizens' rights in the digital space.⁴

In addition, the article *Administrative and Legal Regulation of AI Use in E-Government* (2024) examines issues of regulatory and legal support for the application of AI in e-government in Ukraine and offers recommendations for improving legislation to ensure the ethical use of technology. The study *The Use of AI to Optimize Decision-Making Processes in Public Administration* (2024) analyzes the advantages and challenges of introducing AI into the public sector, particularly in the context of ethical, legal, and security aspects.⁵

The administrative and legal regulation of the use of AI technologies in the public administration system in Ukraine is still characterized by a number of gaps and unresolved issues. Particular attention should be paid to developing effective mechanisms for legal oversight of AI functioning, ensuring transparency and accountability of automated decision-making processes, and aligning national legislation with international standards in this area.

Purpose of the Study

The purpose of the article is to conduct a comprehensive analysis of the administrative and legal aspects of the application of artificial intelligence technologies in the decision-making process of Ukrainian public authorities, to identify the advantages and risks of their use, and to develop recommendations for improving the regulatory framework in order to ensure transparency, efficiency and respect for citizens' rights in the process of integrating AI into public administration. To achieve the goal of the study, the following tasks were set:

1. Analyse the current state of artificial intelligence application in public administration in Ukraine and abroad, particularly in terms of administrative and legal regulation.
2. Identify the key advantages and potential risks of using automated systems in the decision-making process by state authorities.
3. To examine national and international legal approaches to the regulation of AI in public administration, taking into account the priority of human rights and freedoms and European Union standards.

⁴ Дорожня карта з регулювання штучного інтелекту [Roadmap for AI regulation]. Retrieved from <https://www.kmu.gov.ua/news/rehulivannia-shtuchnoho-intelektu-v-ukraini-mintsyfy-prezentovalo-dorozhniu-kartu>.

⁵ Mytkalyk, S. (2023). Використання штучного інтелекту в роботі Національного агентства з питань запобігання корупції [Use of artificial intelligence in the work of the National Agency on Corruption Prevention]. Kyiv: State University of Infrastructure and Technologies.

4. To assess the level of legal certainty, transparency and accountability of automated decisions in the activities of public administration bodies.
5. Develop recommendations for improving the regulatory framework for the use of AI to enhance the efficiency and security of management processes.

Analysis and Discussion

The integration of artificial intelligence (AI) technologies into public administration is considered one of the key factors in the digital transformation of the state. In the European Union, the United States, and a number of Asian countries, the development of the legal framework for AI use is guided by the principles of algorithmic transparency, accountability, and the protection of human rights. In particular, the recently adopted Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) establishes a risk-based approach to the legal regulation of AI and specifies criteria for its application within public administration.⁶ The practical implementation of such approaches covers the use of AI in public procurement procedures, anti-corruption monitoring, management of urban infrastructure, healthcare, and security.

International examples show a trend towards deeper integration of AI into administrative processes. For example, Estonia has developed a system for the automated adjudication of minor court cases, which reduces the burden on the judicial system and enhances its efficiency.⁷ Singapore has implemented a comprehensive 'Smart Nation' strategy, which provides for the use of AI in the management of urban infrastructure, transportation, and environmental monitoring.⁸ In the United States, predictive analytics systems are being implemented to identify vulnerable or high-risk population groups and prevent crisis situations, which has led to both positive assessments of their effectiveness and discussions regarding potential risks of discrimination.⁹ The need to strike a balance between innovation and compliance with the principles of the rule of law is widely recognised as the key challenge in applying AI in the public sector, a point that is

⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

⁷ Ministry of Justice of Estonia. (2021). *AI in the Estonian judiciary: Automating small claims*. Tallinn: MoJ.

⁸ Government of Singapore. (2020). *Smart nation strategy*. Singapore: Government of Singapore.

⁹ Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Cambridge, MA: Harvard University Press.

frequently highlighted by international organisations such as the Organisation for Economic Co-operation and Development (OECD)¹⁰.

In Ukraine, the process of introducing AI into public administration is still at an early stage of development. A significant step in this direction was the 2023 Roadmap for the Regulation of Artificial Intelligence,⁴ which defined the principles of future legal regulation and alignment with European Union standards. At the same time, practical examples of AI application are mainly concentrated in the areas of the electronic service 'Diia', automated processing of citizens' requests, and identification of risky public procurement.¹¹

Despite the existence of individual initiatives, the national legal framework remains fragmented. The rules governing the use of AI are enshrined in legislation on digitalisation, e-government, and personal data protection, but there is no coherent administrative and legal framework.¹² This results in legal uncertainty regarding the limits of the discretionary powers of public authorities when delegating functions to AI systems, the level of algorithmic transparency, and accountability for the consequences of decisions made using AI.¹³

Thus, a comparative analysis shows that foreign practice is gradually forming a systematic approach to the integration of AI into public administration, whereas in Ukraine the deployment of such technologies remains largely experimental. This underscores the need to develop a comprehensive administrative and legal model that would combine technological innovations with the principles of the rule of law and provide for the implementation of European standards.

The current state of development of artificial intelligence in public administration allows for an analysis of its practical effectiveness and associated risks. Alongside technological capabilities, there is a need for a legal assessment of the consequences of using automated systems in the decision-making process of public authorities.

The key advantages of integrating AI into the activities of public authorities can be grouped into several areas:

Improving the efficiency of administrative procedures. The automation of routine tasks reduces case processing times, streamlines document flow, and contributes to

¹⁰ OECD. (2021). State of implementation of the OECD AI principles: Insights from national AI policies. Paris: OECD Publishing. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fa1/eedfee77-en.pdf.

¹¹ Transparency International Ukraine. (2022). Використання штучного інтелекту у сфері публічних закупівель [Use of AI in public procurement]. Kyiv: TI Ukraine.

¹² Verkhovna Rada of Ukraine. (2021). Закон України «Про національну інфраструктуру цифрових даних» [Law of Ukraine "On the National Infrastructure of Digital Data"]. *Vidomosti Verkhovnoi Rady Ukrainy*, (5).

¹³ Petrov, R. (2022). Artificial intelligence and administrative law in Ukraine: Emerging challenges. *Kyiv-Mohyla Law and Politics Journal*, (8).

the reduction of bureaucratic burdens.¹⁴ For instance, in Denmark and the Netherlands, automated systems for the allocation of social benefits have significantly shortened application processing times.

Transparency and accountability. The use of algorithmic tools to analyse procurement processes, budget expenditures, or corruption risks creates conditions for enhancing citizens' trust in public authorities.¹⁵ In the United Kingdom, automated analytical systems assist in monitoring expenditures on social programmes, although errors in payment calculations occurred during the initial implementation phase.

Predictive analytics. AI is capable of identifying trends and risks in social security, healthcare, and public safety, thereby enabling authorities to make more evidence-based decisions.¹⁶ For example, in the United States, predictive analytics systems are employed to detect high-risk crime areas and to optimise the allocation of police resources.

Unification of management practices. Algorithmic systems facilitate a consistent approach to resolving similar administrative cases, thereby reducing opportunities for subjectivity and selective law enforcement.¹⁷ In Estonia, the automated system for reviewing minor court cases has enabled the standardisation of decisions and alleviated the workload of the courts.

At the same time, the use of AI entails a number of risks that are particularly significant in the administrative and legal context:

Lack of algorithmic transparency. The opacity of the internal logic of algorithms poses a threat to the principles of transparency and accountability in public authorities.¹⁸

Risk of discrimination. The use of low-quality data or algorithms with embedded biases can result in unequal treatment of citizens in access to social or administrative services.¹⁹ A notable example is the COMPAS algorithm in the United States, used to assess the risk of recidivism, which exhibited bias against African Americans.

¹⁴ Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, 42(7), 596–615.

¹⁵ Transparency International. (2021). *Artificial intelligence against corruption: Opportunities and challenges*. Berlin: TI.

¹⁶ Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*.

¹⁷ Kuner, C., Marelli, M., & González Fuster, G. (2022). Artificial intelligence and administrative law: A comparative perspective. *Common Market Law Review*.

¹⁸ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*.

¹⁹ O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown Publishing.

Blurring of responsibility. Determining legal responsibility for the outcomes of decisions made with AI—whether it lies with the developer, the system operator, or the public official—remains problematic.²⁰

Legal uncertainty. The absence of a comprehensive administrative and legal framework complicates the definition of the limits of officials' discretionary powers when employing automated systems.²¹

Threats to information security. The widespread use of data for training algorithms increases the risk of data breaches or unauthorised access.²² For example, during the testing of the Smart Nation system in Singapore, incidents of unauthorised access to personal data occurred.

Risk of job losses. The integration of AI into administrative processes, particularly through the automation of routine tasks, may lead to the transformation of job functions or a reduction in staff numbers. This poses challenges for government agencies in managing the social and organisational consequences.

Thus, the integration of AI into public administration is a dual-faceted phenomenon: on one hand, it enhances the efficiency, transparency, and predictability of state activities; on the other hand, it raises concerns regarding algorithmic fairness, accountability, and legal certainty. This underscores the need to develop a balanced model of administrative and legal regulation capable of minimising risks while preserving the benefits of digital transformation.

Research on international and national experience in integrating artificial intelligence (AI) technologies into public administration demonstrates the development of various administrative and legal mechanisms aimed at combining innovative capabilities with the protection and prioritisation of human rights and freedoms.

Firstly, European Union countries are implementing a risk-based approach to regulation, as enshrined in the recently adopted Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). This approach provides for the classification of AI systems according to their potential risk to human rights and establishes mandatory requirements for testing, certification, and auditing of high-risk algorithms.⁶

Secondly, the principle of algorithmic transparency is gaining increasing importance. For instance, in the United States and Canada, when employing predictive analytics,

²⁰ Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review*.

²¹ OECD. (2021). *AI, data and privacy: Balancing innovation and security*. Paris: OECD Publishing.

²² U.S. Government Accountability Office. (2018). *Artificial intelligence: Emerging opportunities, challenges, and implications* (GAO-18-142SP). Washington, D.C.: GAO.

public authorities are required to ensure the explainability of algorithmic outcomes and to disclose the criteria underlying decision-making processes.²³

Thirdly, legal systems in European countries, particularly the Netherlands and the United Kingdom, are establishing practices for accountability and auditing, including maintaining logs of algorithmic actions, documenting decision-making processes, and conducting regular independent audits of automated systems. These measures allow for the identification of responsible parties and ensure legal certainty.

Fourthly, an approach aimed at minimising discrimination risks is widely adopted. In Singapore and the United States, algorithms used in social programmes undergo specific testing for gender, age, or ethnic bias prior to their practical implementation.²⁴

Fifthly, European practice emphasises the principle of preserving the decisive role of humans (human-in-the-loop). In Finland, France, and the United Kingdom, automated algorithmic outputs are treated solely as advisory, while the final decision rests with a public official. This approach guarantees legal accountability and provides an adequate level of protection for citizens' rights.²⁵

Ethical standards and international recommendations remain an important benchmark, particularly the 2019 OECD AI Principles, which enshrine requirements for fairness, transparency, privacy protection, and human oversight of automated processes.²⁶

Data governance is another crucial aspect. In EU countries, authorities are required to comply with the General Data Protection Regulation (GDPR) and with specific regulations governing the use of personal data for algorithm training. This enhances public trust in digital tools.²⁷

At the national level, Ukraine is still developing its legal approaches to AI use. In particular, the 2023 Roadmap for the Regulation of Artificial Intelligence, prepared by the Ministry of Digital Transformation, highlights the need to harmonise Ukrainian legislation with European standards, primarily the Artificial Intelligence Act (AI Act). Meanwhile, Transparency International Ukraine demonstrates the effectiveness of using algorithms in public procurement to identify 'risky tenders,'

²³ UK Government Digital Service. (2020). *Algorithmic accountability act: United Kingdom and Netherlands practices*. London: UK GDS.

²⁴ Singapore Personal Data Protection Commission. (2020). *Model AI governance framework* (2nd ed.). Singapore: PDPC.

²⁵ High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. Brussels: European Commission.

²⁶ OECD. (2019). *Recommendation of the Council on artificial intelligence* (OECD/LEGAL/0449). Paris: OECD Publishing.

²⁷ European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 4.5.2016.

exemplifying a successful integration of AI into anti-corruption efforts. Additionally, the adoption of the Law of Ukraine 'On National Digital Data Infrastructure' in 2021¹³ laid the groundwork for a more systematic implementation of data management mechanisms within administrative activities.

Thus, the analysis of international and national experiences in integrating AI into public administration indicates the emergence of a comprehensive regulatory model that combines technological innovation with the principles of legal certainty, transparency, and accountability, while upholding the primacy of human rights and freedoms. In Ukraine, the key challenge is to adapt European standards, particularly the AI Act, to the national administrative context, taking into account the specific features of public administration and democratic requirements. The principles of transparency, accountability, and legal certainty can serve as guiding benchmarks for developing effective legal mechanisms to ensure the safe integration of AI into the operations of public authorities.

In view of Ukraine's course toward digital transformation and integration into the European legal space, and taking into account both national and international experience, the following approach to the practical implementation of artificial intelligence in public administration is proposed:

I. Regulation, Transparency, and Accountability. To ensure the security and legality of AI use in public administration, mechanisms for control, transparency, and accountability must be implemented ²⁷

1. Risk-Oriented Regulation

- Legislate mandatory auditing and certification of high-risk algorithms used in public procurement, social benefits, and healthcare .
- Establish administrative liability for the use of uncertified algorithms.⁸

Example: The Prozorro system, Ukraine's public electronic procurement platform, uses algorithms to analyse tenders and identify 'risky' bids based on predefined indicators (e.g., unusual pricing, lack of competition, or deviations from standard procedures). This functionality, which is critical for anti-corruption monitoring, should be codified as a mandatory legal requirement, including administrative sanctions for ignoring AI-generated alerts.¹²

2. Transparency of Algorithms and Decisions

- Amend the Law on Administrative Services to require authorities to create 'algorithmic passports' — detailed descriptions of AI functionality.
- Establish procedures for administrative appeals against decisions made by automated systems.

Example: The Diya portal provides online services, but its data verification algorithms are not transparent. Legislation should oblige the Ministry of Digital Transformation to publish descriptions of the algorithms and ensure that their decisions can be challenged through administrative appeal mechanisms.

3. Accountability and Responsibility

- Decisions made using AI must be signed by an official who bears administrative responsibility¹¹.
- Establish liability for discriminatory or unlawful decisions made with the involvement of AI.

Example: In healthcare systems, risk prediction algorithms do not absolve the physician of responsibility — the final decision remains with the official.

4. Integration of EU Standards and International Practices

- Adapt key provisions of the Artificial Intelligence Act (AI Act) into national legislation, particularly in the Law on Public Service, regarding the use of certified algorithms.
- Amend the Code of Administrative Procedure to introduce specific procedures for appealing decisions made using AI.³

Example: Following the Estonian model (KrattAI), Ukraine could implement pilot projects for the automated consideration of administrative cases (traffic fines, land disputes), with mandatory appeal procedures.

5. Enhancing Staff Competence and Methodological Support

- Require civil servants working with algorithms to undergo regular professional development.
- Develop methodological guidelines for internal control of AI use within government agencies⁶.

Example: Training courses at the Diya Academy should be made mandatory for category “A” civil servants and incorporated into AI competency certification.

II. Automation of Administrative Procedures. AI can enhance the efficiency of government agencies, reduce bureaucracy, and shorten application processing times.²⁴

6. Automated Guidance on Administrative Procedures

Chatbots or voice assistants inform citizens about the procedure for submitting applications, deadlines, required documents, rights, and obligations.

Advantages: shorter queues at Administrative Service Centres (ASCs), faster access to information, fewer errors in documents.

Administrative and legal aspect: bots serve as ‘reference guides’; the final decision remains with an official.

7. Verification of Document Accuracy and Completeness

Algorithms check administrative service applications for completeness and compliance with legal requirements.

Advantages: reduced processing time, fewer refusals due to formal errors.

Administrative and legal aspect: the decision to provide the service remains with the civil servant.

8. Monitoring of Administrative Procedure Deadlines

The system tracks application processing times and automatically notifies citizens of delays or the possibility of appeal.

Advantages: increases transparency and control, reduces violations of deadlines.

Administrative and legal aspect: notifications can serve as official evidence in disputes.

9. Automatic Generation of Draft Protocols and Decisions

AI generates drafts of administrative decisions and provides templates based on legislation¹².

Advantages: reduces the risk of errors and saves employees' time.

Administrative and legal aspect: signing and responsibility remain with the official.

10. Forecasting Workload on Public Authorities

Algorithms analyse the expected number of applications and identify areas requiring additional support **Chyba! Záložka nie je definovaná..**

Advantages: optimises resources and enables faster service for citizens.

Administrative and legal aspect: supports planning of administrative processes and compliance with legal deadlines.

11. Automated Generation of Administrative Certificates

AI generates certificates regarding application status, progress in registration procedures, and confirmation of tax or fee payments.

Advantages: certificates are available electronically, reducing the need for citizens to visit government offices.

Administrative and legal aspect: signing is performed by an official or automatically via digital signature.

12. Intelligent Assistance for Filing Complaints and Appeals

AI analyses the grounds of complaints and provides templates for administrative lawsuits or requests for decision review .

Advantages: reduces formal errors and saves time for judges and civil servants.

Administrative and legal aspect: the final submission and legal responsibility remain with the citizen.

13. Early Detection Systems for Violations of Administrative Deadlines

AI monitors where government agencies fail to meet deadlines for application review and notifies citizens and management.

Advantages: improves civil servants' efficiency and allows citizens to respond promptly.

Administrative and legal aspect: notifications can serve as official evidence in cases concerning deadline violations.

14. Intelligent Public Registry Management System.

Algorithms verify data in state registries, detect inconsistencies and duplicates.

Advantages: reduces bureaucracy, enhances data accuracy, and accelerates service delivery.

Administrative and legal aspect: final entries are made by officials; AI improves oversight efficiency.

Ukraine's digital transformation, particularly in the context of European integration, requires not only the implementation of new technologies but also the establishment of a robust institutional framework. Artificial intelligence is one of the key technologies with the potential to fundamentally transform public administration, yet its uncontrolled application poses significant risks.

Conclusions

An analysis of national and international practices in integrating artificial intelligence (AI) into public administration demonstrates that these technologies have significant potential to improve the efficiency of government agencies and the quality of public services. AI enables the automation of routine administrative processes, optimisation of document flow, reduction of application processing times, and alleviation of bureaucratic burdens, directly enhancing service delivery for citizens.

At the same time, the implementation of AI presents several challenges, including ensuring algorithmic transparency, defining the limits of officials' discretionary powers, establishing accountability for decisions made, and preventing discrimination risks. The experience of other countries shows that effective AI use is possible only when technological innovations are combined with a clear regulatory framework, audit and control systems, and adherence to the principles of the rule of law and human rights protection.

Special attention should be given to preserving the key role of humans in decision-making: automated systems should serve a supportive function, with ultimate responsibility remaining with the official. Equally important is the continuous development of civil servants' competence in AI, ensuring the safe and effective application of technology in public administration.

Thus, the integration of artificial intelligence into public administration offers broad opportunities for Ukraine's digital transformation and for enhancing the transparency and accountability of public authorities, but requires a comprehensive approach that combines technology, legal standards, and human oversight.

Bibliography

1. Straub, V. J., Morgan, D., Bright, J., & Margetts, H. (2022). Artificial intelligence in government: Concepts, standards, and a unified framework. arXiv preprint arXiv:2210.17218.

2. Pushkaryova, N. (2023). Правове регулювання та потенційні ризики застосування штучного інтелекту в правоохоронній діяльності [Legal regulation and potential risks of artificial intelligence in law enforcement]. Uzhhorod: Uzhhorod National University.
3. Дорожня карта з регулювання штучного інтелекту [Roadmap for AI regulation]. Retrieved from <https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuvalo-dorozhniu-kartu>.
4. Mytkalyk, S. (2023). Використання штучного інтелекту в роботі Національного агентства з питань запобігання корупції [Use of artificial intelligence in the work of the National Agency on Corruption Prevention]. Kyiv: State University of Infrastructure and Technologies.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
6. Ministry of Justice of Estonia. (2021). AI in the Estonian judiciary: Automating small claims. Tallinn: MoJ.
7. Government of Singapore. (2020). Smart nation strategy. Singapore: Government of Singapore.
8. Pasquale, F. (2020). New laws of robotics: Defending human expertise in the age of AI. Cambridge, MA: Harvard University Press.
9. OECD. (2021). State of implementation of the OECD AI principles: Insights from national AI policies. Paris: OECD Publishing Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fa1/eedfee77-en.pdf.
10. Transparency International Ukraine. (2022). Використання штучного інтелекту у сфері публічних закупівель [Use of AI in public procurement]. Kyiv: TI Ukraine.
11. Verkhovna Rada of Ukraine. (2021). Закон України «Про національну інфраструктуру цифрових даних» [Law of Ukraine "On the National Infrastructure of Digital Data"]. Vidomosti Verkhovnoi Rady Ukrainy, (5).
12. Petrov, R. (2022). Artificial intelligence and administrative law in Ukraine: Emerging challenges. Kyiv-Mohyla Law and Politics Journal, (8).
13. Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. International Journal of Public Administration, 42(7), 596–615.
14. Transparency International. (2021). Artificial intelligence against corruption: Opportunities and challenges. Berlin: TI.

15. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*.
16. Kuner, C., Marelli, M., & González Fuster, G. (2022). Artificial intelligence and administrative law: A comparative perspective. *Common Market Law Review*.
17. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*.
18. O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown Publishing.
19. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review*.
20. OECD. (2021). *AI, data and privacy: Balancing innovation and security*. Paris: OECD Publishing.
21. U.S. Government Accountability Office. (2018). *Artificial intelligence: Emerging opportunities, challenges, and implications (GAO-18-142SP)*. Washington, D.C.: GAO.
22. UK Government Digital Service. (2020). *Algorithmic accountability act: United Kingdom and Netherlands practices*. London: UK GDS.
23. Singapore Personal Data Protection Commission. (2020). *Model AI governance framework (2nd ed.)*. Singapore: PDPC.
24. High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. Brussels: European Commission.
25. OECD. (2019). *Recommendation of the Council on artificial intelligence (OECD/LEGAL/0449)*. Paris: OECD Publishing.
26. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union, L119, 4.5.2016.

Contact details

prof. Yaroslav Lazur, DrSc.

yaroslav.lazur@uzhnu.edu.ua

Dean of the Faculty of Law, Uzhhorod National University. e-mail:

mgr. Ivan Gabani, PhD.

ivan.habani@uzhnu.edu.ua

Senior Lecturer of the Department of International Law, Faculty of Law, Uzhhorod National University.

INOVATÍVNE MOŽNOSTI VYUŽITIA UMELEJ INTELIGENCIE PRI ROZHODOVANÍ VO VEREJNEJ SPRÁVE

INNOVATIVE POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN PUBLIC ADMINISTRATION DECISION-MAKING

Alan Lengyel¹

Abstrakt: Umelá inteligencia sa čoraz častejšie spája aj s rozhodovacími procesmi vo verejnej správe, kde prináša nové príležitosti, ale aj právne výzvy. Najväčší potenciál má pri automatizácii rutinných administratívnych úkonov, spracovaní podaní či pri využívaní prediktívnych analýz. Zahraničné skúsenosti (Estónsko, Holandsko, Rakúsko) ukazujú, že umelá inteligencia môže zefektívniť výkon správy, no zároveň vyvoláva zásadné otázky týkajúce sa dodržiavania zásady zákonnosti, ochrany práv účastníkov konania, určovania právnej zodpovednosti a možnosti preskúmania rozhodnutí. Príspevok sa preto sústreďuje na právne limity využívania umelej inteligencie vo verejnej správe a navrhuje odporúčania pre slovenské prostredie, presnejšie normatívne vymedzenie jej použitia, posilnenie požiadaviek na odôvodnenie rozhodnutí, nastavenie mechanizmov súdneho preskúmania a garanciu právnej istoty.

Kľúčové slová: umelá inteligencia, verejná správa, rozhodovanie, zásada zákonnosti, právna zodpovednosť

Abstract: Artificial intelligence is increasingly associated with decision-making processes in public administration, where it brings new opportunities as well as legal challenges. Its greatest potential lies in the automation of routine administrative tasks, the processing of applications, and the use of predictive analyses. Foreign experience (Estonia, the Netherlands, Austria) shows that artificial intelligence can make administration more efficient, but at the same time raises fundamental questions concerning compliance with the principle of legality, the protection of the rights of parties to proceedings, the determination of legal liability, and the possibility of judicial review of decisions. The paper therefore focuses on the legal limits of the use of artificial intelligence in public administration and proposes recommendations for the Slovak context, including a more precise normative definition of its use,

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra správneho a environmentálneho práva.

strengthening the requirements for reasoning of decisions, establishing mechanisms for judicial review, and guaranteeing legal certainty.

Key words: Artificial Intelligence, Public Administration, Decision-making, Principle of Legality, Legal Liability

Úvod

Umelá inteligencia sa v poslednom desaťročí stala jednou z najdiskutovanejších tém v prostredí práva, technológií a verejnej politiky. Jej potenciál meniť spôsob, akým spoločnosť funguje, je obrovský, a to nielen v súkromnom sektore, ale čoraz viac aj vo verejnej správe. Zatiaľ čo digitalizácia a e-Government umožnili presun mnohých služieb do elektronickej podoby, umelá inteligencia otvára úplne novú kapitolu vstupuje do samotného jadra rozhodovacích procesov a poskytovania verejných služieb. Verejná správa, ktorá bola tradične spájaná s byrokraciou, zásadou zákonnosti a kontrolou výkonu moci, dnes čelí otázke, ako tieto princípy udržať v prostredí, kde rozhodnutia môžu byť prijímané alebo podporované algoritmami.

Dôležité je pritom odlíšiť umelú inteligenciu ako široký technologický pojem od automatizovaného rozhodovania, ktoré predstavuje špecifický právny problém. Umelá inteligencia môže pôsobiť ako podporný nástroj, napríklad pri analýze dát alebo príprave podkladov, zatiaľ čo automatizované rozhodovanie znamená, že systém vydá rozhodnutie s priamym právnym účinkom pre občana bez zásahu človeka. Tento rozdiel je zásadný, pretože na každý z týchto javov sa vzťahujú odlišné právne a etické požiadavky. GDPR v článku 22 poskytuje jednotlivcovi právo nebyť predmetom výlučne automatizovaného rozhodnutia, ktoré má právne účinky alebo ho významne ovplyvňuje, zatiaľ čo Akt o umelej inteligencii prijatý v roku 2024 zaradil mnohé systémy využívané vo verejnej správe medzi tzv. vysokorizikové aplikácie, ktoré musia spĺňať prísne požiadavky transparentnosti, kontrolovateľnosti a dohľadu človeka.

Výskum využitia umelej inteligencie vo verejnej správe sa preto prirodzene sústreďuje na dve dimenzie. Prvou je technická a organizačná stránka, aké sú možnosti implementácie umelej inteligencie, v ktorých oblastiach už nachádza uplatnenie a aké prínosy môže priniesť. Druhou je právna a etická rovina, ako zabezpečiť, aby sa uplatňovanie umelej inteligencie dialo v súlade so zásadami právneho štátu, najmä zásadou zákonnosti, ochranou základných práv a zodpovednosťou orgánov verejnej moci. V tomto kontexte zohrávajú kľúčovú úlohu nielen európske normy, ale aj medzinárodné odporúčania, najmä OECD, ktoré zdôrazňujú potrebu transparentnej umelej inteligencie.

Cieľom tohto článku je analyzovať postavenie umelej inteligencie vo verejnej správe so zameraním na možné využitie v rozhodovacích procesoch. Text sa opiera o

teoretické modely rozhodovania vo verejnej správe, predstavuje inovatívne aplikácie umelej inteligencie, posudzuje ich výhody a riziká a hodnotí ich v kontexte európskej a medzinárodnej regulácie. Osobitná pozornosť je venovaná slovenskému kontextu, ktorý ukazuje, že aj v domácom prostredí sa otvárajú možnosti implementácie umelej inteligencie, či už pri spracovaní žiadostí, prediktívnych analýzach alebo komunikácii s občanmi. Ambíciou článku je preto nielen poskytnúť prehľad, ale aj formulovať odporúčania, ktoré môžu prispieť k vyváženiu medzi inováciou a zachovaním princípov právneho štátu.

Verejná správa v kontexte umelej inteligencie

Rozvoj digitálnych technológií zásadne ovplyvnil podobu verejnej správy a nástup umelej inteligencie predstavuje ďalšiu fázu tejto transformácie. Zatiaľ čo digitalizácia a e-Government umožnili elektronické podávanie žiadostí a elektronickú komunikáciu s úradmi, umelá inteligencia potencionálne môže zasahovať priamo do samotného rozhodovania, spracovania dát a poskytovania verejných služieb. Verejná správa tak stojí pred výzvou, ako využiť inovačný potenciál umelej inteligencie pri zachovaní základných princípov právneho štátu a zásady zákonnosti.²

Umelá inteligencia a automatizované rozhodovanie sa často spomínajú spolu, no nejde o rovnaké pojmy.³ Umelá inteligencia je široký súbor technológií, ktoré dokážu spracúvať dáta, učiť sa zo skúseností a pomáhať úradníkom pri práci. Automatizované rozhodovanie je užšia kategória – znamená, že systém vydá rozhodnutie s právnymi účinkami pre jednotlivca bez zásahu človeka.⁴ Kým teda umelá inteligencia môže byť iba pomocníkom, automatizované rozhodovanie priamo zasahuje do práv a povinností občanov.⁵

Európske dokumenty tieto pojmy jasne rozlišujú. **GDPR** (čl. 22) poskytuje fyzickým osobám ochranu pred výlučne automatizovaným rozhodnutím, pričom zdôrazňuje potrebu možnosti ľudského zásahu. **AI Act** prijatý v roku 2024 priniesol prvý komplexný rámec regulácie umelej inteligencie v Európe a zaviedol systém

² **ALON BARKAT, Sh.**, 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration*. Roč. 7, č. 1, s. 1–12.

³ **ALMIOTTO, F.**, 2024. When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis. *German Law Review*. forthcoming, s. 1–27. SSRN preprint dostupný na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4578761

⁴ **BRKAN, M.**, 2019. Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond. *International Journal of Law and Information Technology*. 27(2), 91–121. doi:10.1093/ijlit/eay01

⁵ **HUBKOVÁ, P.**, 2024. EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. *Acta Universitatis Carolinae – Iuridica*. 70(2), 22. doi:10.14712/23366478.2024.25.

kategorizácie rizík.⁶ Verejná správa sa pritom často ocitá v kategórii tzv. vysokorizikových aplikácií, kde sú stanovené prísne požiadavky na transparentnosť, kontrolovateľnosť a dohľad človeka.⁷ Z tohto dôvodu je potrebné v každom prípade skúmať, či ide o využitie AI ako podporného nástroja, alebo o automatizované rozhodovanie, ktoré má právne následky – lebo len od toho sa odvíja rozsah právnych povinností štátu.^{8,9}

Možné aplikácie umelej inteligencie vo verejnej správe sú rôznorodé a možno ich rozdeliť do niekoľkých oblastí. Významná je automatizácia interných procesov, kde umelá inteligencia dokáže spracovať veľké množstvá dokumentov, analyzovať dáta a pripravovať podklady pre úradníkov. Takéto systémy znižujú administratívnu záťaž a umožňujú efektívnejšie nakladanie s verejnými financiami.¹⁰ Ďalšou oblasťou je rozhodovací proces. Algoritmy môžu podporovať rozhodovanie napríklad pri hodnotení žiadostí o sociálne dávky alebo pri posudzovaní rizík v oblasti bezpečnosti. Výhodou je rýchlosť a konzistentnosť, no zároveň vzniká problém tzv. „black box“ efektu, teda nedostatočnej vysvetliteľnosti algoritmov.¹¹ V neposlednom rade má umelá inteligencia uplatnenie v komunikácii s občanmi prostredníctvom chatbotov či inteligentných portálov, ktoré sú schopné poskytovať základné informácie a spracovávať jednoduché žiadosti. V niektorých prípadoch sa umelá inteligencia využíva aj na tvorbu verejných politík prostredníctvom prediktívnych modelov, ktoré umožňujú simulovať dopady rozhodnutí ešte pred ich prijatím.¹²

Zavádzanie umelej inteligencie prináša množstvo pozitív. Predovšetkým ide o efektívnosť systémy dokážu spracovať tisíce podaní denne, čím sa skracuje čas konania a znižujú náklady štátu. Umelá inteligencia navyše umožňuje personalizáciu verejných služieb, pretože na základe dát dokáže lepšie identifikovať potreby jednotlivcov a prispôbiť im poskytované služby. Veľkým prínosom je aj nepretržitá

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act).

⁸ ZUIDERWIJK, A. a CHEN, Y. C., 2021. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*. 38(3), 101577.

⁹ CORVALÁN, J. G., 2018. Digital and Intelligent Public Administration: Transformations in the Era of Artificial Intelligence. *A&C – Revista de Direito Administrativo & Constitucional*. 18(71), 55–77. doi:10.21056/aec.v18i71.857.

¹⁰ VAN NOORDT, C., VAN DEN BERG, J. a BEKKERS, V., 2023. The dynamics of AI capability and its influence on public administration. *Government Information Quarterly*. Roč. 40, č. 4.

¹¹ SIMON, H. A., 1997. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. 4. vyd. New York: Free Press. s. 109.

¹² JONES, B. D., 2003. Bounded Rationality and Political Science: Lessons from Public Administration and Public Policy. *Journal of Public Administration Research and Theory*. 13(4), 395–412. s. 88.

dostupnosť, aplikácie sú schopné poskytovať služby občanom 24 hodín denne, sedem dní v týždni, čím sa zvyšuje rovnosť prístupu k verejným službám.¹³

Súčasne však využívanie umelej inteligencie vo verejnej správe prináša vážne výzvy. Najzásadnejšou je otázka zásady zákonnosti. Rozhodnutia orgánov verejnej správy musia byť opreté o zákon a musia byť zrozumiteľné adresátovi. Ak je však rozhodnutie založené na algoritme, ktorý nie je možné dostatočne vysvetliť, dochádza k oslabeniu právnej istoty.¹⁴ Nemenej problematická je otázka právnej zodpovednosti – kto nesie následky za škody spôsobené rozhodnutím AI? Úradník, ktorý rozhodnutie podpísal, dodávateľ softvéru, alebo štát ako taký? Bez jasného nastavenia zodpovednosti môže dôjsť k právnemu vákuu, ktoré je nebezpečné pre ochranu základných práv občanov.¹⁵

Ďalšou výzvou je transparentnosť a dôvera verejnosti. Algoritmické rozhodovanie je často neprehľadné a občania nemajú možnosť overiť, na akých základoch bolo rozhodnutie prijaté. Tento nedostatok môže oslabiť legitimitu verejnej správy a znížiť dôveru občanov v štátne inštitúcie. Rizikom je aj diskriminácia a reprodukovanie predsudkov, ak sú tréningové dáta zaujaté alebo neúplné. Verejná správa preto musí dbať na to, aby používané algoritmy spĺňali kritériá férovosti a nestrannosti.¹⁶

Na európskej úrovni je kľúčovým dokumentom pripravovaný AI Act, ktorý klasifikuje využitie umelej inteligencie vo verejnej správe často ako „high-risk“ a zavádza prísne požiadavky na transparentnosť, dohľad človeka a audit algoritmov. Tento aspekt má zásadný význam pre zabezpečenie ochrany práv občanov a posilnenie zodpovednosti orgánov verejnej moci. V slovenskom prostredí je dôležité prepojiť požiadavky AI Act s vnútroštátnou legislatívou, najmä so zákonom o e-Governmente a správnym poriadkom, ktoré stanovujú základné procesné princípy verejnej správy.¹⁷

Inšpiratívne príklady využitia AI možno nájsť v Estónsku, ktoré je považované za digitálneho lídra. AI sa tu využíva pri inteligentnej daňovej správe alebo v oblasti zdravotníctva, kde prediktívne modely pomáhajú odhaľovať riziká ochorení. Vo Fínsku bol zavedený program AuroraAI, ktorý má za cieľ systémovo integrovať AI do verejných služieb na národnej úrovni.¹⁸ Tieto príklady ukazujú, že úspešná

¹³ VAN NOORDT, C., VAN DEN BERG, J. a BEKKERS, V., 2023. The dynamics of AI capability and its influence on public administration. *Government Information Quarterly*. Roč. 40, č. 4, 101879.

¹⁴ Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, 21(7),

¹⁵ ALON BARKAT, Sh., 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration*. Roč. 7, č. 1, s. 1–12.

¹⁶ Ibid.

¹⁷ VAN NOORDT, C., VAN DEN BERG, J. a BEKKERS, V., 2023. The dynamics of AI capability and its influence on public administration. *Government Information Quarterly*. Roč. 40, č. 4, 101879.

¹⁸ BABŠEK, M., et al. (2025). Artificial Intelligence Adoption in Public Administration. *Journal of Cyber Policy*, 10(2), s. 211–230

implementácia si vyžaduje nielen technologické inovácie, ale aj vhodné legislatívne a organizačné nastavenie.

Zhrnutím možno konštatovať, že umelá inteligencia je pre verejnú správu príležitosťou aj rizikom zároveň. Prináša možnosť zlepšiť efektívnosť a kvalitu poskytovaných služieb, ale zároveň vyvoláva zásadné otázky o zákonnosti, zodpovednosti a dôvere verejnosti. Budúcnosť verejnej správy tak bude závisieť od schopnosti vytvoriť rovnováhu medzi inováciami a ochranou základných princípov právneho štátu.

Teoretické východiská rozhodovania vo verejnej správe

Rozhodovanie vo verejnej správe je jedným z kľúčových procesov, ktoré určujú, ako štátne a samosprávne orgány plnia svoje funkcie. Na rozdiel od súkromného sektora, kde sa rozhodnutia prijímajú s cieľom maximalizovať zisk alebo efektívnosť, vo verejnej správe sú rozhodnutia viazané zásadou zákonnosti, verejným záujmom a demokratickou legitimitou. Práve preto je užitočné pozrieť sa na základné teoretické modely rozhodovania.¹⁹

Klasickým modelom je tzv. byrokratický model rozhodovania. Tento model zdôrazňuje hierarchiu, presné pravidlá a formalizované postupy. Rozhodnutia sú prijímané na základe zákonom predpísaných procesov a minimalizujú sa v ňom subjektívne faktory. V prostredí verejnej správy ide o záruku rovnakého prístupu a predvídateľnosti rozhodnutí.²⁰

Ďalším vplyvným konceptom je model racionálneho rozhodovania, podľa ktorého úradník (či inštitúcia) zhromažďuje všetky dostupné informácie, analyzuje možné alternatívy a vyberá optimálne riešenie. Tento model predpokladá vysokú mieru informovanosti a schopnosti objektívne porovnávať varianty.²¹ V praxi je však často limitovaný nedostatkom času, informácií alebo zdrojov, čo viedlo k rozvoju modelu obmedzenej racionality, ktorý reflektuje skutočnosť, že rozhodujúci aktéri hľadajú „dostatočne dobré“ riešenie, nie absolútne optimálne.²²

V prostredí verejnej správy je významný aj inkrementalistický model, ktorý zdôrazňuje postupné, malými krokmi prijímané rozhodnutia. Ukazuje sa, že úradníci a politici často nemajú kapacity na radikálne riešenia a namiesto toho sa spoliehajú

¹⁹ ALON-BARKAT, Sh., 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration*. s. 3.

²⁰ WEBER, M., 1978. *Economy and Society*. Berkeley: University of California Press. s. 58.

²¹ SIMON, H. A., 1997. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. 4. vyd. New York: Free Press. s. 109.

²² JONES, B. D., 2003. Bounded Rationality and Political Science: Lessons from Public Administration and Public Policy. *Journal of Public Administration Research and Theory*. 13(4), 395–412. s. 88.

na čiastočné zlepšenia oproti existujúcemu stavu. Tento prístup je blízky realite, kde sa rozhodovanie odohráva v politickom prostredí s tlakom rôznych záujmov.²³ Tieto teoretické modely vytvárajú základ, ktorý je potrebné zohľadniť pri diskusii o umelej inteligencii vo verejnom rozhodovaní. Umelá inteligencia má potenciál posilniť racionálny model tým, že umožňuje spracovanie obrovského množstva dát a analýzu viacerých alternatív naraz. Na druhej strane môže prispieť k ešte väčšej formalizácii a rigidite, ak sa stane súčasťou byrokratického modelu. Umelá inteligencia zároveň môže pomôcť prekonávať limity obmedzenej racionality, keďže poskytuje nástroje na spracovanie komplexných informácií a prediktívnu analytiku.²⁴ Prepojenie teoretických modelov s praxou využívania umelej inteligencie otvára nové otázky o legitímnosti a transparentnosti rozhodovania. Kým tradičné modely sú postavené na ľudskom faktore, umelá inteligencia vstupuje do procesu ako „tichý partner“, ktorý môže významne ovplyvniť výsledok, no nie vždy je jasné, ako k nemu dospel. Preto je dôležité, aby diskusia o inovatívnych možnostiach využitia umelej inteligencie nadväzovala na tieto klasické teoretické východiská.²⁵

Inovatívne aplikácie umelej inteligencie v rozhodovaní vo verejnej správe

Jednou z najvýraznejších aplikácií umelej inteligencie je prediktívne rozhodovanie. Systémy dokážu analyzovať obrovské objemy dát a odhaliť vzory, ktoré by človek len ťažko identifikoval. V praxi to znamená, že umelá inteligencia vie predvídať napríklad regióny s vyšším rizikom nezamestnanosti, kriminality či environmentálnych problémov a umožniť tak prijatie preventívnych opatrení.²⁶ V USA sa testovali prediktívne policajné systémy, ktoré mali efektívnejšie rozdeľovať zdroje. Hoci výsledky boli rozporuplné a často kritizované pre diskriminačné efekty, ukázali potenciál umelej inteligencie v oblasti prevencie.²⁷ Podobné prístupy skúma aj Slovensko, v rámci Ministerstva vnútra SR sa v diskusiách uvádza možnosť využívania

²³ LINDBLOM, C. E., 1959. The Science of Muddling Through. *Public Administration Review*. 19(2), 79–88. s. 85.

²⁴ WIRTZ, B. W. a MÜLLER, W. M., 2019. An integrated artificial intelligence framework for public management. *Public Management Review*. 21(7), 1076–1100. s. 7.

²⁵ ALON-BARKAT, Sh., 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration*. 7(1), s. 1–12.

²⁶ ALON-BARKAT, Sh., 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration*. 7(1), 1–12. s. 5–7.

²⁷ JONES, M. L., 2019. The ethics of predictive policing. *International Journal of Law in Context*. 15(4), 409–425. s. 412.

umelej inteligencie pri tvorbe mapy kriminality, čo by umožnilo lepšie plánovanie kapacít polície a preventívnych opatrení.²⁸

Umelá inteligencia sa využíva aj pri automatizácii jednoduchých administratívnych rozhodnutí. Ide o situácie, keď algoritmus spracúva žiadosti občanov a rozhoduje na základe vopred nastavených kritérií, či žiadateľ spĺňa zákonné podmienky. Typickým príkladom sú žiadosti o sociálne dávky alebo registrácie do verejných programov.²⁹ Automatizácia šetrí čas a odbreňuje úradníkov od rutinných úkonov, no rizikom je tzv. „algoritmická rigidita“ – neschopnosť zohľadniť individuálne okolnosti, ktoré by človek prirodzene posúdil. OECD preto odporúča zavádzať tieto systémy iba tam, kde existuje jasná právna regulácia, kvalitné dáta a mechanizmus spätnej väzby.³⁰ Významnou inováciou je aj koncept „augmented decision-making,“ umelá inteligencia nie je autonómnym rozhodcom, ale nástrojom, ktorý úradníkom poskytuje analýzy, upozorňuje na nezrovnalosti a navrhuje alternatívy. Tento model sa osvedčil v zdravotníctve, kde umelá inteligencia pomáha pri posudzovaní žiadostí o liečbu alebo plánovaní nemocničných kapacít³¹ Aj v slovenských podmienkach sa diskutuje o využití AI ako asistenta, ktorý uľahčí spracovanie právnych predpisov alebo vyhľadávanie relevantných údajov pre rozhodovanie úradníkov.³² Takýto prístup zachováva ľudskú kontrolu a zároveň zvyšuje kvalitu rozhodnutí.

Ďalším trendom je využívanie chatbotov a inteligentných rozhraní, ktoré občanom poskytujú predbežné rozhodnutia a asistenciu pri komunikácii s úradmi. Estónsko či Fínsko patria medzi krajiny, kde sú tieto technológie už v praxi – občania prostredníctvom digitálnych asistentov podávajú žiadosti, odovzdávajú dokumenty a dostávajú predbežné vyjadrenia.³³ Podobný projekt pripravuje aj Ministerstvo vnútra Slovenskej republiky, ktoré vyvíja chatbota dostupného na svojich webových stránkach.³⁴ Tento prístup zvyšuje dostupnosť služieb, pretože občania môžu komunikovať s verejnou správou nepretržite. OECD však zároveň upozorňuje, že aj

²⁸ Ministerstvo vnútra Slovenskej republiky, 2025. *Zápis z pracovnej skupiny pre riešenie problematiky umelej inteligencie*(22. 7. 2025). Bratislava: MV SR.

²⁹ WIRTZ, B. W. a MÜLLER, W. M., 2019. An integrated artificial intelligence framework for public management. *Public Management Review*. 21(7), 1076–1100. s. 1083.

³⁰ OECD, 2019. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD Publishing.

³¹ ZUIDERWIJK, A. a CHEN, Y. C., 2021. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*. 38(3), 101577. s. 301.

³² Ministerstvo vnútra Slovenskej republiky, 2025. *Zápis z pracovnej skupiny pre riešenie problematiky umelej inteligencie*(22. 7. 2025). Bratislava: MV SR.

³³ VAN NOORDT, C., VAN DEN BERG, J. a BEKKERS, V., 2023. The dynamics of AI capability and its influence on public administration. *Government Information Quarterly*. 40(4), 101879. s. 213.

³⁴ Ministerstvo vnútra Slovenskej republiky, 2025. *Zápis z pracovnej skupiny pre riešenie problematiky umelej inteligencie*(22. 7. 2025). Bratislava: MV SR.

pri chatbotových službách je nutné dbať na transparentnosť a jasné označenie, že ide o komunikáciu s umelou inteligenciou, nie s človekom. Osobitnú pozornosť si zaslúži využívanie umelej inteligencie v oblasti súdnych a správnych rozhodnutí. V Číne sa experimentuje s tzv. inteligentnými súdmi, kde umelá inteligencia navrhuje verdikty v jednoduchých prípadoch na základe analýzy judikatúry. V Európe je tento trend zatiaľ obmedzený, no objavujú sa diskusie o využití umelej inteligencie pri rozhodovaní o priestupkoch alebo menších správnych deliktoch. Slovenská právna teória vníma, že takýto prístup si vyžaduje prísny dohľad a zachovanie možnosti súdneho prieskumu. V zápise z pracovnej skupiny Ministerstva vnútra Slovenskej republiky sa spomína, že pilotné projekty umelej inteligencie sa pripravujú aj v oblasti správneho konania od spracovania žiadostí o občianstvo až po analýzu dopravných priestupkov.³⁵

Zasadnutie pracovnej skupiny pre riešenie problematiky umelej inteligencie ukazuje, že Slovensko vníma umelú inteligenciu ako nástroj modernizácie verejnej správy. Diskutované projekty zahŕňajú nielen využitie v oblasti kriminality, ale aj v HR procesoch, správe majetku či kybernetickej bezpečnosti. Zástupcovia inštitúcií zdôraznili potrebu systematicky usporiadať dáta, školenia zamestnancov a nastavenie etických mantinelov.³⁶ Táto diskusia dobre korešponduje s odporúčaniami OECD, ktoré považujú kvalitu dát, školenia pracovníkov a etické zásady za základné predpoklady pre zavedenie transparentnej umelej inteligencie vo verejnom sektore.³⁷

Z poznatkov zo zasadnutia Ministerstva vnútra Slovenskej republiky je zrejmé, že téma je aktuálna aj v našich podmienkach, pričom kľúčové je nastaviť jasnú právnu reguláciu, zabezpečiť kvalitu dát a vyškoliť personál. OECD odporúča, aby verejné inštitúcie pri zavádzaní umelej inteligencie vždy uplatňovali princípy transparentnosti, vysvetliteľnosti a ochrany základných práv. Inovácie v rozhodovaní teda musia kráčať ruka v ruke s ochranou zásady zákonnosti a dôvery verejnosti.³⁸

Záver

Uplatňovanie umelej inteligencie vo verejnej správe je dnes realitou, ktorá so sebou prináša zásadné zmeny. Analýza ukázala, že jej prínosy sú zjavné rýchlosť spracovania údajov, konzistentnosť rozhodnutí, odľahčenie úradníkov od rutinných úloh a zvýšená dostupnosť služieb pre občanov. Umelá inteligencia umožňuje

³⁵ Ministerstvo vnútra Slovenskej republiky, 2025. *Zápis z pracovnej skupiny pre riešenie problematiky umelej inteligencie*(22. 7. 2025). Bratislava: MV SR.

³⁶ Ibid.

³⁷ OECD, 2019. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD Publishing

³⁸ OECD, *OECD Principles on Artificial Intelligence*, 2019, dostupné na: <https://oecd.ai/en/ai-principles>

verejnej správe reagovať flexibilnejšie, presnejšie a v niektorých prípadoch aj predvídať problémy skôr, než nastanú. Tieto výhody však nemožno vnímať izolovane, pretože s nimi neoddeliteľne súvisia riziká, ktoré sa dotýkajú samotných základov právneho štátu.

Najzásadnejšími problémami sú otázky transparentnosti, vysvetliteľnosti a právnej zodpovednosti. Automatizované rozhodovanie prináša hrozbu „čiernej skrinky“, keď občan nemá možnosť zistiť, na základe akých úvah systém rozhodol. To môže viesť k oslabeniu zásady zákonnosti a práva na spravodlivý proces. Ďalším rizikom je oslabenie dôvery verejnosti vo verejnú správu, ak bude mať občan pocit, že jeho veci rozhoduje stroj a nie človek. Regulácia na úrovni Európskej únie – GDPR a Akt o umelej inteligencii – poskytuje rámec ochrany, no jej implementácia v praxi bude vyžadovať dôsledný dohľad, audit algoritmov a systematickú kontrolu. OECD a ďalšie medzinárodné organizácie zdôrazňujú, že dôveryhodná umelá inteligencia vo verejnom sektore musí stáť na etike, kvalite dát a dostatočnej príprave ľudí, ktorí s technológiou pracujú.

Pre Slovensko z analýzy vyplýva niekoľko kľúčových odporúčaní. V prvom rade je potrebné systematicky budovať kvalitu dát a informačných systémov, pretože bez spoľahlivých vstupov nie je možné zabezpečiť ani spoľahlivé výstupy umelej inteligencie. Ďalej treba klásť dôraz na vzdelávanie a školenie úradníkov, aby boli schopní nielen technicky pracovať s umelou inteligenciou, ale aj posúdiť jej výsledky v právnom a etickom kontexte. Nevyhnutné je vytvoriť jasný legislatívny rámec, ktorý bude reflektovať požiadavky Aktu o umelej inteligencii a zabezpečí mechanizmy zodpovednosti za rozhodnutia prijaté s využitím umelej inteligencie. V neposlednom rade je potrebné aktívne komunikovať s verejnosťou a posilňovať dôveru občanov v to, že umelá inteligencia vo verejnej správe nie je hrozbou, ale nástrojom, ktorý má slúžiť v ich prospech.

Záverom možno konštatovať, že budúcnosť využívania umelej inteligencie vo verejnej správe závisí od schopnosti štátov vyvážiť technologické inovácie so základnými princípmi právneho štátu. Verejná správa nesmie rezignovať na zásadu zákonnosti, právnu zodpovednosť a ochranu práv občanov, no zároveň musí byť pripravená na využívanie moderných nástrojov, ktoré môžu zefektívniť jej fungovanie. Úlohou právnej vedy a praxe je preto hľadať mechanizmy, ktoré umožnia harmonické spolunažívanie inovácií a právnych istôt a práve to je kľúčová výzva pre Slovensko aj celú Európu v nadchádzajúcich rokoch.

Zoznam použitej literatúry

Monografie a knihy

1. SIMON, H. A., 1997. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. 4. vyd. New York: Free Press. ISBN 978-0684835822.
2. WEBER, M., 1978. *Economy and Society*. Berkeley: University of California Press. ISBN 978-0520035003.

Kapitoly a články v časopisoch

1. ALMIOTTO, F., 2024. When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis. *German Law Review* [online]. forthcoming, s. 1–27. SSRN preprint [cit. 28. 9. 2025]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4578761.
2. ALON-BARKAT, Sh., 2024. Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making. *Journal of Behavioral Public Administration* [online]. 7(1), 1–12. ISSN 2579-5974 [cit. 28. 9. 2025]. Dostupné na: <https://journal-bpa.org/index.php/jbpa/article/view/261>
3. BABŠEK, M. a kol., 2025. Artificial Intelligence Adoption in Public Administration. *Journal of Cyber Policy*. 10(2), 211–230. ISSN 2373-4786.
4. BRKAN, M., 2019. Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond. *International Journal of Law and Information Technology* [online]. 27(2), 91–121. ISSN 0967-0769. doi:10.1093/ijlit/eay017 [cit. 28. 9. 2025]. Dostupné na: <https://academic.oup.com/ijlit/article/27/2/91/5512383>
5. CORVALÁN, J. G., 2018. Digital and Intelligent Public Administration: Transformations in the Era of Artificial Intelligence. *A&C – Revista de Direito Administrativo & Constitucional* [online]. 18(71), 55–77. doi:10.21056/aec.v18i71.857 [cit. 28. 9. 2025]. Dostupné na: <https://revistaaec.com/index.php/revistaaec/article/view/857>.
6. HUBKOVÁ, P., 2024. EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. *Acta Universitatis Carolinae – Iuridica* [online]. 70(2), 22. doi:10.14712/23366478.2024.25 [cit. 28. 9. 2025]. Dostupné na: <https://karolinum.cz/en/casopis/auc-iuridica/rocnik-70/cislo-2/clanek/eu-administrative-decision-making-delegated-to-machines-legal-challenges-and-issues>.
7. JONES, B. D., 2003. Bounded Rationality and Political Science: Lessons from Public Administration and Public Policy. *Journal of Public Administration Research and Theory*. 13(4), 395–412. ISSN 1053-1858.

8. JONES, M. L., 2019. The ethics of predictive policing. *International Journal of Law in Context*. 15(4), 409–425. ISSN 1744-5523. doi:10.1017/S1744552319000183.
9. LINDBLOM, C. E., 1959. The Science of Muddling Through. *Public Administration Review*. 19(2), 79–88. ISSN 0033-3352.
10. VAN NOORDT, C., VAN DEN BERG, J. a BEKKERS, V., 2023. The dynamics of AI capability and its influence on public administration. *Government Information Quarterly*. 40(4), 101879. ISSN 0740-624X. doi:10.1016/j.giq.2023.101879.
11. WIRTZ, B. W. a MÜLLER, W. M., 2019. An integrated artificial intelligence framework for public management. *Public Management Review*. 21(7), 1076–1100. ISSN 1471-9037. doi:10.1080/14719037.2018.1549268.
12. ZUIDERWIJK, A., CHEN, Y.-C. a SALEM, F., 2021. Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly* [online]. 38(3), 101577. ISSN 0740-624X. doi:10.1016/j.giq.2021.101577 [cit. 28. 9. 2025]. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S0740624X21000512>

Právne predpisy

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. L 119, 4.5.2016, s. 1–88.
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. L 202, 12.7.2024, s. 1–108.
3. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov – GDPR). *Úradný vestník Európskej únie*, L 119, 4.5.2016, s. 1–88.
4. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a menia niektoré legislatívne akty Únie (Akt o umelej inteligencii). *Úradný vestník Európskej únie*, L 202, 12.7.2024, s. 1–108.

Medzinárodné dokumenty

1. OECD, 2019. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Paris: OECD Publishing.

2. OECD, 2019. *OECD Principles on Artificial Intelligence* [online]. Paris: OECD. [cit. 28. 9. 2025]. Dostupné na: <https://oecd.ai/en/ai-principles>.

Interné dokumenty

1. MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, 2025. *Zápis z pracovnej skupiny pre riešenie problematiky umelej inteligencie* (22. 7. 2025). Bratislava: MV SR.

Kontaktné údaje

Mgr. Alan Lengyel

lengyel23@uniba.sk

Katedra správneho práva a environmentálneho práva Univerzita
Komenského v Bratislave, Právnická fakulta

SKÚMANIE MATERIÁLNEJ STRÁNKY PRIESTUPKU UMELOU INTELEGENCIU

INVESTIGATION OF THE MATERIAL ASPECT OF THE OFFENCE WITH ARTIFICIAL INTELLIGENCE

Martin Krajčí¹

Abstrakt: Cieľom príspevku je vyhodnotiť využiteľnosť umelej inteligencie na skúmanie a vyhodnocovanie materiálnej stránky priestupku vo vzťahu ku konkrétnemu skutku s možnosťou využitia výsledku vyprodukovaného umelou inteligenciou ako odôvodnenia rozhodnutia vo veci. Príspevok poukáže aj na možné neprávne otázky, ako napríklad filozofické a morálne aspekty posudzovania ľudského konania prostredníctvom systému, ktorý nedokáže vnímať a precítiť subjektívnu stránku skutku. Príspevok tak môže pomôcť odpovedať na otázku, či je využívanie umelej inteligencie vhodné aj na rozhodovanie o právach, právom chránených záujmoch a povinnostiach vo verejnej správe.

Kľúčové slová: priestupok, materiálna stránka, umelá inteligencia

Abstract: The aim of the contribution is to evaluate the usability of artificial intelligence for examining and evaluating the material aspects of an misdemeanor in relation to a specific act with the possibility of using the result produced by artificial intelligence as a justification for a decision in the case. The contribution will also point out possible non-legal issues, such as the philosophical and moral aspects of assessing human action through a system that cannot perceive and feel the subjective aspect of the act. The contribution can help answer the question of whether the use of artificial intelligence is also suitable for making decisions about rights, legally protected interests and obligations in public administration.

Key words: misdemeanor, material aspect, artificial intelligence

¹ Univerzita Komenského v Bratislave, Právnická fakulta.

Úvod

Agenda prejednávania priestupkov v správnom konaní tvorí veľkú časť činnosti všeobecných správnych orgánov, ktorými sú najmä okresné úrady,² alebo príslušné útvary Policajného zboru.³ Vydanie meritórneho rozhodnutia je pritom už iba zhmotnením celého konania o priestupku do jedného individuálneho aktu, ktorému predchádza zložitý proces vykonávania procesných úkonov, vyhľadávania a vyhodnocovania dôkazov a uplatňovania správnej úvahy. Celý popísaný proces má zásadný vplyv na zákonnosť a správnosť konania a následného rozhodnutia vo veci, avšak ak aj celý tento postup bol bez vady, vada v rozhodnutí môže zapríčiniť zmarenie celého konania. V tomto smere môže aj umelá inteligencia napomôcť správnym orgánom, a to napríklad v časti vyhodnocovania naplnenia materiálnej stránky priestupku, ktorej odôvodnenie je neraz (aj časovo) náročné a môže obsahovať rozsiahle právne úvahy viažuce sa ku konkrétnemu skutku. Uvedená činnosť by tak bola súčasťou automatizovaného posudzovania, ktorého definíciu už vytvoril Ústavný súd Slovenskej republiky.⁴ K materiálnej stránke priestupku sa na druhej strane častokrát pristupuje mechanicky, pričom po naplnení formálnej stránky priestupku sa prezumuje aj naplnenie stránky materiálnej, čo však nie je správny prístup. Skúmanie materiálnej stránky priestupku by malo byť obligatórnou súčasťou konania o priestupku a výsledok tohto skúmania by mal správny orgán zhmotniť v rozhodnutí, nakoľko aj priamo zákon o priestupkoch⁵ explicitne zakotvuje materiálnu stránku v legálnej definícii priestupku ako „*konanie, ktoré porušuje alebo ohrozuje záujem spoločnosti*“.⁶ Následne v legálnej definícii priestupku je explicitne definovaná aj formálna stránka vyjadrujúca, že priestupkom je iba konanie, ktoré „*je za priestupok výslovne označené v tomto alebo v inom zákone*“,⁴ pričom medzi materiálnou a formálnou stránkou je použitá spojka „a“. Na základe uvedeného je zrejmé, že na spáchanie priestupku je potrebné osobitne skúmať naplnenie ako materiálnej, tak aj formálnej stránky priestupku a teda nie je správne vždy prezumovať naplnenie formálnej stránky z dôvodu naplnenia stránky materiálnej.

² § 52 ods. 1 zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

³ § 52 ods. 2 zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

⁴ Nález Ústavného súdu Slovenskej republiky z 10. novembra 2021, sp. zn. PL. ÚS 25/2019-117.

⁵ Zákon Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

⁶ § 2 ods. 1 zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

Materiálna stránka priestupku

Aj keď úvod in medias res pojednával o materiálnej stránke priestupku, je vhodné uviesť základné teoretické východiská k tejto problematike.

O materiálnej stránke priestupku možno vo všeobecnosti uviesť, že vyjadruje mieru ohrozenia alebo porušenia záujmu, ktorý je chránený zákonom.⁷ Ako už bolo uvedené, nie je správne automaticky spájať splnenie formálnej stránky priestupku so stránkou materiálnou, aj keď obe spolu úzko súvisia. Vo všeobecnosti možno uviesť, že v prípade okolností hodných osobitného zreteľa, ktoré vylučujú ohrozenie alebo porušenie zákonom chráneného záujmu, nebude materiálna stránka naplnená, pričom Najvyšší správny súd Českej republiky tento výklad použil pri prekročení rýchlosti v obci o 2 km/h na úseku, ktorý bol prehľadný, jednalo sa o výjazd z obce a zároveň doprava bola v danom úseku riedka.⁸ V tomto smere aj Najvyšší súd Slovenskej republiky vyjadril názor, že pre zodpovednosť za priestupok je rozhodujúca aj materiálna stránka priestupku, a nie len jeho stránka formálna,⁹ pričom v ďalšom rozhodnutí *expressis verbis* uviedol, že „*pri skúmaní zodpovednosti za priestupok je správny orgán povinný zisťovať nielen naplnenie formálnej stránky priestupku, ale aj naplnenie jeho materiálnej stránky...*“.¹⁰

Materiálna stránka priestupku tak môže byť použitá ako korektív spoločenskej škodlivosti, kedy odlišuje skutok od beztrestného konania alebo od trestného činu, alebo ako kritérium na určenie druhu sankcie a jej výmery, nakoľko aj dva skutky formálne kvalifikované ako rovnaký priestupok môžu byť s ohľadom na materiálnu stránku rôzne závažné a preto sa v oboch prípadoch môže páchatelovi uložiť iná sankcia s rôznou výmerou,¹¹ čo potvrdil aj Najvyšší súd Slovenskej republiky.¹² Zároveň zákon o priestupkoch *expressis verbis* ustanovuje, že „*pri určení druhu sankcie a jej výmery sa prihliadne na závažnosť priestupku, najmä na spôsob jeho spáchania a na jeho následky, na okolnosti, za ktorých bol spáchaný...*“.¹³ Týmto priamo zákon ukladá príslušnému orgánu na prejednanie priestupku povinnosť, aby pri určovaní sankcie a jej výmery zohľadnil materiálnu stránku priestupku.

⁷ HAMULÁKOVÁ, Zuzana, HORVAT, Matej: Základy správneho práva trestného. Bratislava: Wolters Kluwer, 2019. s. 85.

⁸ Rozsudok Najvyššieho správneho súdu Českej republiky z 14. decembra 2009, sp. zn. 5 As 104/2008-45.

⁹ Rozsudok Najvyššieho súdu Slovenskej republiky z 20. marca 2014, sp. zn. 8Sžo/25/2013.

¹⁰ Rozsudok Najvyššieho súdu Slovenskej republiky z 30. mája 2018, sp. zn. 10Asan/23/2017.

¹¹ FIALA, Zdeněk, FRUMAROVÁ, Kateřina, HORZINKOVÁ, Eva, ŠKUREK, Martin: Správní právo trestní. Praha: Leges, 2017. s. 65.

¹² Rozsudok Najvyššieho súdu Slovenskej republiky z 2. júna 2011, sp. zn. 8 Sžo 163/2010, R zn. R 90/2012.

¹³ § 12 ods. 1 zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

Nakoľko spoločenská škodlivosť priestupku nie je právnym poriadkom definovaná, bude závisieť od správnej úvahy príslušného správneho orgánu vo vzťahu ku konkrétnemu skutku.¹⁴ A práve táto činnosť, ktorá môže byť subjektívne náročná a vyžaduje zohľadnenie veľkého množstva faktorov, by mohla byť vykonávaná prostredníctvom umelej inteligencie, čím by mohlo dôjsť k administratívne odľahčeniu správnych orgánov a tým aj k urýchleniu celého správneho konania. Zároveň však je potrebné položiť otázku, či by naozaj vyhodnocovanie materiálnej stránky mohlo (alebo malo) byť zverené umelej inteligencii.

Právny rámec umelej inteligencie v Slovenskej republike

Pre odpoveď na otázku, či právny poriadok Slovenskej republiky umožňuje použitie umelej inteligencie na skúmanie materiálnej stránky priestupku, je potrebné v prvom rade určiť okruh právnych predpisov, ktoré môžu taký postup upravovať.

Práve konanie o priestupkoch je v oblasti správneho práva špecifické, a to dvojitou subsidiaritou. Uvedené znamená, že v bežných podmienkach je konanie o priestupku upravené zákonom o priestupkoch a subsidiárne Správnym poriadkom. Nakoľko však hmotnoprávna a aj procesnoprávna úprava priestupkov je obsiahnutá aj v ďalších právnych predpisoch, v tomto prípade sa ako *lex specialis* použije úprava osobitného predpisu, a úprava zo zákona o priestupkoch sa uplatní iba subsidiárne.¹⁵ Na základe uvedeného nepostačuje vyhodnotiť aplikovateľnosť umelej inteligencie v procese konania o priestupku iba v úprave zákona o priestupkoch a Správneho poriadku, ale aj v úprave ďalších predpisov obsahujúcich osobitné procesné ustanovenia.¹⁶

Analýzou ustanovení zákona o priestupkoch je možné dospieť k záveru, že uvedený predpis *de lege lata* upravuje možnosť vykonať procesný úkon iba príslušným orgánom, a to či už v postavení objasňujúceho orgánu, alebo orgánu oprávnenému prejednať priestupok. Zákon v tomto smere nedefinuje ani to, že v mene tohto orgánu konajú konkrétne fyzické osoby, in concreto zamestnanci. Uvedené však nachádzame v právnej vede, ktorá predikuje osobné zložky, resp. vykonávateľov

¹⁴ MATES, Pavel, a kol.: Základy správneho práva trestného. 7. vydání. Praha: C. H. Beck, 2017. s. 62.

¹⁵ VRABKO, Marián a kolektív: Správne právo procesné. Osobitná časť. 2. aktualizované a doplnené vydanie. Šamorín: Heuréka, 2018. s. 289.

¹⁶ Napríklad § 151 až 153 zákona č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 55 až 60 zákona č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov, § 92 a 93 zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov.

verejnej správy, ako súčasť organizácie verejnej správy.¹⁷ Logickým výkladom ustanovení zákona o priestupkoch prichádzame k rovnakému záveru, nakoľko orgán verejnej správy nemôže konať sám, obdobne ako to je v prípade konania právnickej osoby.¹⁸ In kontextu vyššie uvedeného možno konštatovať, že procesný úkon podľa zákona o priestupkoch môže vykonať iba príslušný orgán, resp. jeho zamestnanec a úkon vykonaný umelou inteligenciou by bol nezákonný z dôvodu porušenia princípu legality, podľa ktorého *„štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobilom, ktorý ustanoví zákon.“*¹⁹

Obdobnú úpravu obsahuje Správny poriadok s tým rozdielom, že citovaný predpis už *expressis verbis* upravuje zamestnancov príslušného orgánu.²⁰ Úprava využitia umelej inteligencie však rovnako absentuje a preto ju v zmysle zásady legality nebude možné uplatniť v procese správneho konania.

In fine, skúmané osobitné predpisy rovnako neumožňujú vykonávať procesné úkony prostredníctvom umelej inteligencie, na základe čoho možno konštatovať, že v zmysle právneho poriadku *de lege lata* bude môcť viesť konanie stále iba konkrétna fyzická osoba v pozícii zamestnanca príslušného orgánu.

V oblasti využívania umelej inteligencie v podmienkach verejnej správy *de lege ferenda* je významným krokom schválenie Aktu o umelej inteligencii²¹ na pôde Európskej únie, pričom tento akt má priamy účinok aj pre Slovenskú republiku. Uvedené nariadenie *expressis verbis* umožňuje spracúvanie osobných údajov umelou inteligenciou v pôsobnosti orgánu verejnej správy za účelom zvýšenia efektivity verejnej správy.²² Nariadenie však možno v súčasnosti označiť za „štartovaciu čiaru“, nakoľko umožňuje využívanie umelej inteligencie vo verejnej správe iba v kontrolovanom experimentálnom prostredí, čo však možno považovať za prvý krok v jej následnom zavádzaní do aplikačnej praxe.

Na citované nariadenie v podmienkach Slovenskej republiky nadväzuje legislatívny proces č. LP/2025/401, ktorý obsahuje návrh zákona *„o organizácii štátnej správy v oblasti umelej inteligencie a o zmene a doplnení niektorých zákonov“* a ktorý v čase

¹⁷ Napríklad VRABKO, Marián a kol.: Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2018. s. 7 alebo CEPEK, Branislav a kolektív: Správne právo hmotné. Všeobecná časť. Bratislava: Wolters Kluwer, 2018. s. 35.

¹⁸ § 20 Občianskeho zákonníka v znení neskorších predpisov.

¹⁹ Čl. 2 ods. 2 Ústavy Slovenskej republiky v znení neskorších predpisov.

²⁰ Napríklad § 9 až 12, § 22 a 25 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

²¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

²² Čl. 59 ods. 1 písm. a) bod v Aktu o umelej inteligencii.

prezentovania príspevku na konferencii bol v štádiu vyhodnocovania pripomienkového konania.

V neposlednom rade je potrebné uviesť, že právny poriadok Slovenskej republiky de lege lata upravuje používanie informačných technológií vo verejnej správe, pričom legálna definícia informačných technológií²³ obsahuje iba demonštratívny výpočet možných technológií a tým pro futuro umožňuje rozšírenie aj o umelú inteligenciu bez potreby priamej novely.

Zhrnutím predchádzajúcich odsekov možno konštatovať, že poriadok Slovenskej republiky de lege lata neupravuje možnosť vydávania rozhodnutí vo veci priestupkov za použitia umelej inteligencie, pričom táto činnosť je stále zverená výlučne správnym orgánom, resp. ich zamestnancom. Situácia de lege ferenda však môže byť odlišná, nakoľko aj Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky uvádza digitalizáciu verejnej správy ako dlhodobú prioritu, pričom expressis verbis pomenúva aj podmienku zmeny Správneho poriadku²⁴ ako predpoklad digitalizácie verejnej správy.²⁵ Využívanie umelej inteligencie v rámci rozhodovacej právomoci vo verejnej správe pro futuro pritom pripúšťa aj Najvyšší súd Slovenskej republiky.²⁶

Riziká spojené s používaním umelej inteligencie

Aj keď používanie umelej inteligencie je dnes populárne a môže výrazne znížiť administratívnu vyťaženosť správnych orgánov v rozhodovacom procese, je v tomto smere potrebné zvážiť aj otázku zabezpečenia údajov a nastavenia hraníc, v rámci ktorých bude môcť umelá inteligencia samostatne konať.

Národná jednotka pre riešenie kybernetických incidentov Národného bezpečnostného úradu taktiež upozorňuje na riziká spojené s využívaním umelej inteligencie, pričom osobitne zdôrazňuje možný únik informácií, s ktorými umelá inteligencia pracuje, porušenie ochrany súkromia alebo cieľené vytváranie zaujatých výsledkov priamo zo strany algoritmov umelej inteligencie.²⁷ Ďalšie riziko môže vzniknúť z nesprávneho nastavenia algoritmov umelej inteligencie hneď v úvode, pričom tieto algoritmy môžu následne nesprávne vyhodnocovať vstupné údaje a tým môžu vytvoriť nesprávne výstupy, čím môže dôjsť k vade úkonu s vplyvom na správnosť, alebo aj zákonnosť celého konania o priestupku a vydaného rozhodnutia.

²³ § 2 ods. 1 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

²⁴ Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

²⁵ Stratégia digitálnej transformácie Slovenska 2030, dostupné online <https://mirri.gov.sk/wp-content/uploads/2019/06/Strategia-digitalnej-transformacie-Slovenska-2030.pdf>.

²⁶ Rozsudok Najvyššieho súdu Slovenskej republiky z 10. mája 2018, sp. zn. 1Sžf/97/2016.

²⁷ Dostupné online na stránke Národného bezpečnostného úradu <https://www.sk-cert.sk/sk/hrozby-spojene-s-technologiami-umelej-inteligencie/index.html>.

V neposlednom rade je potrebné vnímať aj riziká spojené s cieľným útokom na kybernetickú infraštruktúru verejnej správy, ako sa to stalo napríklad v roku 2025 pri útoku na Kataster portál. Je nepochybné, že zvýšená digitalizácia verejnej správy kladie čoraz vyššie nároky na zabezpečenie informačných systémov, čo sa však spravidla prejavuje v zvýšenej cene obstarávania a prevádzkovania informačných systémov a taktiež v náročnejšom využívaní týchto systémov ich užívateľmi.

Výhody spojené s používaním umelej inteligencie

Aj keď v predchádzajúcej časti príspevku boli uvedené najzásadnejšie riziká spojené s využitím umelej inteligencie, jej využitie nepochybne prináša aj viaceré benefity.

Ako už bolo uvedené v tomto príspevku, posudzovanie materiálnej stránky prístupku môže byť rozsahom veľmi náročné a zároveň každý zamestnanec správneho orgánu bude subjektívne vyhodnocovať závažnosť skutku odlišne. Aj keď by sa každý zamestnanec mal pri vyhodnocovaní skutku riadiť zákonmi, internými (zjednocujúcimi) inštrukciami a judikatúrou, nikdy nebude možné zabezpečiť rovnaký prístup k vyhodnocovaniu závažnosti skutku. V tomto je zamestnanec správneho orgánu ovplyvnený množstvom faktorov, okrem iného výchovou, náboženstvom, kultúrou ale aj vlastnými záujmami. Pravdepodobne inak vyhodnotí skutok spočívajúci v prekročení najvyššej dovolenej rýchlosti zamestnanec správneho orgánu, ktorý je vo voľnom čase závodným pretekárom a jeho záujmom sú autá a rýchla jazda, ako zamestnanec, ktorý ani nie je držiteľom vodičského oprávnenia.

A práve popísanú nejednotnosť v rozhodovacej činnosti môže odstrániť využitie umelej inteligencie, ktorá na základe vopred určených kritérií vždy rovnako a objektívne posúdi závažnosť skutku.

Z uvedeného vyplýva ďalšia výhoda, ktorou by bolo pravdepodobné skrátenie konania o prístupku, nakoľko časť procesu by po zabezpečení celého podkladového spisového materiálu bola vykonaná automaticky umelou inteligenciou bez potreby náročného skúmania príslušným zamestnancom, čím by došlo k dôslednejšiemu naplnení zásady rýchlosti a hospodárnosti konania.²⁸ Taktiež by použitím umelej inteligencie bolo zabezpečené, že spracovanie údajov nebude iba rýchle, ale aj presné, čo umožní prijímať informovanejšie a bezvadné rozhodnutia.²⁹ Zároveň s tým je však spojená potreba digitalizácie prístupkových spisov, aby boli všetky

²⁸ § 3 ods. 4 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

²⁹ ŠIMKO, Ervín, MESARČÍK, Matúš. Vplyv regulácie umelej inteligencie na legislatívu kybernetickej bezpečnosti vo verejnej správe. 1. diel. In: Acta Facultatis Iuridicae Universitatis Comenianae. [online]. Bratislava: Diel 43, č. 2, s. 165. Dostupné online: <https://afi.flaw.uniba.sk/index.php/AFI/issue/view/74/75>.

podklady a listiny prístupné aj v elektronickej verzii, pričom tento krok by bol v oblasti verejnej správy finančne nákladný a pravdepodobne aj časovo zdĺhavý.

Prípadová štúdia posúdenia materiálnej stránky umelou inteligenciou

Nasledujúci text obsahuje prípadovú štúdiu v podobe vyhodnotenia materiálnej stránky fiktívneho priestupku prostredníctvom umelej inteligencie, in concreto Google Geminy.

Pre upresnenie je potrebné uviesť, že konverzácia bola vykonaná v rámci jedného vlákna, aby na seba odpovede priamo nadväzovali. Cieľom štúdie bolo v prvom rade zistiť, či umelá inteligencia vôbec rozoznáva materiálnu stránku priestupku od stránky formálnej. V prípade pozitívnej odpovede je následne druhým cieľom na základe zmeny skutkových okolností zistiť, či umelá inteligencia bude naozaj schopná rozlišovať závažnosť skutkov a tak potvrdiť, resp. vyvrátiť naplnenie materiálnej stránky priestupku.

Otázka:

„Čo je materiálna stránka priestupku?“

Odpoveď Google Geminy:

„Materiálna stránka priestupku sa zaoberá spoločenskou škodlivosťou konania. Zatiaľ čo formálna stránka definuje priestupok na základe splnenia formálnych znakov (napríklad porušenie zákona), materiálna stránka sa pýta, do akej miery je toto konanie nebezpečné pre spoločnosť.“

Inými slovami, aj keď niekto formálne poruší zákon, jeho čin nemusí byť potrestaný, ak sa preukáže, že jeho spoločenská škodlivosť je zanedbateľná alebo chyba úplne...“

Otázka:

„Vieš spoľahlivo posúdiť materiálnu stránku priestupku?“

Odpoveď Google Geminy:

„Ako jazykový model nemôžem spoľahlivo posúdiť materiálnu stránku priestupku. Na to, aby sa dospelo k záveru, či je konanie dostatočne spoločensky škodlivé na to, aby bolo považované za priestupok, je potrebná dôkladná analýza konkrétnych okolností prípadu. Tieto okolnosti posudzujú príslušné orgány štátnej správy, najčastejšie polícia alebo správny orgán.“

Môžem ti však poskytnúť informácie a vysvetlenia, ktoré ti pomôžu pochopiť, čo sa pri posudzovaní materiálnej stránky zohľadňuje:

- *Charakter a závažnosť následku: Aká škoda vznikla (napríklad finančná škoda, zranenie, ohrozenie verejnej bezpečnosti)?*
- *Miera ohrozenia chránených záujmov: Aké hodnoty boli ohrozené (napríklad život, zdravie, majetok, verejný poriadok)?*
- *Spôsob spáchania: Bol čin spáchaný úmyselne alebo z neobľahlosti?*
- *Okolnosti prípadu: Dôvod konania, čas a miesto spáchania.*

Príklad:

Formálne prejsť cez cestu na červenú je priestupok. Ak sa tak stane v noci na prázdnej ceste, bez prítomnosti iných áut či chodcov, materiálna stránka môže byť posúdená ako nepatrná. Naopak, ak sa tak stane počas rannej špičky pred školou, kde sú deti, spoločenská škodlivosť je výrazne vyššia a konanie má materiálnu stránku priestupku.

Zhrnutie:

Na posúdenie materiálnej stránky priestupku je potrebný kontext a znalosť všetkých skutočností, čo je úloha pre príslušné štátne orgány. Ja ti viem vysvetliť, aké kritériá sa na to používajú."

Otázka:

„Ak vodič nezastaví vozidlom na značke "STOJ, daj prednosť v jazde" v nočných hodinách, pričom na ceste nie sú iné vozidlá a z križovatky má vodič dobrý výhľad, naplňa tento skutok materiálnu stránku priestupku?"

Odpoveď Google Gemini:

„Na základe teoretického výkladu, ktorý sa zohľadňuje pri posudzovaní materiálnej stránky priestupku, by sa dalo argumentovať, že v takomto prípade skutok nenaplňuje materiálnu stránku priestupku.

Dôvody sú nasledovné:

- 1. **Chýba spoločenská škodlivosť:** Konanie vodiča (nezastavenie na značke „STOJ, daj prednosť v jazde“) síce porušilo dopravné predpisy (formálna stránka), ale z dôvodu nočnej hodiny a absencie iných vozidiel a chodcov neohrozilo život, zdravie ani majetok iných osôb.*
- 2. **Zanedbateľná miera ohrozenia:** Keďže mal vodič dostatočný rozhľad a križovatka bola prázdna, nevzniklo žiadne reálne nebezpečenstvo kolízie. Miera ohrozenia pre spoločnosť je tak v tomto konkrétnom prípade nulová alebo zanedbateľná."*

Otázka:

„Bola položená rovnaká otázka ako predchádzajúca s tým rozdielom, že nočná doba bola zmenená na dennú dobu."

Odpoveď Google Gemini:

„Táto situácia je z hľadiska posudzovania materiálnej stránky priestupku komplikovanejšia ako v noci a názory sa môžu líšiť, hoci pravdepodobnosť naplnenia materiálnej stránky je vyššia ako v prípade nočnej prevádzky."

Otázka:

„Čo ak sa skutok stane v noci, ale o dve ulice ďalej prebieha festival?"

Odpoveď Google Gemini:

„Prítomnosť festivalu o dve ulice ďalej v noci opäť mení kontext situácie a zvyšuje pravdepodobnosť naplnenia materiálnej stránky priestupku.

Argumenty pre naplnenie materiálnej stránky:

1. **Formálne porušenie zákona:** Porušenie § 20 ods. 2 písm. b) Zákona o cestnej premávke ostáva nezmenené – vodič nezastavil na značke "Stoj, daj prednosť v jazde".
2. **Zvýšená koncentrácia osôb a vozidiel v okolí:** Festival generuje zvýšený pohyb ľudí (chodcov, účastníkov festivalu, organizátorov) a vozidiel (taxíky, zásobovanie, policajné hliadky, súkromné autá) aj v neskorých nočných hodinách a v širšom okolí miesta konania.
3. **Nepredvídateľné správanie:** V blízkosti festivalov môžu byť ľudia pod vplyvom alkoholu, rozptýlení alebo menej ostražití, čo zvyšuje riziko náhleho vstupu do vozovky.
4. **Potenciálna prítomnosť záchranných zložiek:** V oblasti festivalov často hliadkuje polícia, záchranná služba alebo hasiči, ktorí sa môžu kedykoľvek a rýchlo presúvať..."

Vyhodnotenie prípadovej štúdie

Zhodnotením prvého cieľu spočívajúceho v zistení, či umelá inteligencia rozlišuje materiálnu stránku priestupku je možné uviesť, že v predloženej prípadovej štúdii dokázala umelá inteligencia rozoznať faktory, ktoré budú mať na posúdenie materiálnej stránky vplyv. Jednalo sa o podstatné skutkové okolnosti ako miesto a čas spáchania a situácia v cestnej premávke.

Druhý cieľ možno hodnotiť ako splnený čiastočne, nakoľko umelá inteligencia sa na jednej strane dokázala prikloniť k naplneniu, resp. nenaplneniu materiálnej stránky na základe zmien skutkového stavu, nesprávne však kvalifikovala porušenie pravidiel cestnej premávky. In concreto, nerešpektovanie dopravnej značky „STOJ, daj prednosť v jazde“ umelá inteligencia kvalifikovala ako porušenie § 20 ods. 2 písm. b) zákona č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o cestnej premávke“), pričom však správna kvalifikácia je porušenie § 3 ods. 2 písm. b) zákona o cestnej premávke.

Záver

Zhrnutím právneho poriadku Slovenskej republiky de lege lata je možné konštatovať, že využitie umelej inteligencie na vykonávanie procesného úkonu alebo uplatňovanie správnej úvahy v konaní o priestupku nie je možné a takýto úkon by bol konaním ultra vires, čím by mohlo dôjsť k vade konania a vydaného rozhodnutia.

Aj prípadová štúdia poukázala na skutočnosť, že umelá inteligencia (in concreto Google Gemini) nie je pripravená s dostatočnou presnosťou a spoľahlivosťou vyhodnocovať naplnenie materiálnej stránky priestupku, nakoľko odpovede boli nejednoznačné a porušenie zákona bolo nesprávne kvalifikované.

Zároveň je však potrebné uviesť, že právny poriadok, a to tak aj nadnárodné pramene práva, už postupne vytvárajú priestor pre využívanie umelej inteligencie v oblasti verejnej správy, avšak tento proces je postupný a časovo náročný a musí byť zavŕšený prijatím novej právnej úpravy, čo potvrdzuje aj právna veda.³⁰

Pri využití umelej inteligencie však nebude postačovať iba formálne skúmať legalitu jej použitia, ale aj iné otázky, ako napríklad etickosť a morálnosť. Tieto otázky budú ako filozofické, tak aj psychologické, pričom cieľom bude zistiť, či je vôbec spravodlivé a možné, aby ľudské správanie bolo vyhodnocované počítačom. Dokáže umelá inteligencia posudzovať aj znaky subjektívnej stránky skutkovej podstaty priestupku? Dokáže umelá inteligencia zohľadňovať objekt skutkovej podstaty priestupku v poňatí reálneho záujmu ľudskej spoločnosti? Aj to sú otázky, na ktoré bude potrebné zodpovedať pred zavedením umelej inteligencie do konania o priestupku.

Aj keď je nepochybné, že umelá inteligencia by mohla konanie o priestupku zrýchliť a zefektívniť, právny poriadok a ani spoločnosť (vrátane verejnej správy) na tento krok podľa môjho názoru ešte pripravené nie sú. Správnou otázkou ale nie je, či sa umelá inteligencia začne využívať v konaní o priestupku. Dnešná otázka znie, kedy sa začne využívať a v akom rozsahu.

Zoznam použitej literatúry

1. ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022. ISBN 978-80-7676-548-1.
2. CEPEK, Branislav a kolektív: Správne právo hmotné. Všeobecná časť. Bratislava: Wolters Kluwer, 2018, 492 s. ISBN 978-80-8168-784-6.
3. FIALA, Zdeněk, FRUMAROVÁ, Kateřina, HORZINKOVÁ, Eva, ŠKUREK, Martin: Správni právo trestní. Praha: Leges, 2017, 304 s. ISBN 978-80-7502-219-6.
4. HAMULÁKOVÁ, Zuzana, HORVAT, Matej: Základy správneho práva trestného. Bratislava: Wolters Kluwer, 2019, 308 s. ISBN 978-80-571-0142-0.
5. Hrozby spojené s technológiami umelej inteligencie, dostupné online <https://www.sk-cert.sk/sk/hrozby-spojene-s-technologiami-umelej-inteligencie/index.html>.
6. MATES, Pavel, a kol.: Základy správneho práva trestného. 7. vydání. Praha: C. H. Beck, 2017, 239 s. ISBN 978-80-7400-680-7.
7. Nález Ústavného súdu Slovenskej republiky z 10. novembra 2021, sp. zn. PL. ÚS 25/2019-117.

³⁰ ANDRAŠKO, Jozef a kol.: Regulačné výzvy e-governmentu v Slovenskej republike v kontexte práva Európskej únie. Praha: Wolters Kluwer ČR, 2022. s. 351.

8. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).
9. Rozsudok Najvyššieho správneho súdu Českej republiky z 14. decembra 2009, sp. zn. 5 As 104/2008-45.
10. Rozsudok Najvyššieho súdu Slovenskej republiky s 30. mája 2018, sp. zn. 10Asan/23/2017.
11. Rozsudok Najvyššieho súdu Slovenskej republiky z 10. mája 2018, sp. zn. 1Sžf/97/2016.
12. Rozsudok Najvyššieho súdu Slovenskej republiky z 2. júna 2011, sp. zn. 8 SŽo 163/2010, R zn. R 90/2012.
13. Rozsudok Najvyššieho súdu Slovenskej republiky z 20. marca 2014, sp. zn. 8SŽo/25/2013.
14. Stratégia digitálnej transformácie Slovenska 2030, dostupné online <https://mirri.gov.sk/wp-content/uploads/2019/06/Strategia-digitalnej-transformacie-Slovenska-2030.pdf>.
15. ŠIMKO, Ervín, MESARČÍK, Matúš. Vplyv regulácie umelej inteligencie na legislatívu kybernetickej bezpečnosti vo verejnej správe. 1. diel. In: Acta Facultatis Iuridicae Universitatis Comenianae. [online]. Bratislava: Diel 43, č. 2, s. 165. Dostupné online: <https://afi.flaw.uniba.sk/index.php/AFI/issue/view/74/75>.
16. Ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov.
17. VRABKO, Marián a kol.: Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2018, 338 s. ISBN 978-80-89603-8.
18. VRABKO, Marián a kolektív: Správne právo procesné. Osobitná časť. 2. aktualizované a doplnené vydanie. Šamorín: Heuréka, 2018, 382 s. ISBN 978-80-8173-049-9.
19. Zákon č. 124/1992 Zb. o Vojenskej polícii v znení neskorších predpisov
20. Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
21. Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
22. Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.
23. Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.
24. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

25. Zákon Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

Kontaktné údaje

Mgr. Martin Krajči

krajci30@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Katedra správneho a environmentálneho práva

VYUŽITIE DIGITALIZÁCIE ÚDAJOV A UMELEJ INTELIGENCIE PRI OCHRANE BEZPEČNOSTNÝCH ZÁUJMOV ŠTÁTU¹

USE OF DATA DIGITIZATION AND ARTIFICIAL INTELLIGENCE IN PROTECTING THE SECURITY INTERESTS OF THE STATE

Michal Aláč²

Abstrakt: Postupná dynamizácia vzťahov v spoločnosti spôsobená technologickým pokrokom sa v práci bezpečnostných zložiek odráža dvojakým spôsobom. Na jednej strane poskytuje možnosť automatizovať spracovanie dát, čo skracuje dobu vyhodnocovania informácií a tým je práca bezpečnostných zložiek efektívnejšia a naplňa to preventívnu funkciu ich úloh. Zároveň však dynamizácia vzťahov a technologický pokrok ponúka väčšie možnosti pre hrozby, resp. záujmové osoby, a tým vzniká veľké množstvo dát, s ktorými sa musia bezpečnostné zložky vysporiadať. Práve to vo vymedzenom rozsahu vytvára priestor pre použitie funkcionalít umelej inteligencie. Špecifické aspekty získavania informácií, ich uchovávanie a následného analytického spracovania a záverečného vypracovania spravodajskej informácie alebo inej formy produktu, ktorý bude odstúpený zákonnému príjemcovi, však neumožňujú v súčasnosti tieto procesy plne automatizovať. Funkcionality umelej inteligencie môžu spravodajským službám spracovať údaje, pri ktorých nie je potrebné využiť právno-bezpečnostnú úvahu, v oveľa kratšom čase, vo väčšom objeme a v súvislostiach (napr. rôzne jazykové mutácie), ktoré by bolo náročné zanalyzovať prostredníctvom ľudských zdrojov, ale nie je možné ich použiť ako výlučnú možnosť.

Kľúčové slová: bezpečnostný záujem, spravodajské služby, analýza, umelá inteligencia

Abstract: The gradual dynamization of relations in society caused by technological progress is reflected in the work of security forces in two ways. On the one hand, it provides the opportunity to automate data processing,

¹ Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0543.

² Právnická fakulta Univerzity Komenského v Bratislave, katedra správneho práva a environmentálneho práva.

which shortens the time for evaluating information, making the work of security forces more efficient and fulfilling the preventive function of their tasks. At the same time, however, the dynamization of relations and technological progress offer greater opportunities for threats, or persons of interest, and thus creates a large amount of data that security forces have to deal with. This is precisely what creates space for the use of artificial intelligence functionalities to a limited extent. However, the specific aspects of obtaining information, its storage and subsequent analytical processing and final preparation of intelligence information or another form of product that will be transferred to the legal recipient do not currently allow these processes to be fully automated. Artificial intelligence functionalities can allow intelligence services to process data that does not require legal and security considerations in a much shorter time, in a larger volume and in contexts (e.g. various language mutations) that would be difficult to analyze using human resources, but they cannot be used as an exclusive option.

Key words: security interest, intelligence services , security analysis, artificial intelligence

Úvod

Postupná dynamizácia vzťahov v spoločnosti spôsobená technologickým pokrokom sa v práci bezpečnostných zložiek odráža dvojakým spôsobom. Na jednej strane poskytuje možnosť automatizovať spracovanie dát, čo skracuje dobu vyhodnocovania informácií a tým je práca bezpečnostných zložiek efektívnejšia a naplňa to preventívnu funkciu ich úloh. Zároveň však dynamizácia vzťahov a technologický pokrok ponúka väčšie možnosti pre hrozby, resp. záujmové osoby, a tým vzniká veľké množstvo dát, s ktorými sa musia bezpečnostné zložky vysporiadať. Aby bolo možné zanalyzovať možnosti využitia digitalizácie dát a využitie umelej inteligencie pri ochrane bezpečnostných záujmov štátu, musíme najskôr zodpovedať niekoľko fundamentálnych otázok. Čo sú bezpečnostné záujmy štátu? Kto zodpovedá za ochranu bezpečnostných záujmov štátu? O aké procesy vo verejnej správe, resp. v spoločnosti pri ochrane bezpečnostných záujmov ide?

Bezpečnostné záujmy Slovenskej republiky

Pojem bezpečnostný záujem štátu nie je možné presne definovať. Ide o všeobecný pojem, ktorý v sebe odzrkadľuje záujem štátu zachovať pre svojich občanov určitú dlhodobu udržateľnú pozitívnu kvalitu spoločenských vzťahov. **Bezpečnostný záujem** štátu môžeme chápať aj ako právne relevantný záujem štátu, ktorého ochrana je nevyhnutná na udržanie stability, vnútorného poriadku, suverenity,

integrity či bezpečného fungovania verejnej moci, a ktorý môže legitímne odôvodniť obmedzenia určitých práv alebo povinností v konkrétnych situáciách.

Kvalitatívne a kvantitatívne požiadavky na definíciu pojmu bezpečnostný záujem štátu vieme čiastočne odvodiť z právnej úpravy pôsobnosti a úloh jednotlivých zložiek bezpečnostného systému štátu, resp. *in concreto* bezpečnostného systému Slovenskej republiky.

Zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov v ust. § 1 ods. 1 definuje Policajný zbor ako ozbrojený bezpečnostný zbor, ktorý plní úlohy vo veciach vnútorného poriadku, bezpečnosti, boja proti zločinnosti vrátane jej organizovaných foriem a medzinárodných foriem.

Podľa ust. § 2 ods. 1 cit. zákona Policajný zbor najmä

- a) spolupôsobí pri ochrane základných práv a slobôd, najmä pri ochrane života, zdravia, osobnej slobody a bezpečnosti osôb a pri ochrane majetku,
- b) odhaľuje trestné činy a zisťuje ich páchatelov,
- c) vedie boj proti terorizmu a organizovanému zločinu,
- d) zabezpečuje kontrolu hraníc,
- e) spolupôsobí pri zabezpečovaní verejného poriadku; ak bol porušený, robí opatrenia na jeho obnovenie,
- f) vykonáva vyšetrovanie trestných činov a
- g) odhaľuje priestupky a ich páchatelov.³

Ďalším orgánom, ktorého prioritnou úlohou je ochrana bezpečnostných záujmov Slovenskej republiky je Slovenská informačná služba, ktorú zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších zákonov definuje ako všeobecnú spravodajskú a bezpečnostnú službu, ktorá plní úlohy vo veciach ochrany ústavného zriadenia, vnútorného poriadku, bezpečnosti štátu a ochrany zahraničnopolitických a hospodárskych záujmov štátu v rozsahu vymedzenom týmto zákonom. Podľa ust. § 2 ods. 1 cit. zákona Slovenská informačná služba v rozsahu svojej pôsobnosti získava, sústreďuje a vyhodnocuje najmä informácie najmä o

- a) činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť Slovenskej republiky,
- b) činnosti smerujúcej proti bezpečnosti Slovenskej republiky,
- c) aktivite cudzích spravodajských služieb,
- d) organizovanej trestnej činnosti a terorizme,

³ Bližšie pozri § 2 ods. 1 zákona č. 171/1993 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.

e) ohrození alebo úniku informácií a vecí chránených podľa osobitného predpisu alebo medzinárodných zmlúv alebo medzinárodných protokolov.⁴

Vojenské spravodajstvo ako spravodajská služba, ktorá plní úlohy na úseku obrany, obranyschopnosti a bezpečnosti Slovenskej republiky v pôsobnosti Ministerstva obrany Slovenskej republiky plní obdobné úlohy ako Slovenská informačná služba.⁵

Na základe analýzy uvedených právnych predpisov možno dospieť k záveru, že medzi elementárne bezpečnostné záujmy Slovenskej republiky patrí ochrana ústavného zriadenia, územnej celistvosti, zvrchovanosti a vnútorného poriadku Slovenskej republiky, potláčanie kriminality (čím je zároveň zabezpečovaná ochrana života, zdravia a majetku občanov Slovenskej republiky), ochrana utajovaných skutočností, a to v úzkej súvislosti, ako aj ochrana hospodárskych záujmov Slovenskej republiky. Pri definovaní bezpečnostných záujmov Slovenskej republiky je potrebné poukázať na skutočnosť, že Slovenská republika, rovnako ako ostatné štáty, pri hodnotení bezpečnostných záujmov musí posudzovať viacero rovín, resp. viacero vzťahov. Ide predovšetkým o bezpečnostný záujem Slovenskej republiky reprezentujúcej záujem spoločnosti *in generalis* (občania Slovenskej republiky a osoby s legálnym pobytom) vs. individuálny záujem konkrétnej osoby (napr. záujem na ochrane niektorých informácií v správnom, súdnom alebo v trestnom konaní), záujem Slovenskej republiky, resp. občanov Slovenskej republiky reprezentovaných konkrétnym štátnym orgánom vs. cudzí štátni príslušníci. Každý štát primárne ochraňuje všeobecný bezpečnostný záujem pred súkromným, a rovnako prioritne poskytuje ochranu bezpečnostným záujmom svojich občanov pred cudzími štátnymi príslušníkmi. Takýto postup je úplne prirodzený a súdmi aprobovaný napríklad pri ochrane národnej bezpečnosti, resp. vnútorného poriadku v konaní o povolení pobytu.⁶

Orgány štátu zabezpečujúce bezpečnostné záujmy

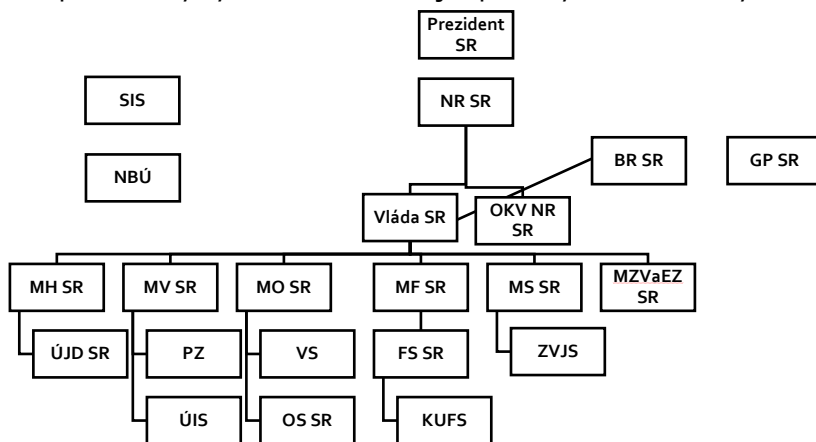
V nadväznosti na skutočnosť, že neexistuje exaktná legálna definícia pojmu bezpečnostný záujem, je možné viacerými spôsobmi definovať príslušné orgány na jeho ochranu. V širšom zmysle možno zodpovednosť za ochranu bezpečnostných záujmov priznať veľkému počtu orgánov, ktoré plnia rôzne čiastkové úlohy. Toto vnímanie však môže pôsobiť zmätočne, pretože úloha jednotlivých aktérov je značne rozdielna, kde na jednej strane môžeme niektoré orgány definovať ako tvorcov politík a koncepcií, niektoré ako administrátorov a niektoré orgány aktívne získavajú informácie a vykonávajú bezpečnostné opatrenia na zabezpečenie ochrany bezpečnostných záujmov Slovenskej republiky.

⁴ Bližšie pozri § 2 ods. 1 zákona č. 46/1993 Z. z.

⁵ Pozri § 4 až 7 zákona č. 500/2022 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

⁶ II. ÚS 480/2014

Bezpečnostný systém Slovenskej republiky v širšom zmysle:



Uvedené grafické znázornenie, ako bolo uvedené, poskytuje náhľad na všetky zúčastnené subjekty na ochrane bezpečnostných záujmov Slovenskej republiky.

Na účely tohto článku sa však zameriame len na orgány, ktorých hlavnou úlohou je súbor špecifických činností pri ochrane záujmov štátu, a to spravodajských služieb a Národného bezpečnostného úradu. Ako už bolo uvedené spravodajské služby plnia úlohy na úseku ochrany ústavného zriadenia, vnútorného poriadku, bezpečnosti štátu a ochrany zahraničnopolitických a hospodárskych záujmov Slovenskej republiky. Tieto úlohy plnia prostredníctvom foriem, metód a prostriedkov spravodajskej činnosti. Zjednodušene môžeme konštatovať, že získavajú, sústreďujú a vyhodnocujú informácie spôsobilé ohroziť bezpečnostné záujmy Slovenskej republiky.

Na tieto účely sú spravodajské služby oprávnené v rozsahu svojej pôsobnosti požadovať od štátnych a iných orgánov, právnických a fyzických osôb poskytnutie pomoci, podkladov a informácií, ktoré môžu prispieť k objasneniu skutočností dôležitých na plnenie úloh ustanovených príslušnými zákonmi.⁷ V rozsahu potrebnom na plnenie úloh ustanovených zákonom majú spravodajské služby právo na sprístupnenie a poskytnutie informácií a osobných údajov z informačných systémov orgánov verejnej moci. Orgány verejnej moci sú povinné žiadosti spravodajskej služby o sprístupnenie a poskytnutie informácií a osobných údajov zo svojich informačných systémov vyhovieť. Tieto údaje sa poskytujú a sprístupňujú bez

⁷ § 15 ods. 1 zákona č. 46/1993 Z. z.

§ 32 ods. 1 zákona č. 500/2022 Z. z.

súhlasu dotknutej osoby a o ich poskytnutí a sprístupnení sa tieto osoby neinformujú, a to z dôvodu, aby nedošlo ohrozeniu alebo zmareniu úloh spravodajskej služby alebo k ohrozeniu jej príslušníkov.

Oprávnenie na poskytnutie údajov má aj Národný bezpečnostný úrad, ktorému toto oprávnenie vyplýva z ust. § 16 ods. 1 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podľa ktorého sú jedným z podkladov na vykonanie bezpečnostnej previerky navrhovanej osoby

- a) informácie o bezpečnostnej spoľahlivosti navrhovanej osoby z evidencií Policajného zboru, Slovenskej informačnej služby a Vojenského spravodajstva,
- b) informácie o bezpečnostnej spoľahlivosti navrhovanej osoby od ďalších štátnych orgánov a iných právnických osôb, týkajúce sa navrhovanej osoby,
- c) informácie vyžiadané od obce, v ktorej má navrhovaná osoba trvalý pobyt alebo prechodný pobyt,
- d) informácie z previerok vykonaných Policajným zborom, Slovenskou informačnou službou alebo Vojenským spravodajstvom o bezpečnosti prostredia, v ktorom navrhovaná osoba žije a pohybuje sa, a o možnosti výskytu bezpečnostných rizík.

Formy participácie na ochrane bezpečnostných záujmov v rámci rozhodovacích procesov a možnosti využitia umelej inteligencie

Ako už bolo uvedené, spravodajské služby získavajú, sústreďujú a vyhodnocujú informácie o skutočnostiach, ktoré sú spôsobilé ohroziť bezpečnostné záujmy Slovenskej republiky.

Po spravodajsko-analytickom spracovaní spravodajská služba odstúpi spravodajský produkt vo forme spravodajskej informácie. Spravodajskou informáciou sa podľa vyhlášky Národného bezpečnostného úradu č. 48/2019 Z. z. o administratívnej bezpečnosti rozumie utajovaná skutočnosť, ktorej pôvodcom je spravodajská služba, obsahujúca informácie získané metódami a prostriedkami podľa osobitného predpisu.⁸ Proces vzniku spravodajskej informácie je náročným procesom analytického spracovania informácií získaných spravodajskou činnosťou. Každá informácia, ktorá slúži ako podklad na vypracovanie spravodajskej informácie, je vyhodnocovaná prostredníctvom tzv. systému 4x4. Ide o hodnotiaci systém, ktorý hodnotí hodnovernosť zdroja a hodnovernosť informácie, a to tak, že zdroju aj informácii je pridelený jeden zo stupňov hodnovernosti. Hodnovernosť zdroja informácie sa označuje písmenami abecedy:

⁸ Zákon č. 46/1993 Z. z., zákon č. 500/2022 Z. z.

- A – ak nie sú pochybnosti o hodnovernosti zdroja, alebo ak je informácia poskytnutá zo zdroja, ktorý sa v minulosti ukázal ako spoľahlivý vo všetkých prípadoch,
- B – zdroj, od ktorého sa získané informácie ukázali ako spoľahlivé vo väčšine prípadov,
- C – zdroj, od ktorého sa získané informácie ukázali ako nespoľahlivé vo väčšine prípadov,
- D – ak hodnovernosť zdroja nemôže byť hodnotená.

Spoľahlivosť informácie sa označuje číslicami:

- 1 – ak je správnosť informácie nespochybniteľná,
- 2 – ak informáciu zdroj osobne pozná, ale osobne ju nepozná spravodajský dôstojník,
- 3 – ak informáciu zdroj osobne nepozná, ale táto bola potvrdená inou informáciou,
- 4 – ak informáciu zdroj osobne nepozná a nemôže byť potvrdená.

Za verifikovanú informáciu sa označuje informácia, ktorá v hodnotení obsahuje kombináciu písmena „A“ alebo „B“ s číslom „1“ alebo „2“. Informácia, ktorá v hodnotení obsahuje ľubovoľnú kombináciu písmena „C“ alebo „D“ alebo ľubovoľnú kombináciu čísla „3“ alebo „4“ je považovaná za neverifikovanú informáciu.⁹ Uvedené hodnotenie vykonáva priamo príslušník spravodajskej služby, ktorý informáciu získal, a to na základe svojej predchádzajúcej empirie so zdrojom informácie. Pri vyhodnocovaní hodnovernosti zdroja informácie a samotnej informácie spravodajský dôstojník, t. j. príslušník spravodajskej služby vyhodnocuje aj okolnosti získania informácie, ktoré môžu mať vplyv na jej vyhodnotenie (napr. osoba konajúca v prospech spravodajskej služby, ktorá informáciu poskytla, nevidela dobre na pozorovaný objekt alebo dobre nerozumela). Z uvedeného dôvodu sa domnievame, že nie je možné využiť spôsobilosti umelej inteligencie pri tomto prvotnom spôsobe vyhodnocovania informácií. Jej využitie je však možné pri vyhodnocovaní informácií získaných, resp. poskytnutých z evidencií a informačných systémov orgánov verejnej moci, kde nie sú pochybnosti o správnosti, pravdivosti a úplnosti informácií. Ďalšou možnosťou, kde je možné využiť umelú inteligenciu je pri komparatívnom spracovaní informácií obsiahnutých v informačných systémoch spravodajskej služby vo vzájomnej súvislosti alebo pri ich porovnaní s informáciami z informačných systémov orgánov verejnej moci, ktoré môžu poukázať na niektoré špecifické väzby medzi jednotlivými informáciami. Taktiež je možné využiť umelú inteligenciu ako jeden z prostriedkov použitých pri záverečnom celkovom vyhodnotení informácií a spracovaní spravodajského produktu vo forme spravodajskej informácie. Ľudský

⁹ STIERANKA, J.: Základy spravodajskej činnosti, Bratislava: Akadémia PZ v Bratislave, 2008, s. 107.

faktor teda nie je možné pri vypracovaní spravodajskej informácie nahradiť umelou inteligenciou.

Spravodajské služby odstupujú svoje poznatky aj vo forme podkladov pre rozhodnutia správnych orgánov. Ide napríklad podklady rozhodnutia v konaní o pobyte cudzincov podľa § 125 ods. 6 zákona č. 404/2011 Z. z. o pobyte cudzincov v znení neskorších predpisov, podľa ktorého je Slovenská informačná služba povinná do 10 dní poskytnúť príslušnému policajnému útvaru na základe jeho žiadosti vyjadrenie potrebné na posúdenie žiadosti o udelenie prechodného pobytu a žiadosti o udelenie trvalého pobytu na päť rokov. Obdobnú povinnosť poskytnúť podklady k osobe žiadateľa má Slovenská informačná služba aj podľa zákona č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Podľa § 14 ods. 4 zákona č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) v znení neskorších predpisov si Ministerstvo vnútra Slovenskej republiky alebo krajské riaditeľstvo Policajného zboru vždy vyžiada vyjadrenie Slovenskej informačnej služby, ak ide o posúdenie spoľahlivosti fyzickej osoby, ktorá žiada o udelenie licencie na prevádzkovanie bezpečnostnej služby, fyzickej osoby, ktorá je štatutárnym orgánom alebo členom štatutárneho orgánu právnickej osoby, ktorá žiada o udelenie licencie na prevádzkovanie bezpečnostnej služby, fyzickej osoby, ktorá má najmenej 15 % majetkový podiel v právnickej osobe, vedúceho organizačnej zložky podniku, zodpovedného zástupcu, prokuristu, splnomocnenca prevádzkovateľa, vedúceho podniku zahraničnej osoby a fyzickej osoby, ktorá vykonáva fyzickú ochranu alebo pátranie v objekte osobitnej dôležitosti. Pri poskytovaní podkladov do konaní uvedených v tejto demonštratívnej enumerácii opätovne Slovenská informačná služba, prípadne Vojenské spravodajstvo vyhodnotia informácie, ktorými disponujú a vypracujú odpoveď na konkrétne dožiadanie správneho orgánu. Ani pri vypracovaní týchto odpovedí, ktoré majú slúžiť ako podklad rozhodnutia nie je možné využívať výlučne umelú inteligenciu, ale je potrebné použiť právno-bezpečnostnú úvahu. Umelú inteligenciu, resp. iný digitalizovaný systém je možné využiť jedine v prípade, že spravodajské služby na základe automatizovanej lustrácie vo svojich informačných systémoch konštatujú, že k osobe, ktorej sa týka dožiadanie, nedisponuje žiadnymi negatívnymi poznatkami. Samostatnou oblasťou ochrany bezpečnostných záujmov Slovenskej republiky je vydávanie rozhodnutí, pri ktorých majú spravodajské služby a Národný bezpečnostný úrad postavenie správneho orgánu. Ide napríklad o konanie vo veciach služobného pomeru príslušníkov, kedy má spravodajská služba postavenie služobného úradu.¹⁰

¹⁰ Zákon č. 73/1998 Z. z., zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Spravodajské služby a Národný bezpečnostný úrad majú postavenie správnych orgánov aj v konaní o bezpečnostnej previerke, kde spravodajské služby vo vzťahu k svojim príslušníkom, zamestnancom alebo k uchádzačom o prijatie do služobného pomeru alebo do pracovného pomeru majú postavenie správneho orgánu.¹¹ Národný bezpečnostný úrad vedie konanie vo vzťahu k ostatným navrhovaným osobám a k právnickým osobám a fyzickým osobám, ktoré požiadali o vydanie osvedčenia priemyselnej bezpečnosti. V konaniach o bezpečnostnej previerke, resp. v konaní previerke priemyselnej bezpečnosti správny orgán aplikuje správno-bezpečnostnú úvahu, na základe záverov ktorej vydá osobe, ktorá spĺňa podmienky osvedčenie o bezpečnostnej spoľahlivosti, resp. osvedčenie o previerke priemyselnej bezpečnosti. V prípade, ak na základe právno-bezpečnostnej úvahy dospeje k záveru, že osoba nespĺňa zákonné predpoklady na vznik oprávnenia na oboznamovanie sa s utajovanými skutočnosťami, vydá rozhodnutie. Pri uvedených postupoch nie je možné nahradiť správno-bezpečnostnú úvahu funkcionalitami umelej inteligencie. Je však možné použiť umelú inteligenciu ako jeden podporných prostriedkov pre vyhodnotenie informácií z bezpečnostného dotazníka a informačných systémov.

Záver

Pri ochrane bezpečnostných záujmov Slovenskej republiky je nevyhnutné, aby spravodajské služby v rámci spravodajsko-analytickej činnosti dôkladne vyhodnotili informácie, ktorými disponujú a následne zákonným príjemcom odstúpili spravodajský produkt. Ako bolo vyššie uvedené, podkladom spravodajskej informácie sú informácie získané spravodajskou službou, ktorých pravdivosť a relevancia musí byť vyhodnotená spravodajským dôstojníkom, ktorý ich získal. Pri tejto činnosti možno využiť funkcionality umelej inteligencie ako podporný prostriedok, avšak domnievame sa, že nie je v súčasnosti možné nahradiť ľudský faktor. Zároveň je však potrebné konštatovať, že umelá inteligencia predstavuje prostriedok, ktorý môže mimoriadne zefektívniť spravodajskú činnosť v oblasti zberu dát, ako aj v oblasti ich parciálneho vyhodnocovania.

Zoznam použitej literatúry

1. STIERANKA, J.: Základy spravodajskej činnosti, Bratislava: Akadémia PZ v Bratislave, 2008
2. VAŠKO, A., KULIK, J., ČUHA, R. Zákon o Slovenskej informačnej službe. Komentár. 1. vydanie. Bratislava: Wolters Kluwer Sr s. r. o., 2024

¹¹ § 18 zákona č. 215/2004 Z. z.

3. VAŠKO, A., KULIK, J., ČUHA, R. Zákon o Vojskom spravodajstve. Komentár. 1. vydanie. Bratislava: Wolters Kluwer Sr s. r. o., 2024

Zákony

1. Zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov
2. Zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov
3. Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov
4. Zákon č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
5. Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
6. Zákon č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) v znení neskorších predpisov
7. Zákon č. 404/2011 Z. z. o pobyte cudzincov v znení neskorších predpisov
8. Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
9. Zákon č. 500/2022 Z. z. o Vojskom spravodajstve v znení neskorších predpisov
10. Vyhláška Národného bezpečnostného úradu č. 48/2019 Z. z. o administratívnej bezpečnosti

Súdne rozhodnutia

1. Nález Ústavného súdu Slovenskej republiky sp. zn. II. ÚS 480/2014

Kontaktné údaje

JUDr. Michal Aláč, PhD.

michal.alac@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

Katedra správneho práva a environmentálneho práva

VÝZVY IMPLEMENTÁCIE NÁSTROJOV UMELEJ INTELIGENCIE VO VEREJNEJ SPRÁVE

CHALLENGES OF IMPLEMENTING ARTIFICIAL INTELLIGENCE TOOLS IN PUBLIC ADMINISTRATION

Stanislava Sopková¹

Abstrakt: Cieľom predloženého príspevku je analyzovať možné riešenia pri zavádzaní umelej inteligencie do oblasti verejnej správy, a to najmä s ohľadom na výber vhodných modelov umelej inteligencie, ktoré naplňajú požiadavky kladené na jej používanie Aktom o umelej inteligencii (AI Act). Príspevok sa zameriava na identifikáciu spôsobov, akými môže verejná správa implementovať moderné technologické nástroje bez neprimeraného zásahu do základných ľudských práv a slobôd, pričom reflektuje na potrebu zachovania transparentnosti a zodpovednosti pri rozhodovacích procesoch. V tejto súvislosti sa príspevok venuje použitiu algoritmickému systému *SyRI* v Holandskom kráľovstve, ktorý nadobúda zásadný rozmer aj pri aktuálnom implementovaní autonómnych systémov do verejnej správy v európskom priestore tým, že analyzuje dôsledky uvedeného súdneho sporu a poukazuje na jeho dopad na vnímanie legitimacy využívania umelej inteligencie vo verejnej správe. Ambíciou predloženého príspevku nie je poskytnúť vyčerpávajúce legislatívne návrhy v oblasti úpravy zodpovednosti štátu za škodu spôsobenú pri výkone verejnej správy pri použití umelej inteligencie, ale usiluje sa identifikovať možné technické riešenia jednotlivých modelov umelej inteligencie, ktoré môžu prispieť k minimalizácii rizika vydávania nezákonných rozhodnutí v rozhodovacích procesoch, ktoré by viedli k aktivácii zodpovednostných mechanizmov.

Kľúčové slová: umelá inteligencia, verejná správa, zodpovednosť za škodu

Abstract: The aim of this paper is to analyze possible solutions for introducing artificial intelligence into public administration, particularly with regard to the selection of suitable artificial intelligence models that meet the requirements for its use set out in the AI Act. The paper focuses on identifying ways in which public administration can implement modern technological tools without excessive interfering with fundamental human rights and freedoms, while

¹ Univerzita Komenského v Bratislave, Právnická fakulta.

reflecting on the need to maintain transparency and accountability in decision-making processes. In this context, the paper discusses the use of the *SyRI* algorithmic system in the Netherlands, which has become crucial in the current implementation of autonomous systems in public administration in Europe. The paper analyzes the consequences of the abovementioned case and points out its impact on the perception of the legitimacy of using artificial intelligence in public administration. The ambition of this paper is not to provide exhaustive legislative proposals for regulating the state's liability for damage caused by the exercise of public administration when using artificial intelligence in decision-making, but rather to identify possible technical solutions that can contribute to minimizing the risk of issuing unlawful decisions that would lead to activating liability mechanisms.

Key words: artificial intelligence, public administration, liability for damage

Úvod

Dynamický vývoj umelej inteligencie (ďalej aj ako „AI“) v posledných rokoch predstavuje nielen nový celospoločenský fenomén, ale zároveň podnecuje široké spektrum vedeckých disciplín k jej intenzívnemu výskumu a ďalšiemu rozvoju. Otázky týkajúce sa interpretácie umelej inteligencie, maximalizácie jej praktickej využiteľnosti pri zachovaní transparentnosti, ako aj jej legislatívne ukotvenie, sa čoraz výraznejšie dostávajú do popredia spoločenskej a vedeckej diskusie. Tieto otázky zároveň prinášajú nový diapazón problémov, ktoré prispievajú k určitému stupňu spoločenského skepticizmu voči novej fáze digitalizácie a technickej transformácie. Právne vedy nepredstavujú žiadnu výnimku, práve naopak, zohrávajú kľúčovú úlohu pri jej ďalšom napredovaní.²

Prvým komplexným legislatívnym nástrojom prijatým na pôde Európskej únie je Nariadenie (EÚ) 2024/1689 (ďalej len „Akt o umelej inteligencii“ alebo „AIA“).³ Uvedené nariadenie predstavuje základný rámec pre právnu úpravu systémov umelej inteligencie pri ich integrovaní do vnútroštátnych právnych poriadkov, ktorého cieľom je zabezpečiť ich bezpečné, transparentné, harmonizované a eticky prijateľné využívanie naprieč členskými štátmi.

² BABŠEK, Matej – RAVŠEJ, Dejan – UMEK, Lan – ARISTOVNIK, Aleksander. Artificial Intelligence Adoption in Public Administration: An Overview of Top-Cited Articles and Practical Applications. In *AI 2025*, vol. 6 (3), 44. Dostupné online z: <<https://doi.org/10.3390/ai6030044>>.

³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizačné pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

Napriek tomu, že sa vo verejnej diskusii umelá inteligencia často prezentuje ako netransparentný a autonómny systém, v skutočnosti existujú rôzne prístupy a konkrétne modely umelej inteligencie navrhnuté tak, aby naplňali požiadavky transparentnosti, interpretovateľnosti a umožňovali následný výkon ľudskej kontroly. Práve tie majú potenciál významne prispieť k dôveryhodnému použitiu umelej inteligencie vo vysokorizikových oblastiach, akou je aj verejná správa.

Cieľom predkladaného príspevku preto nie je predkladať konkrétne legislatívne návrhy týkajúce sa zodpovednosti štátu za škodu spôsobenú nezákonným rozhodnutím vydaným prostredníctvom umelej inteligencie, ale identifikovať vhodné modely umelej inteligencie spĺňajúce požiadavky na riadne fungovanie verejnej správy. Zámerom je ponúknuť také riešenia, ktoré môžu nielen prispieť k zvýšeniu efektívnosti verejnej správy, ale zároveň napomôcť zmierniť jej ekonomické zaťaženie, posilniť postavenie orgánov verejnej správy voči spravovaným subjektom a v konečnom dôsledku aj minimalizovať riziko vydávania nezákonných rozhodnutí, ktoré budú viesť k vzniku zodpovednosti štátu za spôsobenú škodu.

Systém SyRI a jeho vplyv na budúci vývoj umelej inteligencie vo verejnej správe

Prípád *SyRI* (*Systeem Risico Indicatie*)⁴ z roku 2020 predstavuje jeden z prvých významných vnútroštátnych súdnych sporov s presahom do európskeho priestoru, v ktorom sa posudzovala zlučiteľnosť používania algoritmických systémov na hodnotenie rizikovosti osôb orgánmi verejnej moci so základnými ľudskými právami. Systém *SyRI* bol spravovaný holandským Ministerstvom sociálnych vecí a práce (*Ministerie van Sociale Zaken en Werkgelegenheid*), ktoré v spolupráci s ďalšími príslušnými orgánmi verejnej správy prostredníctvom algoritmických operácií zhromažďovalo, uschovávalo a zabezpečovalo vzájomnú výmenu údajov pochádzajúcich z viacerých verejných databáz za účelom identifikácie osôb, ktoré boli systémom vyhodnotené ako potenciálne rizikové, a to predovšetkým v súvislosti so zneužívaním systému sociálneho zabezpečenia. Haagsky vnútroštátny súd (*Rechtbank Den Haag*) (ďalej len „súd“) posudzoval predovšetkým zlučiteľnosť použitia systému *SyRI* orgánmi verejnej moci so záväzkami vyplývajúcimi z článku 8 ods. 2 Európskeho dohovoru o ochrane ľudských práv a základných slobôd v znení dodatkových protokolov (ďalej len „Európsky dohovor“), a to najmä s právom

⁴ Napriek tomu, že systém *SyRI* bol automatizovaným systémom na hodnotenie rizikovosti, nešlo o systém využívajúci pokročilé techniky strojového učenia, ako ich poznáme pri umelej inteligencii dnes, ale o tzv. „rule-based“ systém. K tomu bližšie pozri: ALTY, J. L. – GUIDA, G. The Use of Rule-based System Technology for the Design of Man-Machine Systems. In *IFAC Proceedings Volumes*, vol. 18 (10), 1985, p. 21-41. Dostupné online z: <[https://doi.org/10.1016/S1474-6670\(17\)60196-4](https://doi.org/10.1016/S1474-6670(17)60196-4)>.

jednotlivcov na súkromie a ochranu ich osobných údajov, ktoré vykladal v kontexte princípov GDPR.⁵

Spracovávanie osobných údajov prostredníctvom systému *SyRI* prebiehalo v dvoch fázach. V prvej fáze boli zozbierané údaje o fyzických a právnických osobách z viacerých databáz, ktoré boli následne pseudonymizované tak, že každý záznam bol nahradený jedinečným číselným identifikátorom. Tieto údaje boli následne automatizovane porovnávané s preddefinovaným modelom rizika. Výstupom tejto fázy bol zoznam potenciálne rizikových prípadov, ktorý bol postúpený príslušnému útvaru na ďalšiu analýzu. V druhej, analytickej fáze, boli tieto výstupy podrobené manuálnemu vyhodnoteniu z hľadiska ich vhodnosti na ďalšie preverovanie, pričom sa zohľadňovali jednotlivé okolnosti konkrétneho prípadu.⁶

Súd poukázal na to, že problematickým aspektom systému *SyRI* bola najmä jeho nedostatočná transparentnosť, spočívajúca v utajení metodiky vyhodnocovania rizikovosti osôb. Príslušné orgány verejnej správy ani potenciálne rizikové osoby nemali prístup k informáciám o tom, ktoré konkrétne ukazovatele a kritériá systém použil pri generovaní výstupov. Netransparentnosť systému *SyRI* viedla k absencii možnosti efektívnej kontroly a zároveň znemožnila presvedčivé posúdenie, či systém mohol viesť k diskriminačným výsledkom. Deficit zodpovednosti za výstupy systému *SyRI* a nemožnosť spätnej kontroly v konečnom dôsledku predstavovali pre súd neprimeraný zásah do práva na súkromie podľa článku 8 Európskeho dohovoru.⁷

Štát namietal, že systém *SyRI* nemožno považovať za model strojového učenia využívaný na účely prediktívnej analýzy. Zároveň uviedol, že jeho výstupy neboli priamo použité ako podklady pre rozhodovanie príslušných orgánov verejnej správy. Napriek tomu súd konštatoval, že predmetné tvrdenia nepovažoval za rozhodujúce. Zdôraznil, že napriek absencii plne autonómneho rozhodovacieho mechanizmu mali výstupy systému *SyRI* vplyv na ďalšie preverovanie konkrétnych osôb, čím sa fakticky podieľali na rozhodovacích procesoch verejnej správy bez možnosti spätnej kontroly alebo čitateľnosti interných procesov systému príslušnými orgánmi.⁸ Zastávame názor, že v kontexte požiadaviek vyplývajúcich z Aktu o umelej inteligencii⁹ by tento

⁵ RACHOVITSA, Adamantia – JOHANN, Niclas. *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*. In *Human Rights Law Review*, vol. 22 (2), 2022, s. 3 a 4. [online]. [cit. 25-09-2025]. Dostupné online z: <<https://doi.org/10.1093/hrlr/ngaco10>>.

⁶ Rozhodnutie Rechtbank Den Haag z 5. februára 2020, sp. zn. C/09/550982/HA ZA 18-388 (ECLI:NL:RBDHA:2020:1878). Dostupné online z: <https://www.escri-net.org/wp-content/uploads/2020/09/ecli_nl_rbdha_2020_1878.pdf>.

⁷ Ibidem.

⁸ Ibidem.

⁹ Ak by bol systém *SyRI* implementovaný do holandského právneho poriadku po prijatí Aktu o umelej inteligencii, domnievame sa, že by spadal pod článok 6 ods. 2 v spojení s bodom 5 Prílohy č. 3 tohto Nariadenia.

model mohol byť v súčasnosti posúdený ako nezlučiteľný s požiadavkami kladenými na vysokorizikové systémy¹⁰.

V čiastkovom závere k tejto časti dodávame, že systém *SyRI* poukazuje na zreteľné riziká, ktoré sú spojené s používaním automatizovaných systémov v oblasti verejnej správy, a to hlavne v prípadoch, ak absentuje dostatočná úroveň transparentnosti, kontroly a efektívne mechanizmy vyvodzovania zodpovednosti. Napriek tomu, že systém *SyRI* nefungoval ako pokročilé nástroje strojového učenia typické pre súčasné modely umelej inteligencie, tak právne a etické výzvy, ktoré boli predmetom prípadu, vyvstávajú aj pri nasadzovaní nástrojov AI do činností orgánov verejnej správy a jej rozhodovacích procesov. Zároveň poukazuje na skutočnosť, že predpokladom pre nasadzovanie nástrojov umelej inteligencie do verejnej správy nie je len ich legislatívna regulácia, ale aj technologická schopnosť modelov AI zabezpečiť dostatočnú mieru interpretovateľnosti a spätnej kontroly.

K Aktu o umelej inteligencii a úprave transparentnosti

Akt o umelej inteligencii predstavuje prvú právne záväznú reguláciu umelej inteligencie, ktorou sa Európska únia usiluje usmerňovať vývoj, používanie a uvádzanie systémov umelej inteligencie na trh, s cieľom zabezpečiť ochranu základných ľudských práv a slobôd. Nevyhnutným predpokladom k dosiahnutiu stanoveného cieľa je zavádzanie takých modelov umelej inteligencie, ktoré sú dôveryhodné a etické, pričom budú podliehať ľudskému dohľadu, vykazovať vysokú mieru vysvetliteľnosti a spätnej overiteľnosti interných procesov a v oblasti verejnej správy budú predovšetkým naplňovať požiadavku transparentnosti rozhodovacích procesov.¹¹

Európska únia v rámci AIA kategorizuje jednotlivé systémy umelej inteligencie podľa úrovne rizika, a to od systémov s neprijateľným rizikom, cez vysokorizikové systémy, až po systémy minimálneho alebo žiadneho rizika.¹² V kontexte verejnej správy možno považovať za najrelevantnejšie najmä ustanovenia týkajúce sa vysokorizikových systémov, na ktoré sa vzťahujú prísne požiadavky uvedené v nariadení.

V tejto súvislosti považujeme za dôležité venovať zvýšenú pozornosť predovšetkým článku 13 a 14 a článku 50 Aktu o umelej inteligencii. Článok 13 ods. 1 AIA ukladá prevádzkovateľom povinnosť zabezpečiť takú mieru transparentnosti, aby umožnila

¹⁰ K tomu bližšie pozri: MESARČÍK, Matúš – GYURÁSZ, Zoltán a kolektív. *Právo a umelá inteligencia. Prvé vydanie*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 76.

¹¹ Bod 27 Preambuly k Aktu o umelej inteligencii.

¹² MESARČÍK, Matúš. Regulácia umelej inteligencie v Európe. In MESARČÍK, Matúš, GYURÁSZ, Zoltán a kolektív. *Právo a umelá inteligencia. Prvé vydanie*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 70.

nasadzujúcim subjektom prevádzky systémov umelej inteligencie primeranú interpretáciu ich výstupov, avšak ponecháva otvorený priestor na určenie primeraného rozsahu a spôsobu jej dosiahnutia, pričom v článku 14 ods. 4 písm. c) dodáva, že „ľudský dohľad primerane interpretuje výstupy vysokorizikového systému AI s prihliadnutím [...] na dostupné interpretačné nástroje a metódy“. V článku 50 ods. 1 Aktu o umelej inteligencii zavádza povinnosť informovať fyzické osoby o tom, že „interagujú so systémom AI, pokiaľ to nie je zrejmé“, čím vo vzťahu k jej adresátom vytvára ďalšiu, tentokrát informačnú úroveň transparentnosti.

Napriek tomu, že európsky zákonodarcia viaže požiadavku transparentnosti systémov umelej inteligencie na ich interpretovateľnosť, ponecháva členským štátom značný priestor na rozhodnutie o jej rozsahu.¹³ Táto flexibilita vyvoláva zásadné otázky týkajúce sa výberu vhodného modelu umelej inteligencie pre vysokorizikové procesy,¹⁴ akými sú aj rozhodovacie procesy vo verejnej správe. Ako veľmi musí byť systém AI interpretovateľný, aby spĺňal požiadavky na transparentnosť a dôveryhodnosť? Aké konkrétne riziká a výzvy sú spojené s nasadzovaním menej interpretovateľných *black box* modelov v porovnaní s transparentnejšími *white box* systémami umelej inteligencie? Do akej miery sú dostupné *explainable* metódy umelej inteligencie schopné zmierniť riziká použitia *black box* modelov?

Modely umelej inteligencie a ich špecifické výzvy pre použiteľnosť vo verejnej správe

Vzhľadom na dynamický nárast využívania umelej inteligencie v rôznych oblastiach spoločenského a verejného života je potrebné poukázať na pretrvávajúce ťažkosti pri klasifikácii a identifikácii jednotlivých typov modelov umelej inteligencie. Umeľá inteligencia ako technologický fenomén totiž nie je homogénna. Práve naopak, predstavuje široké spektrum modelov a prístupov, ktoré sa od seba navzájom líšia nielen mierou autonómie, ale aj možnou mierou porozumenia a čitateľnosti jej vnútorných procesov. Ako sme stručne predstavili v predchádzajúcej časti, nie každý model dokáže v rovnakej miere zabezpečiť splnenie podmienok stanovených v Akte o umelej inteligencii, najmä pokiaľ ide o transparentnosť, kontrolovateľnosť a interpretovateľnosť jej výstupov. Pre objektívne posúdenie vhodnosti použitia

¹³ KISELEVA, Anastasiya. 2021. Making AI's Transparency Transparent: Notes on the EU Proposal. In *European Law Blog*. [online]. [cit. 26-09-2025]. Dostupné online z: <<https://doi.org/10.21428/9885764c.0440aef5>>.

¹⁴ Podobne, k tomu pozri aj: WACHTER, Sandra. Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond. In *Yale Journal of Law and Technology*, vol. 26 (3), 2024, s. 691-692. [online]. [cit. 26-09-2025]. Dostupné online z: <<https://yolt.org/limitations-and-loopholes-eu-ai-act-and-ai-liability-directives-what-means-european-union-united>>.

umelej inteligencie vo verejnej správe je však nevyhnutné porozumieť ich rozdielom a kriticky vyhodnotiť ich potenciálne aplikačné dôsledky a vplyv na rozhodovacie procesy vo verejnej správe.

Jednou z najvýznamnejších otázok v tomto kontexte je pojem „interpretovateľnosti“ modelov umelej inteligencie, ktorý je v súčasnosti predmetom intenzívnej odbornej diskusie a rozličných výkladov. Čo konkrétne znamená, že je model interpretovateľný? Aké kritériá by mal spĺňať, aby bol jeho výstup považovaný za dostatočne čitateľný a zrozumiteľný pre jeho používateľov, adresátov a dohliadajúce orgány?

Práve v tejto súvislosti sa ukazuje ako dôležité rozlišovať medzi jednotlivými typmi modelov z hľadiska ich vnútornej štruktúry a schopnosti vysvetliť, akým interným procesom dospeli ku konkrétnemu výstupu. Modely strojového učenia možno v tomto ohľade rozdeliť na *black box* a *white box* modely¹⁵.

Pod pojmom *black box* sa spravidla rozumejú všetky modely umelej inteligencie, ktorých vnútorné rozhodovacie procesy sú pre človeka netransparentné alebo len veľmi ťažko spätne čitateľné. Medzi tieto modely patria spravidla, hoci nie výlučne, modely hlbokých neurónových sietí (*deep learning*), ktoré vykonávajú vysoko komplexné matematické operácie. V dôsledku toho nie je možné jednoznačne určiť, ktoré vstupné premenné viedli ku konkrétnemu výstupu. Napriek vysokej presnosti a flexibilitě pri spracovaní rozsiahleho množstva komplexných informácií, ako je napríklad prirodzený jazyk, zvukové záznamy či obrazový materiál, zostávajú ich vnútorné mechanizmy rozhodovania prevažne netransparentné.¹⁶ Uvedené však nemožno automaticky považovať za problematické. Na jednej strane nemusí byť nevyhnutné, aby dohliadajúca osoba, tzv. ľudský faktor, disponovala detailnou znalosťou všetkých interných operácií prebiehajúcich vo vnútri modelu umelej inteligencie, pokiaľ je schopná dostatočne dôveryhodne vyhodnotiť a interpretovať presnosť jeho výstupov.¹⁷ Na druhej strane, pri rozhodovaní vo verejnej správe nadobúda osobitný význam schopnosť príslušného orgánu verejnej správy presne vedieť identifikovať a odôvodniť, na základe akých podkladov bolo rozhodnutie vydané, prípadne akým spôsobom použil svoju diskrečnú právomoc v konaní.¹⁸ Uvedená požiadavka nadobúda o to väčšiu váhu v prípadoch, keď výstup umelej inteligencie vedie k nezákonnému rozhodnutiu. V týchto situáciách môže

¹⁵ V súčasnosti sa v umelej inteligencii využívajú aj *gray box* modely AI, ktoré predstavujú kombináciu oboch prístupov. Keďže ide v podstate o hybridné modely pozostávajúce z vyššie uvedených kategórií, nebudeme sa im v príspevku venovať samostatne.

¹⁶ LOYOLA-GONZÁLEZ, Octavio. Black Box vs. White Box: Understanding Their Advantages and Weaknesses from a Practical Point of View. In *IEEE Access*, vol. 7, 2019. s. 154096-154113. [online]. [cit. 26-09-2025]. <[10.1109/ACCESS.2019.2949286](https://doi.org/10.1109/ACCESS.2019.2949286)>.

¹⁷ Ibidem, s. 154101.

¹⁸ KOŠIČIAROVÁ, Soňa. *Správny poriadok. Komentár*. Šamorín: Heuréka, 2013, s. 225-227.

nedostatočná interpretovateľnosť interných procesov *black box* modelov umelej inteligencie zapríčiniť, že správny orgán nebude schopný dostatočne odôvodniť svoje rozhodnutie alebo spätne overiť, na základe akých vstupov bol konkrétny výstup generovaný.

V tomto ohľade nemožno opomenúť, že ani súčasná európska úprava transparentnosti a interpretovateľnosti modelov umelej inteligencie neposkytuje dostatočné záruky na detailné objasnenie interného fungovania jednotlivých modelov. V súčasnosti spravidla postačuje taká miera vysvetliteľnosti, ktorá explicitne nevyžaduje úplné odhalenie všetkých interných procesov AI¹⁹ a využívanie *black box* modelov je z tohto dôvodu prípustné aj v kontexte vysokorizikových rozhodovacích procesov v zmysle Aktu o umelej inteligencii.

Určitém korektívom pri používaní *black box* modelov AI sú vysvetliteľné metódy umelej inteligencie, tzv. *explainable AI (XAI)*²⁰, ktoré sa využívajú *post hoc* (aplikované sú až po tréňovaní modelu AI) a slúžia na interpretovanie výstupov *black box* modelov. Uvedené metódy (napríklad LIME a SHAP, ktoré aktuálne predstavujú dve najznámejšie XAI metódy)²¹ sú však v súčasnosti odborníkmi často považované za nepresné, nestabilné a v niektorých prípadoch aj ľahko manipulovateľné v závislosti od poskytnutých vstupných vzoriek. Slúžia teda len na aproximáciu výstupov *black box* modelov, pričom predmetný prístup nemožno považovať za dostatočný, a to najmä vo vysokorizikových rozhodovacích procesoch. Dôvodom je aj tá skutočnosť, že ani dodatočná spätná vysvetliteľnosť prostredníctvom XAI metód často nepostačuje na dosiahnutie požadovanej úrovne dôveryhodnosti výsledkov vygenerovaných *black box* umelou inteligenciou.²²

Na druhej strane, za vhodnejšie riešenie možno považovať *white box* modely umelej inteligencie, ako sú napríklad rozhodovacie stromy alebo lineárne regresné modely, ktoré sa vyznačujú vysokou mierou interpretovateľnosti a sú pre človeka ľahko pochopiteľné. Tieto modely AI umožňujú, aby bol nad použitím umelej inteligencie

¹⁹ WACHTER, Sandra – MITTELSTADT, Brent – RUSSELL, Chris. Counterfactual Explanations Without Opening The Black Box: Automated Decisions and GDPR. In *Harvard Journal of Law & Technology*, vol. 31 (2), 2018. s. 843. <<https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>>.

²⁰ Pojem „explainable AI“ sa často vzťahuje aj na *white box* modely umelej inteligencie, ktoré sú už samé o sebe priamo interpretovateľné.

²¹ SALIH, AM. – RAISI-ESTABRAGH, Z. – GALAZZO, IB. – RADEVA, P. – PETERSEN, SE. – LEKADIR, K. – MENEGAZ, G. A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. In *Advanced Intelligent Systems*, 2024. Dostupné online z: <<https://arxiv.org/abs/2305.02012>>.

²² ALI, Sajid – ABUDMED, Tamer – EL-SAPPAGH, Shaker – MUHAMMAD, Khan – ALONSO-MORAL, Jose M. – CONFALONIERI, Roberto – GUIDOTTI, Riccardo – DEL SER, Javier – DÍAZ-RODRÍGUEZ, Natalia – HERRERA, Francisco. Explainable Artificial Intelligence (XAI): What We Know and What is Left To Attain Trustworthy Artificial Intelligence. In *Information Fusion*, Vol. 99, 2023. Dostupné online z: <<https://doi.org/10.1016/j.inffus.2023.101805>>.

efektívny ľudský dohľad, vrátane možnosti spätnej identifikácie konkrétnej fázy interného rozhodovacieho procesu, počas ktorej došlo k chybnému vyhodnoteniu vstupov. Súčasne umožňujú kontrolu vstupných ukazovateľov vrátane ich vzájomných väzieb a interakcií, ktoré môžu zapríčiniť nesprávny výstup. Zároveň je však potrebné podotknúť, že *white box* modely umelej inteligencie preukazujú v štúdiách nižšiu mieru presnosti, pričom sú charakteristické menšou schopnosťou flexibility pri spracovávaní komplexných údajov.²³ Súčasne sa v ich súvislosti, a to najmä vo vzťahu k rozhodovacím stromom a lineárnym regresným modelom, poukazuje na možnosť nestability rozhodovania v závislosti od nevhodnej vstupnej vzorky pri poskytovaní tréningových dát, kde je vo výsledku poskytnutých viacero výstupov s podobnou predikčnou presnosťou, ale odlišnou štruktúrou. Tento nedostatok však môže byť zmiernený zapojením doménovej expertízy, ktorá umožňuje výber najvhodnejšej alternatívy vzhľadom na praktický kontext.²⁴

S ohľadom na požiadavky spätnej interpretovateľnosti a transparentnosti, ktoré kladie na vysokorizikové procesy Akt o umelej inteligencii, sa možno domnievať, že sa aj napriek určitým nedostatkom javí ako vhodnejšie riešenie pre použiteľnosť vo verejnej správe práve použitie *white box* modelov umelej inteligencie, ktoré umožňujú orgánom verejnej správy presne identifikovať príčiny vygenerovaných výstupov a efektívne overiť jednotlivé fázy interných rozhodovacích procesov.

Záver

Zavádzanie modelov umelej inteligencie do verejnej správy otvára nové možnosti na zvýšenie jej efektívnosti a zníženie administratívneho zaťaženia jej zamestnancov. Zároveň však predstavuje komplexnú výzvu, a to nielen právnu a etickú, ale súčasne aj technologickú, ktorej zvládnutie je nevyhnutným predpokladom pre dôveryhodné fungovanie verejnej správy.

Na prípade *SyRI* sme názorne poukázali na aplikačné následky nasadzovania netransparentných algoritmických systémov do verejnej správy, a to práve pri absencii možnosti spätnej kontroly interných rozhodovacích procesov. Práve v tejto súvislosti nadobúda osobitný význam požiadavka na zrozumiteľnosť a interpretovateľnosť autonómnych systémov, a to predovšetkým pri ich využití vo

²³ OLASEHINDE, Tolamise. 2024. *Comparing Black-Box and White-Box Models in AI-Based Cybersecurity*. [online]. [cit. 26-09-2025]. Dostupné online z: <https://www.researchgate.net/publication/387224780_Comparing_Black-Box_and_White-Box_Models_in_AI-Based_Cybersecurity>.

²⁴ RUDIN, Cynthia. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. In *Nature Machine Intelligence*, 2019. s. 206-215. Dostupné online z: <[10.1038/s42256-019-0048-x](https://doi.org/10.1038/s42256-019-0048-x)>.

vysokorizikových procesoch, ktoré môžu priamo ovplyvňovať práva a povinnosti jednotlivcov.²⁵

Právna regulácia Aktu o umelej inteligencii síce stanovuje rámcové požiadavky na transparentnosť a ľudský dohľad pri ich využívaní vo vysokorizikových oblastiach, no ponecháva pomerne široký priestor pre výber konkrétnych technologických riešení na členské štáty Európskej únie. Práve v tomto ohľade nadobúdajú osobitný význam modely umelej inteligencie, ktoré svojou štruktúrou priamo umožňujú ich spätnú vysvetliteľnosť. Napriek ich nižšej flexibilitate môžu pri vhodnom naprogramovaní predstavovať vo verejnej správe najpriaznivejší prístup k zachovaniu právnej istoty účastníkov konania a minimalizácie zodpovednosti štátu za škodu spôsobenú nezákonným rozhodnutím. Možno sa dôvodne domnievať, že práve tieto modely vhodne naplňajú nielen technologické, ale aj právne a etické požiadavky na interpretovateľnosť interných rozhodovacích procesov AI pri činnosti orgánov verejnej správy. Ich zavedenie preto predstavuje kľúčový krok smerom k dôveryhodnému, legitímnemu a efektívnemu využívaniu umelej inteligencie vo verejnej správe.

Zoznam použitej literatúry

1. ALI, Sajid – ABUDMED, Tamer – EL-SAPPAGH, Shaker – MUHAMMAD, Khan – ALONSO-MORAL, Jose M. – CONFALONIERI, Roberto – GUIDOTTI, Riccardo – DEL SER, Javier – DÍAZ-RODRÍGUEZ, Natalia – HERRERA, Francisco. Explainable Artificial Intelligence (XAI): What We Know and What is Left To Attain Trustworthy Artificial Intelligence. In *Information Fusion*, Vol. 99, 2023. Dostupné online z: <<https://doi.org/10.1016/j.inffus.2023.101805>>.
2. ALTY, J. L. – GUIDA, G. The Use of Rule-based System Technology for the Design of Man-Machine Systems. In *IFAC Proceedings Volumes*, vol. 18 (10), 1985, p. 21-41. Dostupné online z: <[https://doi.org/10.1016/S1474-6670\(17\)60196-4](https://doi.org/10.1016/S1474-6670(17)60196-4)>.
3. BABŠEK, Matej – RAVŠEJ, Dejan – UMEK, Lan – ARISTOVNIK, Aleksander. Artificial Intelligence Adoption in Public Administration: An Overview of Top-Cited Articles and Practical Applications. In *AI 2025*, vol. 6 (3), 44. Dostupné online z: <<https://doi.org/10.3390/ai6030044>>.
4. KISELEVA, Anastasiya. 2021. Making AI's Transparency Transparent: Notes on the EU Proposal. In *European Law Blog*. [online]. [cit. 26-09-2025]. Dostupné online z: <<https://doi.org/10.21428/9885764c.0440ae5f>>.
5. KOŠIČIAROVÁ, Soňa. *Správny poriadok. Komentár*. Šamorín: Heuréka, 2013, 357 s.

²⁵ POTÁSCH, Peter – HAŠANOVÁ, Janka – VALLOVÁ, Jana – MILUČKÝ, Jozef – MEDŽOVÁ, Daniela. *Správny poriadok. Komentár. Štvrté vydanie*. Praha: C. H. Beck, 2022, s. 417-425.

6. LOYOLA-GONZÁLEZ, Octavio. Black Box vs. White Box: Understanding Their Advantages and Weaknesses from a Practical Point of View. In *IEEE Access*, vol. 7, 2019. s. 154096-154113. [online]. [cit. 26-09-2025]. <[10.1109/ACCESS.2019.2949286](https://doi.org/10.1109/ACCESS.2019.2949286)>.
7. MESARČÍK, Matúš – GYURÁSZ, Zoltán a kolektív. *Právo a umelá inteligencia. Prvé vydanie*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, 244 s.
8. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizačné pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).
9. OLASEHINDE, Tolamise. 2024. *Comparing Black-Box and White-Box Models in AI-Based Cybersecurity*. [online]. [cit. 26-09-2025]. Dostupné online z: <https://www.researchgate.net/publication/387224780_Comparing_Black-Box_and_White-Box_Models_in_AI-Based_Cybersecurity>.
10. POTÁSCH, Peter – HAŠANOVÁ, Janka – VALLOVÁ, Jana – MILUČKÝ, Jozef – MEDŽOVÁ, Daniela. *Správny poriadok. Komentár. Štvrté vydanie*. Praha: C. H. Beck, 2022, 682 s.
11. RACHOVITSA, Adamantia – JOHANN, Niclas. The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case. In *Human Rights Law Review*, vol. 22 (2), 2022. s. 1-15. [online]. [cit. 25-09-2025]. Dostupné online z: <<https://doi.org/10.1093/hrlr/ngac010>>.
12. Rozhodnutie Rechtbank Den Haag z 5. februára 2020, sp. zn. C/09/550982/HA ZA 18-388 (ECLI:NL:RBDHA:2020:1878). Dostupné online z: <https://www.escri-net.org/wp-content/uploads/2020/09/ecli_nl_rbdha_2020_1878.pdf>.
13. RUDIN, Cynthia. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. In *Nature Machine Intelligence*, 2019. s. 206-215. Dostupné online z: <[10.1038/s42256-019-0048-x](https://doi.org/10.1038/s42256-019-0048-x)>.
14. SALIH, AM. – RAISI-ESTABRAGH, Z. – GALAZZO, IB. – RADEVA, P. – PETERSEN, SE. – LEKADIR, K. – MENEGAZ, G. A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. In *Advanced Intelligent Systems*, 2024. Dostupné online z: <<https://arxiv.org/abs/2305.02012>>.
15. WACHTER, Sandra. Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond. In *Yale Journal of Law and Technology*, vol. 26 (3), 2024. s. 671-718. [online]. [cit. 26-09-2025]. Dostupné online z: <<https://yjolt.org/limitations-and-loopholes-eu-ai-act-and-ai-liability-directives-what-means-european-union-united>>.

16. WACHTER, Sandra – MITTELSTADT, Brent – RUSSELL, Chris. Counterfactual Explanations Without Opening The Black Box: Automated Decisions and GDPR. In *Harvard Journal of Law & Technology*, vol. 31 (2), 2018. s. 842-887. Dostupné online z: <<https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>>.

Kontaktné údaje

Mgr. Stanislava Sopková

stanislava.sopkova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Katedra správneho a environmentálneho práva

SOUDNÍ TLUMOČENÍ A PŘEKLAD V ÉŘE AI: MEZI PRÁVEM NA SPRAVEDLIVÝ PROCES A TECHNOLOGICKÝMI MOŽNOSTMI

COURT INTERPRETING AND TRANSLATION IN THE AGE OF AI: BETWEEN THE RIGHT TO A FAIR TRIAL AND TECHNOLOGICAL POSSIBILITIES

Kamila Balounová¹

Abstrakt: Příspěvek se zabývá využíváním technologií umělé inteligence v oblasti soudního tlumočení a překladu. Cílem je analyzovat, do jaké míry může AI podporovat nebo nahrazovat lidské tlumočníky a překladatele v soudních a správních řízeních a jaké právní a etické otázky tento vývoj vyvolává. Text vychází z komparace přístupů ve vybraných jurisdikcích, zejména ve Spojených státech amerických, u Soudního dvora Evropské unie a v České republice. Použitá metodologie kombinuje deskriptivní a analytický přístup, zaměřuje se na právní rámec, institucionální praxi a pilotní projekty zavádění AI do překladatelských a tlumočnických služeb.

Hlavní zjištění ukazují, že ve sledovaných jurisdikcích převažuje hybridní model, v němž AI funguje jako podpůrný nástroj a lidský odborník zůstává odpovědný za konečný výstup. Příspěvek identifikuje klíčové podmínky pro bezpečné využití AI: jasné stanovení odpovědnosti, procesních záruk a kvality výstupů. Vědeckým přínosem je systematické shrnutí současných trendů a limitů této technologie, praktickým přínosem pak formulace doporučení pro legislativu a institucionální praxi v České republice.

Klíčové slová: soudní tlumočení a překlad, právo na spravedlivý proces, AI

Abstract: This article deals with the use of artificial intelligence technologies in the field of court interpreting and translation. The aim is to analyze the extent to which AI can support or replace human interpreters and translators in court and administrative proceedings and what legal and ethical issues this development raises. The text is based on a comparison of approaches in selected jurisdictions, particularly in the United States, the Court of Justice of the European Union, and the Czech Republic. The methodology used combines

¹ Katedra správního práva Právnické fakulty Univerzity Karlovy

a descriptive and analytical approach, focusing on the legal framework, institutional practice, and pilot projects for the introduction of AI into translation and interpreting services.

The main findings show that a hybrid model prevails in the jurisdictions studied, in which AI functions as a support tool and human experts remain responsible for the final output. The paper identifies key conditions for the safe use of AI: clear definition of responsibility, procedural safeguards, and output quality. The scientific contribution is a systematic summary of current trends and limitations of this technology, while the practical contribution is the formulation of recommendations for legislation and institutional practice in the Czech Republic.

Key words: Court interpreting and translation, right to a fair trial, AI

Úvod²

V posledních letech zaplňují odborné časopisy vědecké články věnované otázce využití umělé inteligence (AI) při soudním či správním rozhodování. Tento článek se však nezaměřuje na problematiku automatizovaného rozhodování, ale na jinou, v právním diskurzu často opomíjenou oblast, již se nástup éry AI rovněž významně dotýká – **soudní tlumočení a překlad**. S využitím tzv. robotických (strojových) tlumočnicků a překladatelů se již v některých zemích experimentuje, a tato technologie si postupně začíná nacházet cestu i do soudních síní a správních řízení. Zatímco tlumočení je ústní převod sdělení z jednoho jazyka do druhého probíhající v reálném čase (tedy tlumočení mluveného slova),³ překlad je, zjednodušeně řečeno, písemný převod sdělení z jednoho jazyka do druhého (tedy překlad psaného slova).⁴ Jak tlumočení, tak překlad slouží ke zprostředkování mezikulturní komunikace a překonávání jazykových bariér mezi lidmi, kteří nehovoří stejným jazykem. Článek se zaměřuje na současné přístupy k využívání AI v oblasti soudního tlumočení a překladu na půdě Soudního dvora Evropské unie (dále jen „Soudní dvůr“), v USA, a v České republice.

² Článek vznikl jako součást projektu SVV 260 749 - Globální změna světa a reakce veřejného práva na ni.

³ ČEŇKOVÁ, Ivana. *Úvod do teorie tlumočení*. Praha: Česká komora tlumočnicků znakového jazyka, 2008, s. 11.

⁴ KNITTLOVÁ, Dagmar a kol. *Překlad a překládání*. Olomouc: Univerzita Palackého v Olomouci, Filozofická fakulta, 2010, s. 221-225.

Právo na tlumočení

Právo na tlumočení je zakotveno v mnoha mezinárodních dokumentech (např. čl. 14 odst. 3 písm. f) Mezinárodního paktu o občanských a politických právech, čl. 5 odst. 2 a 6 odst. 3 písm. e) Úmluvy o ochraně lidských práv a základních svobod). V českém právním řádu je právo zakotveno v čl. 37 odst. 4 Listiny základních práv a svobod a jednotlivých procesních předpisech.

Právo na tlumočení je obvykle označováno jako součást práva na spravedlivý proces, jako tzv. podpůrné právo zásady rovnosti účastníků v řízení.⁵ Právo na tlumočnicka představuje garanci řádně vedeného řízení před orgány moci veřejné.⁶ Nezajištění práva na tlumočnicka, přestože o něj účastník řízení požádal, způsobuje podstatnou vadu řízení, neboť tak dochází k výraznému zkrácení práv.⁷ Porušením práva na tlumočnicka se nepřipustně zasahuje do lidské důstojnosti a dochází k porušení práva na spravedlivý proces.⁸

Specifika umělé inteligence

Diskuse o využívání AI ve veřejné správě a justici nevyhnutelně otevírá řadu zásadních otázek. Týkají se především ochrany osobních údajů a citlivých informací, odolnosti těchto systémů vůči kybernetickým útokům a problémů spojených s tzv. fenoménem černé skříňky⁹. S tím úzce souvisí i obavy z možného vzniku diskriminačních vzorců v rozhodování, etické otázky spojené se zapojením strojů do procesů, které mohou zásadně ovlivnit životy jednotlivců, a rovněž riziko nadměrného spoléhání se na technologická řešení na úkor lidského úsudku a odpovědnosti.

Samotné tlumočení a překlad pak pro umělou inteligenci představují specifickou výzvu. Nejde totiž o jednoduchý převod slov z jednoho jazyka do druhého, ale o komplexní proces vyžadující porozumění kontextu, kulturním odlišnostem i sociálním a komunikačním nuancím.¹⁰ Problémem u tlumočení je práce s různými jazykovými rejstříky, dvojsmysly, idiomy nebo zvládání rychlého tempa mluveného

⁵ STAVINHOVÁ, Jaruška. Zásada rovnosti účastníků. In: HENDRYCH, Dušan a kol. *Právnícký slovník*. 3. vyd. Praha: C. H. Beck, 2009.

⁶ Nález Ústavního soudu ze dne 12. března 2019, sp. zn. III. ÚS 3464/17.

⁷ Usnesení Nejvyššího soudu ze dne 12. července 2001, sp. zn. 6 To 550/2001.

⁸ Nález Ústavního soudu ze dne 7. července 2021, sp. zn. II. ÚS 482/21.

⁹ NEŠPOR, Jan. Automated Administrative Decision-Making: What Is the Black Box Hiding? *Acta Universitatis Carolinae – Iuridica*. Roč. 2 (2024), s. 69 a násl.

¹⁰ NAVEEN, Palanichamy a TROJOVSKÝ, Pavel. Overview and challenges of machine translation for contextually appropriate translations. *IScience*. 2024, vol. 27, iss. 10, s. 8–9.

projevu.¹¹ U překladu se systémy potýkají s nedostatečnou schopností pracovat s kontextem, odbornou terminologií, stylistikou nebo víceznačností.¹²

Soudní dvůr Evropské unie

Evropská unie klade velký důraz na mnohojazyčnost, která je jedním z jejích základních principů (čl. 22 Listiny základních práv Evropské unie, dále jen „LZP EU“). Jedním z klíčových aktérů v této oblasti je Soudní dvůr. Možnost každého účastníka řízení vyjadřovat se před unijními soudy ve své mateřštině je ztělesněním zásady nediskriminace uvedené v čl. 21 LZP EU a rovného přístupu všech občanů ke spravedlnosti uvedeného v čl. 47 LZP EU. Sám Soudní dvůr rozhoduje ve všech 24 úředních jazycích EU, a proto se intenzivně zabývá otázkou, zda by právě AI mohla přispět k rychlejšímu, nákladově efektivnějšímu a širšímu zpřístupnění práva a judikatury.

V roce 2023 přijal strategický dokument *Artificial Intelligence Strategy* (dále jen „strategie AI“), který stanovuje vizi, cíle a principy využívání AI v rámci soudní činnosti.

V rámci zvýšení efektivity a účinnosti administrativních a soudních procesů se jedná o AI integrovanou do systému SIGA (*Système Intégré de Gestion des Affaires*), informačního systému, který slouží k elektronické správě případů (spisů) a řízení procesních úkonů v rámci jednotlivých řízení před Soudním dvorem a Tribunálem, nebo pro vytváření automatických shrnutí.¹³ V rámci zlepšení kvality a konzistence soudních rozhodnutí se jedná například o využití AI při právních rešerších, a to rychlou analýzou velkého množství dat a identifikací relevantních případů v národních databázích.¹⁴ V rámci zvýšení přístupu ke spravedlnosti a transparentnosti se jedná například o chatboty nebo právní asistenty, kteří by umožnili snazší přístup k informacím poskytovaným Soudním dvorem.¹⁵

Další využití AI v právním překladu a tlumočení je v současné době předmětem výzkumu. Soudní dvůr do budoucna spoléhá zejména na překlad založený na

¹¹ XIAOMAN, Wang a FANTINUOLI, Claudio. Exploring the Correlation between Human and Machine Evaluation of Simultaneous Speech Translation. In: *Proceedings of the 25th Annual Conference of the European Association for Machine Translation (volume 1)*. Sheffield: European Association for Machine Translation, 2024, s. 329–330. Dále CAO, Ying. Comparative Analysis of Machine Interpreting and Human Interpreting: Insights into Consecutive Interpreting Teaching. *Advances in Social Science, Education and Humanities Research*. Roč. 914, č. 851 (2024) [Proceedings of the 2024 3rd International Conference on Social Sciences and Humanities and Arts (SSHA 2024)], s. 730–741.

¹² Komora soudních tlumočnicků a soudních překladatelů ČR. AI – umělá inteligence v překladatelské praxi? *Soudní tlumočnick*. Č. 2 (2023), s. 8.

¹³ Court of Justice of the European Union. *Artificial Intelligence Strategy*. 2023, s. 10–11.

¹⁴ Tamtéž, s. 12–14.

¹⁵ Tamtéž, s. 14–16.

zpracování přirozeného jazyka (NLP), na takový vývoj, který umožní kontextový překlad, který bude brát v úvahu okolní kontext a vytvářet přesné a kulturně vhodné překlady, na zařízení pro převod řeči na text (*speech-to-text-machine*), který automaticky přepisuje mluvené slovo na psaný text,¹⁶ a na multimodální překlad, který nabídne možnost překladu téměř v reálném čase mezi různými typy médií (text, video, obraz, zvuk).¹⁷

Souhrnně je možné říci, že si je Soudní dvůr vědom potenciálu, který umělá inteligence v této oblasti nabízí, zejména pokud jde o zvýšení efektivity, snížení jazykových bariér a optimalizaci nákladů na překladatelské a tlumočnické služby. Současně však přistupuje k využívání těchto technologií s vědomím jejich dosavadních limitů a klade důraz na odpovědné, spravedlivé a transparentní využívání AI.¹⁸ Role AI je vnímána jako podpůrná – jako „asistivní technologie“, která může překladatelům a tlumočnickům pomoci urychlit a usnadnit jejich práci. Důraz je kladen na zásadu „*under user control*“, tedy na nutnost, aby byl každý výstup využíván pod dohledem profesionála, který nese odpovědnost za jeho správnost a vhodnost.¹⁹

Spojené státy americké

Spojené státy americké patří mezi země, které aktivně experimentují s využitím umělé inteligence v oblasti soudního tlumočení a překladu. Hlavním impulsem k těmto snahám je narůstající nedostatek kvalifikovaných soudních tlumočnicků, který zásadně ovlivňuje chod jak státních, tak federálních soudů²⁰ a přitom „[t]he use of competent federal court interpreters in proceedings involving speakers of languages other than English is critical to ensure that justice is carried out fairly for defendants and other stakeholders.“²¹

Jedním z amerických států, které chtějí integrovat robotické tlumočníky a překladatele do soudního řízení, je Wisconsin. V květnu 2025 předložil poslanec Dave

¹⁶ Speech-to-text-machine může sloužit např. k přepisu ústních jednání.

¹⁷ Court of Justice of the European Union. *Artificial Intelligence Strategy*. 2023, s. 15.

¹⁸ HEYINK, Mark. *CJEU AI Strategy sets out courts artificial intelligence strategie*. Online, 2024. [cit. 28. 7. 2025]. Dostupné z: <https://www.michalsons.com/blog/cjeu-ai-strategy/70805>.

¹⁹ WRIGHT, Susan. Artificial Intelligence in Legal Translation at the Court of Justice of the European Union. *International Journal of Language & Law*. Roč. 24 (2025), s. 139.

²⁰ WEISS, Debra Cassens. *Court Interpreter Shortages Worsen, Especially for Rare Languages*. Online, 2008. [cit. 28. 7. 2025]. Dostupné z: https://www.abajournal.com/news/article/court_interpreter_shortages_worsen_especially_for_rare_languages/#:~:text=Courts%20are%20facing%20a%20shortage%20of%20qualified%20interpreters,don%E2%80%99t%20have%20the%20proper%20training%2C%20USA%20Today%20reports

²¹ United States Courts. *Federal Court Interpreters*. Online, 2025. [cit. 28. 7. 2025]. Dostupné z: <https://www.uscourts.gov/court-programs/federal-court-interpreters>.

Maxey (Republikánská strana, New Berlin) návrh zákona Assembly Bill 292, který umožňuje využití AI a jiných forem strojového překladu v soudních řízeních.²²

Návrh zákona stanoví, že soudy mohou povolit použití AI nebo strojového překladu pro tlumočení a překlad v rámci soudních procesů, pokud to soud uzná za vhodné. V zákoně nejsou stanoveny konkrétní technické nebo kvalitativní požadavky na AI systémy, standardy ani pravidla pro použití AI v soudních síních, a to navzdory tomu, že jde o oblast s velmi složitou terminologií a potenciálně zásadními dopady na práva účastníků řízení.²³

Návrh zákona vyvolal výrazné reakce, především kvůli obavám o zachování kvality a spravedlnosti soudního řízení. Kritici upozorňují na nutnost doplnit legislativu o povinnost ověřovat přesnost překladů a tlumočení provedených umělou inteligencí a zajistit trvalý lidský dohled, zejména v klíčových typech řízení. Objevily se rovněž návrhy, aby bylo využití AI omezeno pouze na méně závažné případy nebo administrativní účely, nikoli však na samotná soudní jednání. Zároveň se diskutuje o zavedení pilotních projektů, jejichž výsledky by byly pravidelně vyhodnocovány z hlediska kvality a spolehlivosti AI tlumočení a překladu.²⁴

Dalším americkým státem, který experimentuje s využitím umělé inteligence v oblasti tlumočení a překladu, je Ohio. Nejvyšší soud státu Ohio (*Ohio Supreme Court*) přistoupil k přijetí nových pravidel, jejichž cílem je zvýšit dostupnost a flexibilitu tlumočnických služeb v reakci na nedostatek kvalifikovaných soudních tlumočnicků a překladatelů.

Navržené změny soudních pravidel umožňují využití generativní umělé inteligence (GenAI) k podpoře překladatelských a tlumočnických služeb v právním prostředí.²⁵ Tento rámec je však nastaven velmi restriktivně a fakticky se vztahuje pouze na překlady, nikoliv na samotné tlumočení. Umělá inteligence smí být využívána výhradně pro překlady neprávních textů, obecně informativních materiálů, jako jsou informace zveřejněné na webových stránkách soudu, nápisy a orientační tabule,

²² AB 292. Wisconsin Assembly Bill. Online, 2025. [cit. 28. 8. 2025]. Dostupné z: <https://fastdemocracy.com/bill-search/wi/2025-2026/bills/WI00014559/>.

²³ ALBARINO, Seyma. *Proposed Wisconsin Bill Could See Courts Introduce AI Interpreting and Translation*. Online, 2025. [cit. 28. 7. 2025]. Dostupné z: <https://slator.com/proposed-wisconsin-bill-could-see-courts-introduce-ai-interpreting-translation/>.

²⁴ BAWL, Andrew. *AI as a courtroom interpreter? Bill could make Wisconsin the first*. Online, 2025. [cit. 28. 6. 2025]. Dostupné z: https://captimes.com/news/government/ai-as-a-courtroom-interpreter-bill-could-make-wisconsin-the-first/article_a947a10a-e8ab-4c70-b054-e251cf6bbcde.html.

²⁵ ALBARINO, Seyma. *Proposed Wisconsin Bill Could See Courts Introduce AI Interpreting and Translation*. Online, 2025. [cit. 28. 7. 2025]. Dostupné z: <https://slator.com/proposed-wisconsin-bill-could-see-courts-introduce-ai-interpreting-translation/>.

úřední hodiny nebo údaje o umístění jednotlivých oddělení soudu. Použití AI musí být jasně označeno a uživatelé musí být upozorněni, že překlad může obsahovat chyby.²⁶ AI je zakázána pro překlad jakýchkoli právně závazných nebo podstatných dokumentů, jako jsou soudní rozhodnutí, podmínky podmíněčného propuštění a další dokumenty, které mohou ovlivnit výsledek řízení nebo základní práva účastníků. AI je dále výslovně zakázána pro tlumočení v rámci soudních jednání nebo jiných právních úkonů, kde by mohla být dotčena práva osob. To zahrnuje jak ústní tlumočení, tak například automatické titulkování během soudního řízení.²⁷

I Orange County v Kalifornii testuje využití umělé inteligence pro soudní překlad. Úřady v okrese Orange v Kalifornii začaly experimentovat s využitím nástroje umělé inteligence od společnosti Microsoft k překladu kratších soudních dokumentů do španělštiny a vietnamštiny, které následně nechaly zkontrolovat lidskými soudními překladateli. Úřady a soudy se nyní chystají začít využívat AI i pro překlady delších a složitějších soudních dokumentů. Rozšíření této technologie na tlumočení během soudních jednání však zatím není v plánu.²⁸

Česká republika

Ministerstvo vnitra v roce 2024 předložilo vládní návrh nového zákona o vstupu a pobytu cizinců na území České republiky, který má nahradit v současnosti platný zákon o pobytu cizinců (dále jen „návrh zákona o vstupu a pobytu cizinců“). Tento návrh, který prozatím neprošel legislativním procesem, obsahuje § 477, který měl umožnit tlumočení pomocí technického zařízení: „(1) K tlumočení úkonu v řízení může správní orgán použít namísto tlumočnicka zapsaného v seznamu soudních tlumočnicků a soudních překladatelů technické zařízení.“ Prozatím by se jednalo o jediný právní předpis (hmotněprávní i procesněprávní) v České republice, který by umožňoval strojové tlumočení nebo překlad.

Hlavními důvody pro zavedení možnosti tlumočení prostřednictvím technického zařízení je podle důvodové zprávy snaha zefektivnit a zrychlit správní proces, úspora nákladů, eliminace chyb při tlumočení a rozvoj a podpora digitalizace státní správy.

²⁶ FOX, Renee. *Ohio Supreme Court weighs proposed changes to interpreter services, could allow AI*. Online, 2025. [cit. 28. 6. 2025]. Dostupné z: <https://www.wosu.org/politics-government/2025-05-15/ohio-supreme-court-weighs-proposed-changes-to-interpreter-services-could-allow-ai>.

²⁷ Supreme Court of Ohio. *Court Responds to Growing Demand for Interpreters with Proposed Amendments to the Rules of Superintendence*. Columbus, OH: Supreme Court of Ohio. Online, 2024. [cit. 28. 6. 2025]. Dostupné z: <https://www.supremecourt.ohio.gov/docs/>.

²⁸ BAWL, Andrew. *AI as a courtroom interpreter? Bill could make Wisconsin the first*. Online, 2025. [cit. 28. 6. 2025]. Dostupné z: https://captimes.com/news/government/ai-as-a-courtroom-interpreter-bill-could-make-wisconsin-the-first/article_a947a10a-e8ab-4c70-b054-e251cf6bbcdc.html.

Návrh předpokládá technické zařízení umožňující automatické tlumočení, nezohledňuje však možnost technického zařízení pro automatický překlad. Ustanovení § 477 dává možnost správnímu orgánu využít technického zařízení namísto soudního tlumočníka, ovšem bez jasného vymezení podmínek, za nichž by k tomu mohlo dojít. Z textu není zřejmé, zda by bylo vyžadováno předchozí informované svolení účastníka řízení nebo obviněného v přestupkovém řízení. Text zákona nepředpokládá ani vydání prováděcího předpisu, který by upřesnil podmínky použití tohoto technického zařízení.

Předmětné ustanovení je koncipováno tak, že technické zařízení nelze považovat pouze jako podpůrný nástroj určený k základní asistenci při komunikaci (např. ve formě chatbotu), ale jako autonomní prostředek schopný generovat tlumočnické výstupy ve všech fázích řízení. Právní úprava nestanoví žádná omezení ohledně typu úkonů, pro něž lze zařízení využít. Nerozlišuje se tak mezi situacemi, kdy technologie slouží pouze k neformální komunikaci, a případy, kdy její výstupy mohou mít přímý dopad na obsah rozhodnutí ve věci.

Odstavec 2 sice stanoví požadavek, aby přesnost a rychlost tlumočení byly srovnatelné s výkonem soudního tlumočníka, zcela však chybí specifikace, kdo a jak má tuto srovnatelnost hodnotit. Ani u lidského tlumočníka přitom není zcela zřejmé, podle jakých objektivních kritérií by mělo být jeho tlumočení hodnoceno.

Záver

Technologie strojového tlumočení a překladu bezesporu představují významný krok směrem k digitalizaci veřejné správy a soudnictví. Do budoucna může robotický tlumočník či překladatel nabídnout efektivní alternativu k lidským soudním tlumočnickům a překladatelům, a to především z hlediska rychlosti, ekonomické efektivity a potenciální objektivnosti tlumočnických a překladatelských úkonů.

Z ekonomického pohledu lze očekávat výrazné snížení provozních nákladů. Současně by využití strojového tlumočení významně urychlilo soudní a správní procesy, neboť by odpadly časové prodlevy spojené s organizací přítomnosti soudního tlumočníka nebo zpracováním překladu.

Plné a bezpečné nasazení těchto technologií však podmiňuje vyřešení řady technických aspektů (zejména zajištění kvality a správnosti výstupů, ochranu před únikem dat, kybernetickou bezpečnost nebo zvládnutí výpadků systému během jednání) i otázek právních. Klíčové přitom bude zejména nastavení odpovědnosti za případné chyby ve výstupech, vytvoření účinných procesních mechanismů pro vypořádání námitek vůči nesprávnému tlumočení či překladu a zajištění plné ochrany práv účastníků na spravedlivý proces a tlumočení. Teprve po odstranění těchto překážek bude možné považovat implementaci strojového tlumočení a překladu do správního řízení za plně slučitelnou s principy právní jistoty a procesní spravedlnosti.

Zkušenosti ze Spojených států amerických a Soudního dvora ukazují, že nasazování technologií strojového tlumočení a překladu probíhá převážně v rámci pilotních projektů.

Současná praxe zároveň rozlišuje dva zásadně odlišné způsoby využití umělé inteligence. První z nich představuje využití AI jako nástroje pro zpracování běžných jazykových úkonů mimo soudní či správní řízení – například formou chatbotů, automatických překladů, sumarizací nebo přepisů. Tyto nástroje mohou do určité míry nahrazovat lidské překladatele a tlumočníky, avšak pouze v situacích, kde se nezasahuje do procesních práv osob.

Druhý způsob využití AI se týká soudních nebo správních řízení, v rámci kterých může být zasaženo do práv účastníků řízení, zejména na právo na obhajobu a na spravedlivý proces. Právě v těchto případech je přístup výrazně obezřetnější. Umělá inteligence zde neslouží jako náhrada lidského tlumočníka nebo překladatele, ale pouze jako podpůrný nástroj, jehož úkolem je zvýšit efektivitu, urychlit procesy a snížit administrativní zátěž. V oblasti překladu se jedná o tzv. CAT nástroje (*computer-assisted translation*)²⁹ a v oblasti tlumočení o počítačem podporované tlumočení (*computer-assisted interpreting*).³⁰

Zatímco přístup Spojených států a Evropské unie zůstává v této oblasti spíše zdrženlivý a orientovaný na pilotní ověřování a postupné zavádění hybridních řešení, český legislativní návrh – konkrétně návrh zákona o pobytu cizinců – jde zcela odlišnou cestou. Na rozdíl od mezinárodních trendů se zde strojové tlumočení zamýšlí jako přímá alternativa k soudnímu tlumočnickovi, a to i v procesních úkonech, které mohou mít zásadní dopad do práv účastníků.

V této souvislosti se nabízí legitimní otázka, zda hlavním motivem zavedení strojového tlumočení není primárně ekonomická úspora, a to na úkor kvality tlumočení a ochrany práv účastníků řízení. Zvláště znepokojující je také riziko diskriminace osob, které hovoří méně rozšířenými jazyky, pro něž neexistují dostatečně kvalitní jazykové modely. Je zjevné, že návrh zcela pomíjí základní roli soudního tlumočení jako procesní záruky, která slouží nejen k překonání jazykové bariéry, ale především k ochraně práv účastníků a k zajištění férovosti řízení.

²⁹ SVOBODA, Tomáš. *Kapitoly z překladatelské praxe: odborný překlad mezi němčinou a češtinou*. Praha: Univerzita Karlova, Filozofická fakulta, 2012, s. 80.

³⁰ GUO, Meng; HAN, Lili a ANACLETO, Marta Teixeira. Computer-Assisted Interpreting Tools: Status Quo and Future Trends. *Theory and Practice in Language Studies*. Roč. 13, č. 1 (2023), s. 89–90, dále srov. CHEN, Sijia a KRUGER, Jan-Louis. The effectiveness of computer-assisted interpreting: A preliminary study based on English-Chinese consecutive interpreting. *Translation and Interpreting Studies*. Roč. 18, č. 3 (2022), s. 399–420 nebo PRANDI, Bianca. *Computer-assisted simultaneous interpreting: A cognitive-experimental study on terminology*. Berlin: Language Science Press, 2023, s. 35–38.

Zoznam použitej literatúry

1. Mezinárodní pakt o občanských a politických právech.
2. Úmluva o ochraně lidských práv a základních svobod.
3. Listina základní práv a svobod.
4. Listina základních práv Evropské unie.
5. ČEŇKOVÁ, Ivana. *Úvod do teorie tlumočení*. Praha: Česká komora tlumočnicků znakového jazyka, 2008. S. 78. ISBN 978-80-87153-74-1.
6. KNITTLOVÁ, Dagmar a kol. *Překlad a překládání*. Olomouc: Univerzita Palackého v Olomouci, Filozofická fakulta, 2010. S. 293. ISBN 978-80-244-2428-6.
7. STAVINHOVÁ, Jaruška. Zásada rovnosti účastníků. In: HENDRYCH, Dušan a kol. *Právní slovník*. 3. vyd. Praha: C. H. Beck, 2009. S. 1488. ISBN 978-80-7400-059-1.
8. SVOBODA, Tomáš. *Kapitoly z překladatelské praxe: odborný překlad mezi němčinou a češtinou*. Praha: Univerzita Karlova, Filozofická fakulta, 2012. S. 201. ISBN 978-80-7308-407-3.
9. Nález Ústavního soudu ze dne 12. března 2019, sp. zn. III. ÚS 3464/17.
10. Usnesení Nejvyššího soudu ze dne 12. července 2001, sp. zn. 6 To 550/2001.
11. Nález Ústavního soudu ze dne 7. července 2021, sp. zn. II. ÚS 482/21.
12. CAO, Ying. Comparative Analysis of Machine Interpreting and Human Interpreting: Insights into Consecutive Interpreting Teaching. *Advances in Social Science, Education and Humanities Research*. Roč. 914, č. 851 (2024) [Proceedings of the 2024 3rd International Conference on Social Sciences and Humanities and Arts (SSHA 2024)], s. 730–741.
13. CHEN, Sijia a KRUGER, Jan-Louis. The effectiveness of computer-assisted interpreting: A preliminary study based on English-Chinese consecutive interpreting. *Translation and Interpreting Studies*. Roč. 18, č. 3 (2022), s. 399–420.
14. Court of Justice of the European Union. *Artificial Intelligence Strategy*. 2023, s. 25.
15. GUO, Meng; HAN, Lili a ANACLETO, Marta Teixeira. Computer-Assisted Interpreting Tools: Status Quo and Future Trends. *Theory and Practice in Language Studies*. Roč. 13, č. 1 (2023), s. 89–99.
16. Komora soudních tlumočnicků a soudních překladatelů ČR. AI – umělá inteligence v překladatelské praxi? *Soudní tlumočnick*. Č. 2 (2023), s. 8–12.
17. NAVEEN, Palanichamy a TROJOVSKÝ, Pavel. Overview and challenges of machine translation for contextually appropriate translations. *IScience*. 2024, vol. 27, iss. 10, s. 1–25.
18. NEŠPOR, Jan. Automated Administrative Decision-Making: What Is the Black Box Hiding? *Acta Universitatis Carolinae – Iuridica*. Roč. 2 (2024), s. 69–83.

19. PRANDI, Bianca. Computer-assisted simultaneous interpreting: A cognitive-experimental study on terminology. Berlin: *Language Science Press*, 2023, s. 35–38.
20. XIAOMAN, Wang a FANTINUOLI, Claudio. Exploring the Correlation between Human and Machine Evaluation of Simultaneous Speech Translation. In: *Proceedings of the 25th Annual Conference of the European Association for Machine Translation (volume 1)*. Sheffield: European Association for Machine Translation, 2024, s. 325–334.
21. WRIGHT, Susan. Artificial Intelligence in Legal Translation at the Court of Justice of the European Union. *International Journal of Language & Law*. Roč. 24 (2025), s. 120–142.
22. HEYINK, Mark. *CJEU AI Strategy sets out courts artificial intelligence strategie*. Online, 2024. [cit. 28. 7. 2025]. Dostupné z: <https://www.michalsons.com/blog/cjeu-ai-strategy/70805>.
23. United States Courts. *Federal Court Interpreters*. [cit. 28. 7. 2025]. Online, 2025. Dostupné z: <https://www.uscourts.gov/court-programs/federal-court-interpreters>.
24. AB 292. *Wisconsin Assembly Bill*. Online, 2025. [cit. 28. 7. 2025]. Dostupné z: <https://fastdemocracy.com/bill-search/wi/2025-2026/bills/WIB00014559/>.
25. ALBARINO, Seyma. *Proposed Wisconsin Bill Could See Courts Introduce AI Interpreting and Translation*. Online, 2025. [cit. 28. 8. 2025]. Dostupné z: <https://slator.com/proposed-wisconsin-bill-could-see-courts-introduce-ai-interpreting-translation/>.
26. BAWL, Andrew. *AI as a courtroom interpreter? Bill could make Wisconsin the first*. Online, 2025. [cit. 28. 6. 2025]. Dostupné z: https://captimes.com/news/government/ai-as-a-courtroom-interpreter-bill-could-make-wisconsin-the-first/article_a947a10a-e8ab-4c70-b054-e251cf6bbcdc.html.
27. FOX, Renee. *Ohio Supreme Court weighs proposed changes to interpreter services, could allow AI*. Online, 2025. [cit. 28. 6. 2025]. Dostupné z: <https://www.wosu.org/politics-government/2025-05-15/ohio-supreme-court-weighs-proposed-changes-to-interpreter-services-could-allow-ai>.
28. Supreme Court of Ohio. *Court Responds to Growing Demand for Interpreters with Proposed Amendments to the Rules of Superintendence*. Columbus, OH: Supreme Court of Ohio. Online, 2024. [cit. 28. 6. 2025]. Dostupné z: <https://www.supremecourt.ohio.gov/docs/>.

Kontaktné údaje

Mgr. et Mgr. Kamila Balounová, Ph.D.

balounka@prf.cuni.cz

Katedra správního práva a vědy Právníké fakulty Univerzity Karlovy

INFORMAČNÝ SYSTÉM A JEHO UPLATNENIE STAVEBNÝMI ÚRADMI¹

INFORMATION SYSTEM AND ITS APPLICATION BY BUILDING AUTHORITIES

Viera Jakušová²

Abstrakt: Príspevok sa zameriava na analýzu informačného systému a na jeho aplikačné aspekty z pohľadu stavebných úradov. Cieľom príspevku je identifikovať praktické problémy spojené so zavádzaním digitalizácie stavebnej agendy a poskytnúť návrhy de lege ferenda smerujúce k odstráneniu potenciálnej nejednotnosti postupov stavebných úradov a k naplneniu litery právnych predpisov. Autorka analyzuje štruktúru informačného systému, jeho verejnú a neverejnú časť, ako aj spracovávanie podaní stavebnými úradmi v informačnom systéme. Osobitná pozornosť je venovaná problematike identifikačného čísla stavby (ID stavby), ktoré je generované automaticky po zaregistrovaní „projektu“ v elektronickej forme do portálu výstavby. ID stavby absentuje pri listinných podaniach a informačný systém neposkytuje stavebným úradom funkcionalitu, ktorá by umožňovala generovanie ID stavby po jeho elektronickej konverzii. Táto skutočnosť môže viesť k nejednotnosti postupov stavebných úradov a k zníženiu právnej istoty účastníkov konania. Príspevok preto navrhuje legislatívne zmeny, ktorými by sa stavebným úradom uložila povinnosť generovať ID stavby pri listinných podaniach a zároveň by sa odstránila povinnosť jeho uvádzania v záväzných stanoviskách a vyjadreniach vydávaných vo fáze pred začatím konania o stavebnom zámere.

Kľúčové slová: nový stavebný zákon, informačný systém, portál výstavby, elektronické podanie, id stavby.

Abstract: The paper focuses on the analysis of the information system and its application aspects from the perspective of building authorities. The purpose of the paper is to identify practical problems associated with the implementation of the digitalisation of building administration and to provide

¹ Príspevok bol vypracovaný v rámci výskumnej úlohy „Energetická hospodárnosť budov v Slovenskej republike: zlepšenie organizačného a právneho rámca vo svetle nových požiadaviek Európskej únie“ s podporou grantu udeleného Agentúrou na podporu výskumu a vývoja pod registračným číslom projektu APVV-24-0543.

² Právnická fakulta Univerzity Komenského v Bratislave.

de lege ferenda proposals aimed at eliminating potential inconsistencies in the procedures of building authorities and ensuring compliance with the letter of the law. The author analyses the structure of the information system, its public and non-public sections, as well as the processing of submissions by building authorities within the system. Special attention is devoted to the issue of the building identification number (Building ID), which is automatically generated once a "project" is registered in electronic form on the Construction Portal. The Building ID is absent in paper-based submissions, and the information system does not provide building authorities with a function that would enable the generation of a Building ID after its electronic conversion. This situation may lead to inconsistencies in the building authorities' procedures and to a decrease in the legal certainty of the parties involved in the proceedings. Therefore, the paper proposes legislative amendments that would impose an obligation on building authorities to generate a Building ID for paper-based submissions and, at the same time, remove the obligation to indicate it in binding opinions and statements issued prior to the initiation of proceedings concerning a construction project.

Key words: new Building Act, information system, construction portal, electronic submission, building ID.

Úvod

Zákon č. 200/2022 Z. z. o územnom plánovaní v znení neskorších prepisov (ďalej len „ZoÚP“), ktorý zaviedol pojem informačný systém bol vyhlásený 07. júna 2022. Ustanovením § 41 bod 1. ZoÚP bol k 31. marcu 2025 zrušený zákon č. 50/1976 Zb. o územnom plánovaní a stavebnom poriadku (stavebný zákon) v znení účinnom do 31.03.2025 (ďalej len „pôvodný stavebný zákon“). Dňa 1. apríla 2025 nadobudol účinnosť zákon č. 25/2025 Z. z. Stavebný zákon a o zmene a doplnení niektorých zákonov (Stavebný zákon) v znení neskorších predpisov (ďalej len „NSZ“ alebo „nový stavebný zákon“), ktorý nahradil predchádzajúcu právnu úpravu, a tak i pôvodný stavebný zákon.

Je dôležité uviesť, že informačný systém sa rozvíja postupne, vo viacerých etapách. Tento fázovitý prístup umožňuje postupné zavádzanie nových funkcionalít a adaptáciu používateľov na digitálne prostredie. Možno povedať, že fázy predstavujú postupný a štruktúrovaný prechod od základnej digitálnej platformy k komplexnému a integrovanému Informačnému systému.³ Samotná realizácia informačného systému predstavuje značnú výzvu pre Slovenskú republiku, pretože náročnosť

³ Bližšie pozri: ÚRAD PRE ÚZEMNÉ PLÁNOVANIE A VÝSTAVBU SLOVENSKEJ REPUBLIKY. Plánované časové míľniky, [online] [cit. 05.09.2025] Dostupné na internete: <https://uupv.sk/>

spočíva nielen v technologickej a legislatívnej komplexnosti, ale aj v potrebe koordinácie širokého spektra subjektov – od orgánov štátnej správy, cez orgány samosprávy až po odbornú verejnosť a IT sektor. Prepojenie rôznych databáz, zabezpečenie kybernetickej bezpečnosti a používateľskej dostupnosti vyžaduje komplexný prístup a vysokú úroveň odborných znalostí. Okrem digitalizácie procesov v stavebnej agende prostredníctvom informačného systému stojí Slovenská republika pred ďalšou zásadnou výzvou – zabezpečením organizačného a právneho rámca pre energetickú certifikáciu budov. Táto povinnosť vyplýva zo smernice Európskeho parlamentu a Rady (EÚ) 2024/1275 z 24. apríla 2024 o energetickej hospodárnosti budov, ktorá kladie dôraz na udržateľnosť, znižovanie emisií a zvyšovanie energetickej efektívnosti v rámci Európskej únie.

Na účely príspevku sa zameriavame na informačný systém, pričom analyzujeme jeho použitie z perspektívy stavebných úradov. Pri analýze identifikujeme aj nedostatky, ktoré vznikajú v praxi. V nadväznosti na uvedené, poskytujeme návrhy *de lege ferenda*. Metódami analýzy a pozorovania dospejeme k ucelenému poznaniu skúmanej problematiky. Výsledkom je naplnenie stanoveného vedeckého cieľa, ktorým je vymedziť pojmy informačný systém a portál výstavby, opísať postup stavebných úradov pri používaní informačného systému, identifikovať nedostatky spojené s informačným systémom z pohľadu stavebných úradov a poskytnúť návrhy *de lege ferenda*.

Vymedzenie pojmov

Informačný systém bol zriadený ZoÚP ako nadrezortný informačný systém verejnej správy, určený na plnenie úloh územného plánovania, plnenie úloh vo výstavbe a plnenie iných úloh pri výkone verejnej moci, na ktorých plnenie je potrebné používať údaje evidované v informačnom systéme.⁴

Informačný systém obsahuje verejnú časť a neverejnú časť. **Verejná časť** informačného systému je dostupná prostredníctvom webového sídla úradu a obsahuje územnoplánovaciu dokumentáciu, informácie o území poskytnuté orgánmi územného plánovania na zverejnenie, rozhodnutia a záväzné stanoviská orgánov územného plánovania, vybrané údaje rozhodnutí a opatrení stavebných úradov a digitálny obraz Slovenskej republiky v rozsahu, v akom jeho verejné sprístupnenie nemožno využiť na ohrozenie činnosti informačného systému, alebo ohrozenie bezpečnosti alebo obrany Slovenskej republiky.⁵ **Neverejná časť** informačného systému obsahuje nástroje a funkcionality potrebné na vykonávanie a spracovanie činností územného plánovania podľa ZoÚP a na konanie o výstavbe a výkon štátneho stavebného dohľadu podľa NSZ oprávnenými osobami v rozsahu im udelených

⁴ Pozri § 25 ods. 1 ZoÚP.

⁵ Pozri § 25 ods. 2 ZoÚP.

oprávnení, a slúži na úradnú komunikáciu. K neverejnej časti informačného systému zriadi Úrad pre územné plánovanie a výstavbu Slovenskej republiky (ďalej len „Úrad“) oprávnenej osobe prístup umožňujúci automatizovaný spôsob komunikácie formou registrácie.⁶

Dňa 1. apríla 2025 nadobudla účinnosť vyhláška č. 60/2025 Z. z. Úradu pre územné plánovanie a výstavbu Slovenskej republiky o štruktúre a prevádzke informačného systému územného plánovania a výstavby, o obsahu podaní a obsahu a rozsahu dokumentácie stavby v znení neskorších predpisov (ďalej len „vyhláška č. 60/2025 Z. z.“), ktorá zavádza pojem portál výstavby. **Portál výstavby** je v nej definovaný ako **časť** informačného systému územného plánovania a výstavby, ktorý spravuje Úrad na úseku výstavby a štátneho stavebného dohľadu.⁷

Portál výstavby obsahuje úložisko dokumentácie, register výstavby, register stavieb, zoznam dotknutých orgánov, zoznam dotknutých právnických osôb, zoznam reprezentatívnych združení vlastníkov informačných zariadení.⁸ **Úložisko dokumentácie** je dátové úložisko určené na ukladanie dokumentácie stavby a jej dokladovej časti v elektronickej podobe.⁹ **Register výstavby** slúži na evidenciu všetkých stavieb a ich dokumentácie, ktorých podania sa uskutočnili ako elektronické podania alebo do elektronickej podoby konvertované listinné podania stavebným úradom, vo fáze povoľovacích procesov stavby až do uvedenia stavby do trvalého užívania alebo do vydania overovacej doložky ohlásenej stavby. Register výstavby obsahuje formuláre na príslušné podanie vrátane informácie o rozsahu a obsahu potrebnej dokumentácie stavby.¹⁰ Register stavieb obsahuje údaje o všetkých stavbách, ktoré sa od 1. apríla 2025 uviedli do trvalého užívania alebo im bola vydaná overovacia doložka ohlásenej stavby a ktorých podanie sa uskutočnilo ako elektronické podanie. Údaje o stavbách v registri stavieb nie sú verejne prístupné.¹¹

⁶ Týmito oprávnenými osobami sú

a) orgán územného plánovania, b) odborne spôsobilá osoba, c) spracovateľ, d) dotknutý orgán a dotknutá právnická osoba v rozsahu svojich oprávnení podľa tohto zákona v súvislosti s obstarávaním, spracovaním a prerokovaním územnoplánovacích podkladov a územnoplánovacej dokumentácie, e) dotknutá verejnosť v štádiu prerokovania územnoplánovacej dokumentácie podľa § 31 ZoÚP, f) osoby podľa NSZ v rozsahu svojich oprávnení v konaní vo výstavbe a pri výkone štátneho stavebného dohľadu podľa Stavebného zákona, iní špecialisti, potrební na vypracovanie projektovej dokumentácie a jej kompletizáciu a na vykonanie činností v predprojektovej príprave stavby, pri povoľovaní a zhotovovaní stavby a pri jej kolaudácii, g) osoba podľa § 25 ods. 6 ZoÚP, v rozsahu údajov z digitálneho obrazu Slovenskej republiky, h) osoba podľa osobitného predpisu, v rozsahu plnenia povinností poskytovať údaje do informačného systému, alebo inej časti údajovej základne informačného systému, alebo v rozsahu výkonu práva údaje z nich získavať. Pozri § 25 ods. 3 ZoÚP.

⁷ Pozri § 1 ods. 1 vyhlášky č. 60/2025 Z. z.

⁸ Pozri § 1 ods. 2 vyhlášky č. 60/2025 Z. z.

⁹ Pozri § 1 ods. 3 vyhlášky č. 60/2025 Z. z.

¹⁰ Pozri § 1 ods. 4 vyhlášky č. 60/2025 Z. z.

¹¹ Pozri § 1 ods. 5 vyhlášky č. 60/2025 Z. z.

Možno uviesť, že informačný systém je širší pojem než portál výstavby, pretože ho zahŕňa. Informačný systém má verejnú i neverejnú časť, pričom verejnú časť tvorí portál výstavby. Neverejnú časť informačného systému predstavuje tzv. „správcovský systém“, prostredníctvom ktorého sa prijímajú stavebnými úradmi podania, resp. žiadosti. Stavebné úrady tieto podania prostredníctvom systému spracovávajú, evidujú príslušné správne konania a vydávajú rozhodnutia.¹²

Informačný systém z pohľadu stavebných úradov

Nový stavebný zákon stanovuje povinnosť stavebným úradom zabezpečiť **bezodkladne konverziu** do elektronickej formy a uložiť dokumenty do informačného systému v prípade, ak by stavebník podal listinne ohlásenie stavby a stavebných úprav podľa § 63 NSZ alebo projekt stavby na ohlásenie a ďalšie prílohy.¹³ Táto konverzia a uloženie dokumentov stavebnými úradmi prebieha iba v neverejnej časti informačného systému. Vyhláška č. 60/2025 Z. z. definuje, čo možno rozumieť pod konverziou do elektronickej podoby. Je ním vytvorenie elektronickej kópie z celého pôvodného podania v listinnej podobe vrátane príloh a dokumentácie. Konverzia sa vykoná naskenovaním podania a jeho uložením do formátov PDF/A alebo PNG v takom rozlíšení, aby boli všetky potrebné informácie pre posúdenie podania s ohlášením pri zobrazení v zobrazovacom zariadení čitateľné a zrozumiteľné. Súbor získaný konverziou do elektronickej podoby je možné uložiť do informačného systému ako jeden súbor, bez potreby jeho delenia na jednotlivé výkresy a dokumenty.¹⁴

Pokiaľ ide o ostatné podania, stavebné úrady povinnosť konverzie a uloženie do informačného systému nemajú. Úrad zriaďuje oprávnenej osobe prístup umožňujúci automatizovaný spôsob komunikácie formou registrácie.¹⁵ Z praxe možno uviesť, že oprávnenou osobou na stavebných úradoch je starosta obce, ktorý v prípade existencie osoby vedúceho stavebného úradu mu udelí príslušné oprávnenia. Vedúci stavebného úradu ďalej udeľuje oprávnenia v rámci informačného systému odborným referentom. V priebehu apríla 2025 bolo na každý stavebný úrad doručené prostredníctvom elektronickej schránky meno a heslo do informačného systému.¹⁶ Stavebné úrady už mali vytvorené účty a profily v informačnom systéme

¹² Webinár - Blok č. 3 - Stavebné úrady, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.youtube.com/watch?v=Y5PpiehcZw8>

¹³ Pozri § 63 ods. 3 NSZ.

¹⁴ Pozri § 2 ods. 6 vyhlášky č. 60/2025 Z. z.

¹⁵ Pozri § 25 ods. 3 písm. f) a g) ZoÚP.

¹⁶ Webinár - Blok č. 3 - Stavebné úrady, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.youtube.com/watch?v=Y5PpiehcZw8>

a disponovali aj prístupovými údajmi.¹⁷ Prostredníctvom informačného systému sa evidujú, schvaľujú výstupy, podpisujú dokumenty osobami v rozsahu ich udelených oprávnení. Informačný systém automaticky odosiela podania do elektronickej schránky stavebným úradom. V prípade ak majú stavebné úrady registratúrny systém integrovaný so schránkou na Ústrednom portáli verejnej správy¹⁸, tak sa notifikácie zobrazujú priamo v registratúrach, ktoré stavebné úrady používajú.¹⁹

Je na úvahe stavebných úradov, či budú používať informačný systém i na spracovanie listinných žiadostí. V tom prípade, stavebný úrad zaeviduje podanie vyplnením formuláru a nahrá súbory (listiny) do informačného systému. Vo formulári stavebný úrad vyplní i číslo spisovej značky, pod ktorou je vedený spis v registratúre stavebného úradu.

Po zaevidovaní podania informačný systém ponúka možnosti

- a) výzva na spresnenie žiadosti
- b) zamietnuť žiadosť
- c) pridať konanie.

Ak stavebný úrad zvolí možnosť výzva alebo zamietnuť žiadosť, tak informačný systém vygeneruje automatizované podanie, ktoré je možné upravovať a následne cez systém doručiť do elektronickej schránky žiadateľa ako aj do portálu výstavby. Ak má žiadosť všetky náležitosti, tak stavebný úrad zvolí možnosť „pridať konanie“, pri ktorom je potrebné doplniť aj spisovú značku spisu vedeného v registratúre. Stavebný úrad má možnosť cez systém vytvoriť oznámenie o začatí konania aj ho odoslať. Nahratím podania do informačného systému sa doň automaticky uložia potrebné údaje, napr. subjekty konania, ktoré sa zobrazujú v poliach formulárov, ktoré stavebný úrad vyplní. Stavebný úrad môže takéto pole aj doplniť o ďalšie subjekty konania. Informačný systém obsahuje aj možnosť prerušiť konanie, obnoviť prerušené konanie a „pridať rozhodnutie“. ²⁰ Pre doplnenie možno uviesť, že predtým než je dokument odoslaný do portálu výstavby a žiadateľovi, resp. podávateľovi, tak je potrebné, aby ho odborný referent stavebného úradu odoslal najprv schvaľovateľovi (vedúci stavebného úradu, starosta). Schvaľovateľ dostane automaticky e-mail, že bol požiadaný o schválenie dokumentu. Ak je dokument

¹⁷ Portál výstavby. Stavebné úrady, [online] [cit. 28.08.2025] Dostupné na internete: <https://vystavba.uupv.sk/stranka/stavebne-urady>

¹⁸ Ústredný portál verejnej správy zabezpečuje centrálny a jednotný prístup k informačným zdrojom a službám verejnej správy. Informácie (rady, návody, popisy), ktoré návštevník hľadá, sú v súčasnosti mnohokrát súčasťou informačných serverov jednotlivých rezortov. Cieľom portálu je tieto informácie a služby zintegrovat' a prehľadnou a prístupnou formou poskytovať používateľovi. Pozri SLOVENSKO.SK – ÚSTREDNÝ PORTÁL VEREJNEJ SPRÁVY. O portáli, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.slovensko.sk/sk/o-portali>

¹⁹ Webinár - Blok č. 3 - Stavebné úrady, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.youtube.com/watch?v=Y5PpiehcZw8>

²⁰ Tamtiež.

schválený, tak ho odborný referent odošle na elektronický podpis oprávnenej osobe (vedúci stavebného úradu, starosta). Ak bol dokument aj elektronicky podpísaný, tak ho referent elektronicky odošle adresátovi. Ak adresát nemá elektronickú schránku, tak sa dokument posielá v listinnej forme.²¹

Forma podania

Podanie chápe daná vyhláška ako podanie žiadosti, oznámenia, ohlásenia, odvolania alebo podnetu príslušnému stavebnému úradu, dotknutému orgánu, dotknutej právnickej osobe alebo úradu, ktorého súčasťou je

- a) vyplnený formulár určený pre príslušné podanie,
- b) dokumentácia stavby,
- c) ostatné požadované prílohy a dokumenty,
- d) doklad o úhrade správneho poplatku, ak je úkon spoplatnený.²²

Podanie môže byť uskutočnené v listinnej alebo elektronickej podobe fyzickou alebo právnickou osobou. Elektronické podanie je podanie, ktorého všetky súčasti sú v elektronickej podobe a je uskutočnené elektronicky prostredníctvom informačného systému.²³ Veľkosť elektronického podania vrátane príloh je maximálne 100 MB. Do maximálnej veľkosti podania sa nezapočítava veľkosť elektronickej dokumentácie stavby v úložisku dokumentácie.²⁴ Listinné podanie je podanie, ktorého akákoľvek súčasť je priložená alebo neskôr doplnená v listinnej podobe alebo je uskutočnené inak ako elektronické podanie.²⁵

Podľa § 84 ods. 15 nového stavebného zákona môže právnická osoba vykonať akýkoľvek **procesný úkon** aj v listinnej podobe **do 31. marca 2029**. Fyzická osoba môže vykonať akýkoľvek procesný úkon podľa NSZ aj v listinnej podobe aj po tomto dátume. Z NSZ nevyplýva povinnosť stavebníka podávať podanie v elektronickej podobe, je to len možnosť, ktorú môže stavebník využiť.²⁶

Ak by stavebník podával akúkoľvek inú žiadosť v listinnej podobe (napr. žiadosť o vydanie rozhodnutia o stavebnom zámere, žiadosť o kolaudáciu stavby a pod.), tak správny orgán nie je povinný ju konvertovať do elektronickej podoby. V nových stavebných predpisoch tiež absentuje povinnosť dotknutého orgánu a dotknutej právnickej osoby zasielať záväzné stanoviská a záväzné vyjadrenia elektronicky.²⁷

²¹ Tamtiež.

²² Pozri § 2 ods. 1 vyhlášky č. 60/2025 Z. z.

²³ Pozri § 2 ods. 2 vyhlášky č. 60/2025 Z. z.

²⁴ Pozri § 2 ods. 3 vyhlášky č. 60/2025 Z. z.

²⁵ Pozri § 2 ods. 4 vyhlášky č. 60/2025 Z. z.

²⁶ JAKUŠOVÁ, V., Pohľad na ID stavby z hľadiska elektronickej a listinnej formy podania. In: *Expert pre stavebné úrady*. 2/2025. Bratislava : Verlag dashöfer, s. r. o., s. 8.

²⁷ Tamtiež, s. 8.

Možno tiež uviesť, že ak je podanie s ohlásením uskutočnené v listinnej podobe, jeho prílohy vrátane projektu stavby na ohlásenie, je možné doplniť ako listinné prílohy vo formáte A4 alebo A3 pre projekt stavby na ohlásenie a vo formáte A4 pre iné prílohy.²⁸

ID stavby

Jedným z údajov vo formulároch²⁹, dokumentácii stavby, rozhodnutiach, vyjadreniach a stanoviskách je aj identifikačné číslo stavby, ktoré je pridelené informačným systémom (ďalej len „ID stavby“). Možno uviesť, že ID stavby je obsiahnuté v rôznych podaniach, dokumentoch, dokladoch, napríklad v overovacej doložke ohlásenej stavby³⁰, v rozhodnutí o stavebnom zámere³¹, v overovacej doložke projektu stavby³², v rozhodnutí o skúšobnej prevádzke podľa § 19 písm. c) vyhlášky č. 60/2025 Z. z., v kolaudačnom osvedčení.³³ ID stavby je obsiahnuté aj v záväznom stanovisku dotknutého orgánu³⁴, dotknutej právnickej osoby a orgánu územného plánovania. Obsiahnuté je aj v doložke súladu a doložke súladu dotknutého orgánu, ktorým je orgán územného plánovania.³⁵

V súvislosti s uvedeným je na mieste otázka, ako stavebník, prípadne projektant konkrétne získa ID stavby? ID stavby sa pridružuje **projektu**³⁶ po jeho zaregistrovaní v elektronickej forme do portálu výstavby. Ide o šesť miestny kód, ktorý sa skladá z prvých dvoch číslíc roka, v ktorom bol projekt zaregistrovaný do informačného systému a z následných alfanumerických znakov, ktoré sú náhodné.³⁷ Čo však v prípade, že sa stavebník/projektant rozhodne podať príslušné žiadosti a projektovú dokumentáciu v listinnej forme? Ak by stavebník/projektant podávali **projekt na**

²⁸ Pozri § 2 ods. 5 NSZ.

²⁹ Vzorové formuláre sú prílohami vyhlášky č. 60/2025 Z. z.

³⁰ Pozri § 13 písm. d) vyhlášky č. 60/2025 Z. z.

³¹ Pozri § 14 písm. d) vyhlášky č. 60/2025 Z. z.

³² Pozri § 16 písm. d) vyhlášky č. 60/2025 Z. z.

³³ Pozri § 21 písm. c) vyhlášky č. 60/2025 Z. z.

³⁴ § 8 písm. c), § 9 a § 10 vyhlášky č. 60/2025 Z. z.

³⁵ Pozri § 11 a 12 vyhlášky č. 60/2025 Z. z.

³⁶ Projektom sa v tomto zmysle nerozumie projektová dokumentácia. Po prihlásení sa do informačného systému sa stavebníkovi/projektantovi zobrazuje formulár „vytvorenie nového projektu“, ktorý umožňuje vytvoriť nový projekt, následne pridávať údaje o stavbe, projektovú dokumentáciu k stavbe i vytvárať podania pre schvaľujúce procesy. Po doplnení a uložení údajov, ktorými sú názov projektu, klasifikácia stavby, popis stavby (nepovinné) a uvedenie údaje, či sa jedná o súbor stavieb je projekt vytvorený a automaticky sa mu prideli ID stavby.

³⁷ ÚRAD PRE ÚZEMNÉ PLÁNOVANIE A VÝSTAVBU SLOVENSKEJ REPUBLIKY. Webinár, Blok č. 1 – stavebník, projektant. [online], [cit. 21.05.2025]. Dostupné na internete: <https://uupv.sk/aktuality/druhy-webinar-zamerany-na-predstavenie-jednotlivych-funkcionalit-portalu-vystavby>

ohlásenie v listinnej forme, tak stavebný úrad má povinnosť jeho konverzie do elektronickej podoby.³⁸ Z praxe možno uviesť, že hoci stavebný úrad konvertuje listinné podanie s prílohami do elektronickej formy, tak sa automaticky neprideli podaniu informačným systémom ID stavby. Informačný systém prideli iba číslo žiadosti.

V prípade, ak by stavebník/projektant podávali projektovú dokumentáciu v stupni **stavebný zámer alebo projekt stavby** listinne, tak stavebný úrad nemá stanovenú povinnosť konverzie projektovej dokumentácie do elektronickej podoby.

ID stavby je základnou náležitosťou, ktorá sa má uvádzať vo formulároch, dokumentácii stavby, rozhodnutiach, vyjadreniach a stanoviskách.³⁹ Z praktickej roviny možno uviesť, že ak by stavebný úrad využil možnosť evidencie listinného podania v informačnom systéme, tak pri vyplňaní formulára by narazil na pole „ID stavby“, ktoré by mal stavebný úrad vyplniť. Nedostatkom je, že stavebný úrad nedisponuje týmto údajom a nevie ho ani sám vygenerovať.

Podľa nášho názoru, existuje predpoklad, že stavebné úrady budú vyžadovať doplnenie žiadosti o ID stavby, nakoľko je žiadosť neúplná a bez tohto údaju nemôžu (nemali by) ďalej konať. To však stavebník získa len, ak nahrá projektovú dokumentáciu do systému. V tejto súvislosti je dôležité uviesť znenie § 84 ods. 15 NSZ: „Osoba môže vykonať akýkoľvek **procesný úkon** podľa tohto zákona aj v listinnej podobe do 31. marca 2029; fyzická osoba môže vykonať akýkoľvek **procesný úkon** podľa tohto zákona aj v listinnej podobe aj po tomto dátume.“ Ak sa pozrieme na doslovné znenie ustanovenia, môžeme vnímať skutočnosť, že zákonodarca hovorí o procesnom úkone. Čo môžeme za takýto procesný úkon považovať? Je procesným úkonom **iba** podanie (napríklad žiadosť o vydanie rozhodnutia o stavebnom zámere)? Je procesným úkonom podanie v podobe žiadosti a **aj** v podobe projektovej dokumentácie? Uvedené môže byť problémom v praxi z hľadiska nejednotnej interpretácie, výkladu ustanovenia § 84 ods. 15 NSZ, ktorá môže viesť k „núteniu“ stavebníkov/projektantov podať si dokumenty elektronicke alebo listinne alebo k vydávaniu rozhodnutí bez obligatórnej náležitosti, ktorú stanovuje vyhláška č. 60/2025 Z. z.⁴⁰ Podľa § 2 ods. 1 písm. b) vyhlášky č. 60/2025 Z. z. je (projektová) dokumentácia súčasťou podania. Z hľadiska teleologického výkladu považujeme aj podanie projektovej dokumentácie za procesný úkon. Podľa nášho názoru, by nebolo účelné, aby stavebník/projektant podal podanie (žiadosť) elektronicke a jeho prílohu listinne. Sme toho názoru, že podania a ich súčasti (prílohy) možno vnímať ako procesné úkony účastníka konania. Za aplikácie uvedeného výkladu, možno povedať,

³⁸ Pozri § 63 ods. 3 NSZ.

³⁹ JAKUŠOVÁ, V., Pohľad na ID stavby z hľadiska elektronickej a listinnej formy podania. In: *Expert pre stavebné úrady*. 2/2025. Bratislava : Verlag dashöfer, s. r. o., s. 8.

⁴⁰ Tamtiež, s. 9.

že právnické osoby môžu odosielať podanie s dokumentáciou v zmysle § 84 ods. 15 nového stavebného zákona listinne len do 31. marca 2029. Po tomto dátume sa na vykonanie procesných úkonov vzťahuje výlučne elektronická podoba.

Riešením problému absentujúceho ID stavby pri listinných podaniach, by mohlo byť podľa nášho názoru, zakotvenie ustanovenia do nového stavebného zákona, ktorým by sa určila povinnosť stavebným úradom vygenerovať ID stavby podaniam, ktoré by mu boli doručené v listinnej podobe. Po **zaevidovaní** listinného podania a príloh do informačného systému stavebným úradom, by bolo vygenerované ID stavby, ktoré by už stavebný úrad uvádzal v listinách, ktoré súvisia s konaním. Stavebný úrad by nemal povinnosť pri listinných podaniach vytvoriť ich elektronickú kópiu vrátane príloh. Stavebný úrad by len zaevidoval v systéme listinné podanie ako aj prílohy a ich zaevidovaním by sa vygenerovalo ID stavby.

Nakoľko by bolo ID stavby vygenerované manuálnym zaevidovaním listinného podania do informačného systému, tak by bolo vhodné, aby sa cez portál výstavby zobrazovalo aj ostatným subjektom v konaní (účastníkom konania, dotknutým právnickým osobám, dotknutým orgánom). Navrhujeme preto, aby pri evidencii listinného podania do informačného systému, stavebný úrad vyplnil aj polia subjekty konania o príslušné osoby.

V nadväznosti na uvedené, navrhujeme zakotviť tieto ustanovenia do stavebných predpisov:

- A. *„Ak je podanie v listinnej podobe, správny orgán ho bezodkladne zaeviduje do informačného systému na účely pridelenia id stavby; konverzia ohlásenia, projektu stavby na ohlásenie a ďalších príloh, ktoré sú v listinnej podobe do elektronickej formy a ich uloženie do informačného systému ostáva zachované.“*
- B. *„Zaevidovaním listinného podania v informačnom systéme sa rozumie vloženie údajov o stavbe, o druhoch a počte jeho príloh do informačného systému.“*

Na tomto mieste je potrebné povedať, že záväzné stanoviská dotknutého orgánu a dotknutej právnickej osoby získava, napr. v konaní o stavebnom zámere stavebník/projektant pred samotným podaním žiadosti na stavebný úrad. Vo formulári „Žiadosť o vydanie záväzného stanoviska dotknutého orgánu podľa § 21 Stavebného zákona alebo záväzného vyjadrenia dotknutej právnickej osoby podľa § 22 Stavebného zákona“⁴¹ je uvedené vedľa poľa ID stavby: „ID stavby alebo súboru stavieb, ak bolo pridelené informačným systémom.“ Z uvedeného vyplýva, že stavebník/projektant toto pole vyplní, len v prípade, ak bolo ID stavby už pridelené. Nie je tu povinnosť uviesť ID stavby v žiadosti. Naproti tomu, podľa vyhlášky č. 60/2025 Z. z. záväzné stanovisko dotknutého orgánu, dotknutého orgánu, ktorým je orgán územného plánovania a záväzné vyjadrenie dotknutej právnickej osoby obsahuje okrem všeobecných náležitostí aj základné údaje o stavbe v rozsahu **ID**

⁴¹ Príloha č. 1 vyhlášky č. 60/2025 Z.z.

stavby, názov stavby, identifikačné údaje stavby, členenie stavby.⁴² Podľa danej vyhlášky ide o obligatórnu náležitosť. Tú však *de lege lata* nemožno získať inak ako cez informačný systém.⁴³ *De lege ferenda* sme navrhli generovanie ID stavby cez evidovanie doručeného listinného podania s prílohami stavebným úradom. Záväzná stanoviská a vyjadrenia sa však vydávajú vo fáze, ktorá predchádza konaniu o stavebnom zámere.⁴⁴ *De lege ferenda* by sme zároveň navrhli vypustiť ID stavby ako obligatórnu náležitosť v záväznom stanovisku a záväznom vyjadrení osoby. Tento návrh by odstránil potenciálne rozpory v postupoch príslušných subjektov.

Záver

V príspevku sme vymedzili pojmy informačný systém a portál výstavby, analyzovali postup stavebných úradov pri používaní informačného systému. Hlavným nedostatkom týkajúcim sa informačného systému je absencia ID stavby, ktoré sa vygeneruje informačným systémom po zaregistrovaní projektu. Projektom sa v tomto zmysle nerozumie projektová dokumentácia. Po prihlásení sa do informačného systému sa stavebníkovi/projektantovi zobrazuje formulár „vytvorenie nového projektu“, ktorý umožňuje vytvoriť nový projekt, následne pridávať údaje o stavbe, projektovú dokumentáciu k stavbe i vytvárať podania pre schvaľujúce procesy. Po doplnení a uložení údajov, ktorými sú názov projektu, klasifikácia stavby, popis stavby (nepovinné) a uvedenie údaje, či sa jedná o súbor stavieb je projekt zaregistrovaný a automaticky sa mu prideli ID stavby. Absentujúce ID stavby pri listinných podaniach má potenciál spôsobovať nejednotnosť postupu stavebných úradov. Podľa nášho názoru, existuje predpoklad, že stavebné úrady budú vyžadovať doplnenie žiadosti o ID stavby, nakoľko je žiadosť neúplná a bez tohto údaje nemôžu (nemali by) ďalej konať alebo budú konať v konaní bez ID stavby, ktoré neuvedú v listine (napr. v rozhodnutí) hoci je jej obligatórnou náležitosťou.

Riešením problému absentujúceho ID stavby pri listinných podaniach, by mohlo byť, podľa nášho názoru, zakotvenie ustanovenia do nového stavebného zákona, ktorým by sa určila povinnosť stavebným úradom vygenerovať ID stavby podaniam, ktoré by mu boli doručené v listinnej podobe. *De lege ferenda* by sme zároveň navrhli vypustiť ID stavby ako obligatórnu náležitosť v záväznom stanovisku a záväznom vyjadrení osoby, pretože záväzná stanoviská a vyjadrenia sa vydávajú vo fáze, ktorá predchádza konaniu o stavebnom zámere, t. j. vo fáze prerokovania stavebného zámeru (prípadne i projektu stavby). Tieto návrhy by odstránili potenciálne rozpory v postupoch príslušných subjektov.

⁴² Pozri § 8 písm. c), § 9 a § 10 vyhlášky č. 60/2025 Z.z.

⁴³ Pozri § 63 ods. 3 NSZ.

⁴⁴ Pozri § 20 NSZ.

Zoznam použitých zdrojov

1. JAKUŠOVÁ, V., Pohľad na ID stavby z hľadiska elektronickej a listinnej formy podania. In: *Expert pre stavebné úrady*. 2/2025. Bratislava : Verlag dashöfer, s. r. o., s. 7 - 9. ISSN 2729-8434.
2. Portál výstavby. Stavebné úrady, [online] [cit. 28.08.2025] Dostupné na internete: <https://vystavba.uupv.sk/stranka/stavebne-urady>
3. SLOVENSKO.SK – ÚSTREDNÝ PORTÁL VEREJNEJ SPRÁVY. O portáli, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.slovensko.sk/sk/o-portali>
4. ÚRAD PRE ÚZEMNÉ PLÁNOVANIE A VÝSTAVBU SLOVENSKEJ REPUBLIKY. Plánované časové míľniky, [online] [cit. 05.09.2025] Dostupné na internete: <https://uupv.sk/>
5. ÚRAD PRE ÚZEMNÉ PLÁNOVANIE A VÝSTAVBU SLOVENSKEJ REPUBLIKY. Webinár, Blok č. 1 – stavebník, projektant. [online], [cit. 21.05.2025]. Dostupné na internete: <https://uupv.sk/aktuality/druhy-webinar-zamerany-na-predstavenie-jednotlivych-funkcionalit-portalu-vystavby>
6. Vyhláška č. 60/2025 Z. z. Úradu pre územné plánovanie a výstavbu Slovenskej republiky o štruktúre a prevádzke informačného systému územného plánovania a výstavby, o obsahu podaní a obsahu a rozsahu dokumentácie stavby v znení neskorších predpisov.
7. Webinár - Blok č. 3 - Stavebné úrady, [online] [cit. 29.07.2025] Dostupné na internete: <https://www.youtube.com/watch?v=Y5PpiehcZw8>
8. Zákon č. 200/2022 Z. z. o územnom plánovaní v znení neskorších prepisov.
9. Zákon č. 25/2025 Z. z. Stavebný zákon a o zmene a doplnení niektorých zákonov (Stavebný zákon) v znení neskorších predpisov.

Kontaktné údaje

JUDr. Viera Jakušová, PhD.

viera.jakusova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

AUTOMATIZOVANÝ SYSTÉM ADRESNEJ ENERGOPOMOCI VSLOVENSKEJ REPUBLIKE V KONTEXTE EURÓPSKEHO PRÁVA¹

AUTOMATED SYSTEM OF ADDRESSED ENERGY ASSISTANCE IN THE SLOVAK REPUBLIC IN THE CONTEXT OF EUROPEAN LAW

Kristína Slámková²

Abstrakt: Automatizovaný systém adresnej energopomoci na Slovensku prináša veľa právnych otázok. Aj keď ide o potenciálne efektívny nástroj sociálnej politiky štátu, musí fungovať v medziach právneho štátu. Príspevok analyzuje, či automatizovaný systém adresnej energopomoci podľa návrhu zákona o adresnej energopomoci v SR spĺňa požiadavky nariadenia GDPR a či zároveň napĺňa znaky vysokorizikového systému podľa AI Act. Metodicky vychádza z doktrinálnej analýzy čl. 6 a čl. 22 GDPR a z mapovania relevantných kategórií AI Act a tiež z pripravovaného znenia zákona a dôvodovej správy. Príspevok skúma, či ak systém priamo vedie k priznaniu alebo zamietnutiu pomoci, ide o rozhodnutie s právnym účinkom a uplatní sa čl. 22 GDPR. Tiež skúma, či pri využití profilovania alebo iných AI techník môže systém patriť medzi vysokorizikové podľa AI Act. Identifikuje medzery, ako je absencia explicitných procesných záruk (reálny human-in-the-loop, zrozumiteľné odôvodnenie, jednoduché odvolanie), povinné DPIA, logovanie a audity férovosti a testy nediskriminácie. Pozornosť venuje riziku function creep a zásade minimalizácie. Navrhuje *de lege ferenda* doplniť tieto záruky a prepojiť krátkodobú cenovú dostupnosť energií s dlhodobou energetickou efektívnosťou aby bol systém nielen efektívny, ale aj právne udržateľný a verejne kontrolovateľný.

Kľúčové slová: AI Act, GDPR, energopomoc, zodpovednosť

Abstract: The automated system of targeted energy assistance in Slovakia raises numerous legal questions. Although it is a potentially effective instrument of social policy, it must operate within the bounds of the rule of law. This paper analyzes whether the automated system envisaged by the Draft Act

¹ Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0543.

² Univerzita Komenského v Bratislave, Právnická fakulta.

on Targeted Energy Assistance complies with the GDPR and whether it simultaneously meets the criteria of a high-risk system under the AI Act. Methodologically, it proceeds from a doctrinal analysis of Articles 6 and 22 GDPR, a mapping of the relevant AI Act categories, and an examination of the draft statutory text and its explanatory memorandum. The paper assesses whether, where the system directly grants or denies assistance, this amounts to a decision producing legal effects that triggers Article 22 GDPR. It also considers whether, through the use of profiling or other AI techniques, the system may fall within the AI Act's high-risk class. It identifies gaps such as the absence of explicit procedural safeguards (a genuine human-in-the-loop, intelligible reasoning, and a simple appeal), a mandatory DPIA, logging and fairness audits, and non-discrimination testing. Attention is paid to the risks of function creep and to the principle of data minimisation. *De lege ferenda*, it proposes adding these safeguards and linking short-term energy affordability with long-term energy efficiency so that the system is not only effective but also legally sustainable and publicly accountable.

Key words: AI Act, GDPR, energy assistance, responsibility

Úvod

Miera autonómnosti rozhodovania zverená vo verejnej správe umelej inteligencii („AI“) sa v štátoch európskej únie („EÚ“) líši, no v zásade platí, že dôležité rozhodnutia, ktoré majú vplyv na práva a povinnosti účastníkov konania alebo občanov, by nemali byť ponechané na algoritmy bez toho, aby bol v procese rozhodovania zahrnutý aj ľudský faktor. V praktickej rovine si to môžeme predstaviť ako situáciu, kedy človek potvrdí, alebo môže ešte korigovať výstupy AI. AI má primárnu úlohu v tomto procese poslužiť orgánu verejnej správy ako pomocník, ale ultimátna zodpovednosť je stále na orgáne verejnej správy a na ľudskom posúdení výsledku rozhodovacieho procesu. Napríklad Najvyšší kontrolný úrad začal v roku 2025 využívať AI pri posudzovaní presnosti svojich rozhodnutí a efektivity rozhodovania a práce úradu. Úrad už využíva AI napríklad na automatickú sumarizáciu dokumentov, generovanie zápisov zo stretnutí, návrhy textov záverečných správ z výsledkov kontrol a i.

AI už začína prenikať aj do strategickej úrovne pri tvorbe verejných politík a opatrení na znižovanie energetickej náročnosti. Na Slovensku štát v rokoch 2023-2025 zvolil plošné dotovanie cien energií. Z dôvodu, že takéto dotovanie cien energií predstavovalo obrovskú záťaž pre verejné financie, vznikla vízia adresnej energopomoci.

Cieľom tohto príspevku je vysvetliť navrhovaný systém adresnej energopomoci a jeho právny základ a identifikovať kľúčové problémy tohto systému. Za týmto účelom si autorka stanovila jednu výskumnú otázku: Je navrhovaný automatizovaný systém energopomoci na Slovensku v súlade s právom EÚ?

Príspevok je rozdelený na úvod, záver a jadro, ktoré tvorí tri na seba logicky nadväzujúce časti.

V prvej časti, je základným cieľom poskytnúť informácie o tom, čo je adresná energopomoc, poskytnúť kontext a základné informácie potrebné pre následnú právnu analýzu.

V druhej časti autorka analyzuje relevantné ustanovenia GDPR, najmä čl.6 a čl. 22 a vhodne ich aplikuje na systém energopomoci. Skúma, či je navrhovaný systém adresnej energopomoci automatizované rozhodnutie s právnym účinkom podľa GDPR. V tejto časti sa autorka usiluje o posúdenie za akých podmienok je systém v súlade s GDPR a pokúsi sa identifikovať prípadné nedostatky v podobe absencie procesných záruk v národnej úprave.

V tretej časti autorka rozoberá Nariadenie o umelej inteligencii a odpovedá na otázku, či je systém adresnej energopomoci systémom AI podľa tohto nariadenia a ak áno, či ide o vysokorizikový systém AI.

V celom príspevku je z hľadiska metodológie použitá primárne analýza právnych textov, syntéza, komparácia a dedukcia.

Národný právny rámec a opis systému adresnej energopomoci

Zvyšovanie energetickej efektívnosti je dnes prioritou, pretože najčistejšia a najekologickejšia energia je tá, ktorú vôbec nespotrebujeme. Keďže budovy tvoria približne 40 % spotreby energie v EÚ a asi tri štvrtiny bytového fondu nespĺňajú požiadavky energetickej náročnosti, je nevyhnutné riešiť tento aspekt komplexne už vo fáze architektonického návrhu s ohľadom na lokalitu a klímu.³ Opatrenia na zvýšenie energetickej efektívnosti (zateplovanie, výmena okien, fotovoltika) štát tradične spolufinancuje formou dotácií a grantov. Administrácia týchto schém je však často pomalá a nákladná, čo oslabuje ich dosah na zraniteľné domácnosti.⁴ Zhoda odbornej verejnosti je v tom, že automatizované rozhodovanie by tomuto problému pomohlo, avšak automatizácia takýchto systémov naráža na limity európskeho práva. Európska únia je často vnímaná ako globálny líder v regulácii nových technológií a jej normy majú neraz mimounijný dopad, keď fakticky nastavujú

³ KUDLÍK, Leoš: Průkaz energetické náročnosti budov jako nástroj energetických úspor. In: Acta Universitatis Carolinae Iuridica. 2020. s. 35-36.

⁴ Pozri napr. <https://e.dennikn.sk/3431470/v-lete-rekonstruovat-nebudete-stat-meska-aj-s-vyhodnotenim-tretej-vyzvy-obnov-dom/> alebo aj <https://www.energie-portal.sk/Dokument/zelena-domacnostiam-poukazky-ziadosti-2024-110939.aspx>.

podmienky fungovania podnikov aj mimo EÚ. Regulácia umelej inteligencie však prináša celé spektrum otázok, na ktoré klasické právne nástroje nemusia stačiť. Navyše, rýchla a široká implementácia AI naprieč sektormi a jurisdikciami sťažuje vytváranie koordinovanej a jednotnej právnej úpravy.⁵ Z konštatovania Súdneho vieme základné aplikačné pravidlo, ktorým potvrdil všeobecnú prednosť práva EÚ pred vnútroštátnym právom, a to aj v prípade, ak bol dotknutý právny akt EÚ prijatý skôr ako príslušná vnútroštátna norma. Neuplatňuje sa tu teda pravidlo *lex posterior derogat priori*. Uvedené potvrdzuje, že v prípade rozporu vnútroštátnej normy s európskym právom, orgány dotknutého štátu takúto vnútroštátnu normu nemôžu uplatňovať. Opodstatnenosť tohto rozlíšenia podčiarkuje aj čl. 7 ods. 2 Ústavy SR: „(...) Právne záväzné akty Európskych spoločenstiev a Európskej únie majú prednosť pred zákonmi Slovenskej Republiky (...)“.⁶

V tomto článku sme si dali za úlohu rozobrať nové automatizované rozhodovanie na Slovensku v systéme adresnej energopomoci práve v kontexte práva EÚ. V tejto časti príspevku predstavíme pripravovanú novú národnú legislatívu v tejto oblasti a to Návrh zákona o adresnej energopomoci a o zmene a doplnení niektorých zákonov („**ZoEP**“).⁷

Zákon o adresnej energopomoci sleduje krátkodobý cieľ: automatizovanou finančnou podporou stabilizovať rozpočty domácností ohrozených energetickou chudobou. Energopomoc a dotácie a granty na zvyšovanie energetickej efektívnosti sa vzájomne dopĺňajú. Dotácie a granty znižujú spotrebu dlhodobo (investície do energetickej efektívnosti), kým adresná energopomoc rieši okamžitú a nárazovú cenovú dostupnosť energií pre spotrebiteľov. Aby sa zachoval súlad s GDPR⁸ a posilnila transparentnosť, pridelenie energopomoci by malo obsahovať jasné odôvodnenia, správne procesy a pravidelné audity dopadov. Zároveň môže poskytnúť poznatky a skúsenosti na lepšie zacielenie budúcich investičných programov energetickej efektívnosti, ako je napríklad identifikácia typov domácností s najvyššími úsporovými prínosmi. Prakticky to možno prepojiť tak, že príjemcovia energopomoci dostanú automatickú informáciu o dostupných opatreniach, prípadne bonus na energetický audit a prioritu v poradovníkoch obnovy budov, čím sa krátkodobá pomoc mení na trvalé zníženie spotreby.

⁵ METEŇKANYČ, M. Olexij – GYURÁSZ, Zoltán: Priznanie práv a právnej subjectivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s. 71.

⁶ VRABKO, Marián a kol: Právo v energetike. 1. vydanie. Bratislava: Wolters Kluwer SR, 2023. s. 90-91.

⁷ Návrh zákona o adresnej energopomoci a o zmene a doplnení niektorých zákonov, číslo materiálu UV-27330/2025, rezortné číslo 28272/2025-2062-65920.

⁸ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) („GDPR“).

Ministerstvo hospodárstva Slovenskej republiky oznámilo vývoj automatizovaného systému adresnej energopomoci, prostredníctvom ktorého bude možné integrovať údaje z existujúcich registrov štátu⁹ a má sa umožniť udelenie príspevku domácnostiam bez žiadosti zo strany žiadateľa o dotáciu. ZoEP vytvára právny rámec pre adresnú energopomoc v SR.

V zmysle ZoEP¹⁰ je adresnou energopomocou cielená pomoc štátu energetickej domácnosti na čiastočnú úhradu nákladov na spotrebu elektriny, plynu a tepla. Poskytnutím adresnej energopomoci majú byť dotknuté energetické domácnosti, ktorým vznikne na rok 2026 právo na energopomoc, ochránené pred nárastom úhrad za elektrinu, plyn a teplo. Ku koncu roka 2025 dôjde k ukončeniu plošnej kompenzácie nákladov na energie a od 1. januára 2026 budú uplatňované cenové rozhodnutia Úradu pre reguláciu sieťových odvetví bez aplikovania inštitútu krízovej regulácie podľa § 16a zákona č. 250/2012 Z. z. o regulácii v sieťových odvetviach v znení neskorších predpisov.¹¹

Európsky rámec ochrany osobných údajov a automatizované rozhodovanie

Orgány verejnej moci, ktoré sú v zmysle návrhu ZoEP orgánmi štátnej správy pre adresnú energopomoc Ministerstvo hospodárstva SR („**MH SR**“) a okresné úrady, nevyhnutne pracujú s osobnými údajmi dotknutých osôb. Podľa čl. 6 GDPR musí byť spracúvanie údajov založené na právnom základe. V danom prípade prichádzajú v úvahu najmä č. 6 ods. 1 písm. c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti, a čl. 6 ods. 1 písm. e) spracúvanie je potrebné na výkon úlohy realizovanej vo verejnom záujme. Hoci zákon teoreticky spĺňa požiadavku zákonného základu podľa čl. 6 ods. 1 písm. e) GDPR (spracúvanie vo verejnom záujme), je namieste preskúmať, či zároveň rešpektuje princípy obmedzenia účelu a minimalizácie údajov podľa čl. 5 ods. 1 GDPR.

GDPR vyžaduje, aby osobné údaje boli získavané na konkrétne určené, výslovne uvedené a legitímne účely. Zákon o adresnej energopomoci však formuluje účel pomerne všeobecne „*na účely poskytovania adresnej energopomoci*“. V praxi to znamená, že ministerstvo zhromažďuje údaje preto, aby mohlo posúdiť potrebu kompenzácií nákladov na energie a určiť, kto má nárok na štátom dotované ceny energie. Hoci ide o legitímny verejný záujem, ktorým je ochrana zraniteľných domácností pred energetickou chudobou, zákon bližšie nešpecifikuje podrobnosti spracovania. V texte navrhovaného zákona nenachádzame výslovný opis toho, ako presne budú údaje využité. Najmä tým myslíme to, či iba na jednorazové stanovenie

⁹ § 13 ods. 3, 4 a 5 ZoEP.

¹⁰ § 2 písm.a) ZoEP.

¹¹ Dôvodová správa k zákonu č. 71/2025 o poskytovaní údajov na účel adresnej energopomoci. Všeobecná časť.

kritérií pomoci, na priebežné vyhodnocovanie energetickej chudoby alebo na iné analytické účely. Táto absencia konkrétnejšej definície účelu môže byť problémom z hľadiska zásady obmedzenia účelu podľa GDPR. Účel, ktorým je poskytovanie energopomoci je pomerne široký a vágny, čo znižuje transparentnosť. Dotknuté osoby sa fakticky dozvedajú len to, že ich údaje budú použité niekedy v budúcnosti na neurčito definovanú adresnú podporu. Detailné pravidlá pomoci zákon totiž ponecháva na úpravu vykonávacím predpisom. Z pohľadu GDPR by bolo vhodnejšie, keby zákon presnejšie uvádzal konkrétne úlohy spracúvania, napríklad, že údaje budú použité na výpočet príjmu domácnosti, vyhodnotenie nároku a informovanie oprávnených osôb. Súčasná formulácia tak môže viesť k pochybnostiam, či je účel dostatočne výslovne uvedený a vymedzený.

Zásada minimalizácie údajov podľa GDPR stanovuje, že osobné údaje majú byť „primerané, relevantné a obmedzené na nevyhnutný rozsah vzhľadom na účely“. ZoEP však ministerstvu umožňuje získať mimoriadne široký okruh údajov o fyzických osobách, domácnostiach a členoch spoločných domácností. Zákon vyčerpávajúco vymenúva desiatky údajových položiek z rôznych registrov, od údajov o nehnuteľnostiach¹² cez údaje z registra obyvateľov¹³ až po finančné a sociálne informácie¹⁴ a napokon údaje o spotrebe energií každého odberného miesta¹⁵. Prakticky kompletný socio-ekonomický profil domácností. Inými slovami, štát plánuje zosumarizovať príjmovú stránku každej domácnosti, mzdy, dávky, dôchodky a výdavkovú stránku, najmä energetické náklady.

Je pravdou, že zákon v §13 ods. 6 detailne vypočítava, ktoré konkrétne údaje z jednotlivých registrov sa budú poskytovať. Na prvý pohľad teda právna úprava špecifikuje rozsah údajov pomerne presne. Problémom však zostáva odsek 7, ktorý dopĺňa, že MH SR sa poskytujú aj ďalšie údaje, ktoré sú v súlade s účelom spracúvania a sú potrebné na účel poskytovania adresnej energopomoci. Toto otvorené ustanovenie fakticky umožňuje rezortu dodatočne si vyžiadať akékoľvek ďalšie dáta, pokiaľ ich vyhodnotí ako potrebné pre široko definovaný účel energopomoci. Z hľadiska minimalizácie podľa GDPR je to kritické. Namiesto uzavretého zoznamu nevyhnutných údajov ponecháva zákon dvierka na rozšírenie záberu. Takáto formulácia oslabuje istotu, že sa nebude zbierať viac informácií, než je skutočne nutné. GDPR pritom vyžaduje, aby zákonný podklad spracúvania v rámci čl. 6 ods. 3 jasne vymedzil okruh dotknutých údajov – tu však máme generálnu klauzulu na bližšie nedefinované ďalšie údaje, čo môže byť v rozpore s princípom predvídateľnosti a proporcionality.

¹² kataster: adresa bytu/domu, výmera, vlastník

¹³ meno, rodné číslo, rodinný stav, trvalý pobyt, rodinné vzťahy

¹⁴ príjmy z daňovej správy, dávky zo Sociálnej poisťovne, dôchodky, výsluhové príspevky, dávky v hmotnej núdzi

¹⁵ spotreba elektriny, plynu či tepla, tarif, prípadne cena a objem dodaného tepla

Za diskutabilné sa dajú považovať aj niektoré konkrétne kategórie údajov požadované zákonom. Systém má zbierať napríklad údaje o konečných užívateľoch výhod z registra partnerov verejného sektora¹⁶, čo implikuje prepojenie na podnikateľské aktivity členov domácnosti. Nejasným zostáva odôvodnenie potreby takých údajov v rámci energopomoci. Široko vymedzené sú aj finančné data. Návrh ZoEP hovorí o údajoch „získaných pri správe daní, ktoré sú potrebné pre posúdenie poskytovania energopomoci“, no konkrétne typy daňových údajov, či pôjde o výšku základu dane, druhu príjmov, počet vyživovaných osôb atď., nie sú v zákone explicitne vymenované. Takéto generické odkazy môžu viesť k nadužívaniu zberu osobných údajov. Správny orgán si môže vyžiadať potenciálne veľmi detailné finančné informácie, pokiaľ ich bude považovať za relevantné pre účely pomoci.

Celkovo vzaté, rozsah spracúvania podľa tohto zákona je mimoriadne rozsiahly a podľa názoru autorky neúmerný. Princíp proporcionality, či je zásah do súkromia primeraný sledovanému cieľu, bude kľúčový.

Je pravda, že Slovensko doposiaľ nemalo zavedený mechanizmus merania energetickej chudoby a identifikácie zraniteľných domácností, takže vláda siahla po masívnom zbere dát ako riešení. Z hľadiska GDPR však platí, že aj verejný záujem musí byť dosahovaný spôsobom čo najmenej zasahujúcim do súkromia jednotlivca. Ponúka sa otázka, či by nebolo možné nastaviť adresnú pomoc menej invazívne. Napríklad dobrovoľným podávaním žiadostí o energetickú pomoc zo strany občanov, ktorí by doložili potrebné údaje (prípadne so spätným overením v registroch). Vláda síce argumentuje, že automatické vyhodnotenie bez nutnosti podávania žiadostí je znížením byrokracie pre občanov, no za cenu plošného profilovania populácie.

Profilovanie má v práve EÚ legálne vymedzenie. Ide o automatizované spracúvanie osobných údajov, pri ktorom sa údaje používajú na vyhodnotenie osobných aspektov fyzickej osoby (napr. pracovná výkonnosť, majetkové pomery, zdravie, preferencie, spoľahlivosť, správanie, poloha či pohyb) podľa čl. 4 bod 4 GDPR. Ak však profilovanie nevýústi do individuálneho rozhodnutia, ide v zásade o bežnú spracovateľskú operáciu bez osobitných právnych účinkov oproti iným operáciám (analýza, prenos). Pojmovovo zahŕňa dva kroky (i) získanie a modelovanie charakteristík o jednotlivcovi či skupine, čiže kreáciu profilu a (ii) aplikáciu profilu na konkrétneho jednotlivca alebo skupinu; oba kroky sú viazané na automatizáciu, avšak nevylučujú ľudský zásah, a prvok hodnotenia osobných aspektov sa týka tak kreácie, ako aj aplikácie profilu. Zároveň platí, že nie každá jednoduchá klasifikácia (napr. podľa veku či pohlavia)

¹⁶ Register partnerov verejného sektora nazývaný i „protischránkový zákon“, je jedným z nástrojov celospoločenskej kontroly nakladania s verejnými zdrojmi, pričom jeho cieľom je zvýšiť transparentnosť vzťahov medzi verejným a súkromným sektorom, a to takým spôsobom, že podrobí zverejneniu a prevereniu informácie o skutočných vlastníkoch subjektov, ktoré obchodujú so štátom. In: ZIGO, Daniel. Register partnerov verejného sektora a odhaľovanie vlastníckych štruktúr spoločnosti. *Acta Facultatis Iuridicae Universitatis Comenianae*. 2021, s.222-223.

musí nevyhnutne predstavovať profilovanie v zmysle GDPR. Z pohľadu regulácie sa preto na profilovanie uplatnia všeobecné požiadavky GDPR na zákonnosť, transparentnosť a spravodlivosť spracúvania, vrátane voľby právneho základu a rešpektovania zásad spracúvania.¹⁷ Takéto riešenie možno z hľadiska minimalizácie údajov spochybníť, keďže zahrnie aj údaje ľudí, ktorí nakoniec žiadnu pomoc nepotrebujú ani nedostanú. Môžeme sa teda z hľadiska GDPR opýtať legitímnu otázku, či na odfiltrovanie 10–20 % najbonitnejších domácností je nevyhnutné zbierať detailné osobné údaje 100 % populácie.

Ďalšou otázkou, ktorú navrhovaná právna úprava otvára je súlad s čl. 22 GDPR. Je teda navrhovaný systém adresnej energopomoci automatizované rozhodnutie s právnym účinkom podľa GDPR? Uvedená otázka sa javí ako kľúčová podľa čl. 22 GDPR, ktorý zakazuje, aby bol jednotlivец vystavený rozhodnutiu založeného výlučne na automatizovanom spracúvaní, ktoré ho významne ovplyvňuje a má právne účinky, pokiaľ nie sú splnené podmienky v ods. 2 daného článku. Výnimka sa uplatní len vtedy, ak takéto rozhodnutie povoľuje právny predpis a sú zavedené primerané procesné záruky ako je právo na ľudský zásah, právo vyjadriť vlastný názor a právo rozhodnutie napadnúť.¹⁸ Článok 22 sa často kritizuje za to, že zužuje úlohu človeka v komplexných rozhodovacích procesoch. V praxi sa totiž vykladá tak, že aby sa predišlo plnej automatizácii, musí byť na samom konci prítomný človek s kompetenciou výsledok stroja potvrdiť alebo zmeniť. Tým sa však fakticky opomína významný ľudský zásah v skorších fázach, čo je sporné. Navyše, keď inteligentné systémy preukázateľne prekonávajú ľudské schopnosti, adresáti majú sklon ich rozhodnutia skôr potvrdiť — buď pre tzv. automatizačné skreslenie, alebo preto, že je veľmi ťažké presvedčivo vysvetliť, prečo by sa mal výstup „vysoko presného“ nástroja v konkrétnom prípade zmeniť.¹⁹ V literatúre sa inteligencia a intencionalita zariadení na báze AI často chápu ako technické vlastnosti algoritmov, no významná filozofická línia²⁰ trvá na tom, že vedomie a skutočná intencionalita sú výlučne ľudské. Z praktického hľadiska však možno hovoriť o zámernosti systému v tom zmysle, že správanie autonómnych agentov²¹ vieme do istej miery predikovať, čo

¹⁷ ŽATKOVÁ, Sandra – MESARČÍK, Matúš: Umelá inteligencia, profilovanie a sociálne médiá. In: MESARČÍK, Matúš - GYURÁSZ, Zoltán, a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s.223-224.

¹⁸ EDWARDS, Lilian – VEALE, Michael: Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"? In: *IEEE Security & Privacy*, 16(3), 2018. s.3.

¹⁹ SARRA, Claudio: Artificial Intelligence in Decision-making: A Test of Consistency between the „EU AI Act“ and the „General Data Protection Regulation“. In: *Athens Journal of Law – Volume 11*, č.1 (2025), s.48-49.

²⁰ Pozri napr. SEARLE, J.: *Intentionality: An Essay in the Philosophy of Mind*, Cambridge University Press, 1983 alebo RUSSEL, S.: *Rationality and Intelligence*, 1997, Dostupné na: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.48.9785&rep=rep1&type=pdf>.

²¹ Napríklad robotický vysávač.

legitimizuje používanie intencionálneho slovníka pri opise ich činnosti. Koncepcia dokonalej racionality je v AI problematická. Vzhľadom na časové a výpočtové obmedzenia je rozhodovanie vždy aspoň čiastočne suboptimálne. Súčasný systém preto nemá slobodnú vôľu a konajú v medziach inštrukcií a učiacich pravidiel, hoci sa autonómne učia a upravujú svoje vnútorné parametre.²²

Zároveň je potrebné riešiť aj zodpovednostný režim pri chybách automatizácie, napríklad v prípade zamiestnutia pomoci. Zodpovednostný režim má byť nastavený tak, aby poškodený nemusel dokazovať vnútorné fungovanie algoritmu. V doktríne je použiteľná analógia *respondeat superior*, ktorá hovorí o tom, že na to, aby bolo možné aplikovať doktrínu *respondeat superior*, je potrebné preukázať existenciu primárneho vzťahu medzi nadriadeným a podriadeným, ako aj jasnú súvislosť medzi týmto vzťahom a správaním podriadeného, ktoré by viedlo k vzniku škody.²³ Pri implementácii ZoEP je kľúčové vyriešiť, kto nesie následky chybného rozhodnutia automatizovaného systému. Vychádzajúc z analógie *respondeat superior*, platí, že škody spôsobené konaním umelej inteligencie by mal nahradiť jej vlastník alebo právnická osoba, za ktorú koná.²⁴ Takéto uchopenie zodpovednosti dopĺňa procesné záruky podľa čl. 22 GDPR a vytvára praktický rámec nápravy keď automatizovaný systém pri rozhodovaní zlyhá.

Nariadenie o umelej inteligencii a implikácie pre adresnú energopomoc

AI môže zároveň v závislosti od okolností týkajúcich sa jej konkrétnej aplikácie, použitia a úrovne technologického vývoja vytvárať riziká a ujmu pre verejné záujmy a základné práva, ktoré sú chránené právom Únie. Toto poškodzovanie môže byť hmotné aj nehmotné vrátane fyzickej, psychickej, spoločenskej alebo ekonomickej ujmy.²⁵ Pri algoritmickej rozhodovani je legitímnou otázkou, aká transparentnosť je vlastne užitočná. V tejto časti sa preto snaží autorka ujasniť, či adresná energopomoc podľa ZoEP spĺňa definíciu systému umelej inteligencie podľa čl. 3 AI Act, tiež posudzuje či ide o vysokorizikový systém podľa prílohy III k AI Act a mapuje kľúčové povinnosti pre poskytovateľa a používateľa vo verejnej správe, vrátane ľudského dohľadu a transparentnosti. Transparentnosť často naráža na právo na súkromie. Jednotlivec môže chcieť, aby jeho údaje ostali neverejné, a zároveň žiadať vysvetlenie fungovania systému postaveného na tých istých dátach. V praxi platí, že dôvera predchádza transparentnosti. Informácie sa sprístupňujú len dôveryhodným

²² CIHANOVÁ, Jana – GYURÁSZ, Zoltán: Právo duševného vlastníctva a umelá inteligencia, In: MESARČÍK, Matúš - GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s. 150-151.

²³ GYURÁSZ, Zoltán: Keď umelá inteligencia robí chyby: *respondeat superior*, In: Bratislavské právnické fórum 2024 . Univerzita Komenského v Bratislave. Právnická fakulta UK, 2024. s. 87.

²⁴ Tamtiež. s. 88.

²⁵ Preambula Nariadenia o umelej inteligencii.

partnerom a ani „iba metadáta“ nie sú neškodné, čo ukazujú debaty predstaviteľov informačných služieb o zbere dát a ich konštatovanie, že rozhodnutia o živote a smrti sa robia aj na základe metadát.²⁶

Autorku k skúmaniu otázok v tejto časti viedla tá skutočnosť, že v materiály, ktorý je zverejnený k návrhu ZoEP nenašla vysporiadanie zákonodarcu s nižšie nastolenými otázkami nezaoberal a javia sa ako podstatné.

Nariadenie o umelej inteligencii²⁷ v čl. 3 ods. 1 definuje systém umelej inteligencie ako strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie.²⁸

Je teda systém adresnej energopomoci umelou inteligenciou podľa AI Act?

Dôležité pre posúdenie tejto otázky sú časti definície predmetného článku nariadenia a to prvky autonómie, či generovanie výstupov, ktoré môžu ovplyvniť rozhodovanie človeka. Adresná energopomoc podľa ZoEP je navrhnutá ako informačný systém verejnej správy, ktorý spravuje Ministerstvo hospodárstva Slovenskej republiky a ktorý automatizovane vyhodnocuje a zhromažďuje údaje z registrov štátu, ktoré uvádza ZoEP v § 13. Posúdenie nároku ako aj všetky úkony prebiehajú automatizovane medzysystémovou komunikáciou a následne systém vypočíta bonitu energetickej domácnosti, rovnako tak overuje kritériá nároku.²⁹ Tento proces je plne automatizovaný, bez akéhokoľvek zásahu zamestnanca orgánu verejnej správy.³⁰ Manuálne sa táto fáza nároku na priznanie energopomoci neposudzuje. Je pravda, že systém adresnej energopomoci podľa dostupných informácií nevyužíva strojové učenie a pracuje na pevne daných pravidlách. Podľa čl. 3 ods. 1 a výkladu AI Act nie každý pravidlami riadený softvér spadá pod pojem „AI systém“: rozhodujúce je, či systém inferuje (odvodzuje) zo vstupov spôsob generovania výstupov a či môže po nasadení prejavovať adaptivitu (teda schopnosť meniť výstupy na základe nových dát, spätnej väzby alebo zmeny prostredia). Ak systém len mechanicky uplatňuje zákonom dané pravidlá bez vlastného odvodzovania, systém pravdepodobne nepodlieha AI Act. Naopak, ak by obsahoval znalostný modul alebo komponent

²⁶ WELLER, Adrian: Transparency: Motivation and Challenges. 2017. s. 7.

²⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) ďalej ako („AI Act“).

²⁸ Článok 3 ods. 1 Nariadenia o umelej inteligencii.

²⁹ Dôvodová správa k § 4 zákona č. 71/2025 o poskytovaní údajov na účel adresnej energopomoci. Osobitná časť.

³⁰ § 4 ods. 3 ZoEP.

strojového učenia, už by pod AI Act spadal. Nech je zaradenie podľa AI Act akékoľvek, aktuálny model rozhodovania je výlučne automatizovaný a výsledkom je individuálny správny akt s právnym účinkom, takže sa uplatní čl. 22 GDPR vrátane požiadaviek na ľudský zásah, možnosť namietať a primerané vysvetlenie.³¹

Po zodpovedaní na prvú položenú otázku je potrebné následne zodpovedať si, či systém adresnej energopomoci patrí medzi vysokorizikové systémy umelej inteligencie podľa Nariadenia o umelej inteligencii. Je to dôležité najmä z toho dôvodu, aby sme vedeli posúdiť, či spĺňa všetky podmienky takéhoto systému a jeho uvedenia na slovenský trh, ktoré určuje Nariadenie o umelej inteligencii. Rovnako je to potrebné pre posúdenie súladu vnútroštátneho práva s európskou legislatívou.

Z hľadiska klasifikácie rizika a po preskúmaní prílohy č. III k AI Act môžeme povedať, že tento systém môže za istých okolností byť systémom patriacim do kategórie vysokorizikových. Je to preto, že rozhodovanie o energopomoci je rozhodovaním vo verejnej správe s právnymi účinkami pre jednotlivca. Z tohto dôvodu môžeme povedať, že by sa naň uplatnili povinné požiadavky vysokorizikových systémov AI. Táto klasifikácia sa použije bez ohľadu na to, či použijeme úpravu čl. 22 GDPR. Z pohľadu GDPR to zároveň znamená, že rozhodnutie o energopomoci je automatizované rozhodnutie s právnym účinkom.

Vysokorizikové systémy umelej inteligencie by sa mali uviesť na trh EÚ alebo do prevádzky alebo by sa mali využívať len vtedy, ak spĺňajú určité povinné požiadavky. Týmto požiadavkami by sa malo zabezpečiť, aby vysokorizikové systémy umelej inteligencie, ktoré sú dostupné v EÚ alebo ktorých výstupy sú v EÚ inak využívané, nepredstavovali neprijateľné riziká pre dôležité verejné záujmy EÚ uznané a chránené právom EÚ.³²

Keďže technické špecifikácie riešenia zatiaľ nie sú verejne známe, pracujeme s dvoma alternatívami: ak by systém obsahoval komponenty strojového učenia či iné inferenčné (adaptívne) prvky, spĺňal by definíciu „AI systému“ podľa čl. 3 ods. 1 AI Act a vzhľadom na rozhodovanie o nároku na verejnú pomoc by šlo o vysokorizikové použitie s príslušnými povinnosťami poskytovateľa a používateľa. Ak však pôjde len o čisto deterministický, pravidlami riadený softvér bez inferencie a adaptivity, ktorý mechanicky aplikuje zákonom stanovené kritériá, AI Act sa pravdepodobne neuplatní; v oboch scenároch však platí GDPR vrátane čl. 22, keďže rozhodnutie má právne účinky a je generované výlučne automatizovane.

³¹ Rozhodnutie má svoju legálnu definíciu v § 3 ods. 1 písm. b) SSP. Podľa tohto ustanovenia je rozhodnutím orgánu verejnej správy správny akt vydaný orgánom verejnej správy v administratívnom konaní, ktorý je formálne označený ako rozhodnutie ale je za rozhodnutie považovaný podľa osobitného predpisu a zakladá, mení, zrušuje alebo deklaruje práva, povinnosti fyzickej osoby a právnickej osob, alebo sa jej priamo dotýka. Pozri k tomu: VRABKO, Marián: Správne právo hmotné. Všeobecná časť, 3. vydanie. Bratislava: C.H. Beck, 2025, s. 144.

³² Preambula ods.46 Nariadenia o umelej inteligencii.

Záver

V úvode sme si položili hlavnú výskumnú otázku, ktorá znela nasledovne: Je navrhovaný automatizovaný systém energopomoci na Slovensku v súlade s právom EÚ?

Na to aby sme ju mohli zodpovedať, sme si museli položiť dve nasledujúce otázky 1) Je navrhovaný systém adresnej energopomoci automatizované rozhodnutie s právnym účinkom podľa GDPR? 2) Je systém adresnej energopomoci umelou inteligenciou podľa AI Act?

Na základe vykonanej analýzy môžeme konštatovať, že v predloženej podobe návrhu nemožno automatizovaný systém adresnej energopomoci považovať za plne súladný s právom EÚ, hoci po doplnení určitých garancií je súlad realisticky dosiahnuteľný. Právny základ spracúvania podľa čl. 6 GDPR je obhájiteľný, no návrh pracuje s neurčito vymedzeným účelom a s otvorenou klauzulou na poskytovanie ďalších údajov, čo je ťažko zlučiteľné so zásadami obmedzenia účelu a minimalizácie. Keďže sme dospeli k záveru, že výsledkom procesu je individuálny správny akt s právnymi účinkami, nemôže zákonodarca opomínať čl. 22 GDPR. Návrh však výslovne neustanovuje reálny ľudský zásah, zrozumiteľné odôvodnenie a účinný opravný prostriedok. Návrh zákona neobsahuje ani žiadny z nástrojov ako DPIA, či vedenie záznamov. Rovnako tak neupravuje ani priebežné testovanie či predchádzanie „function creep“.

Na druhú čiastkovú otázku nemožno nájsť jasnú odpoveď práve z dôvodu, že návrh zákona neobsahuje bližšiu technickú špecifikáciu systému. Podľa AI Act systém spadá do režimu vysokého rizika vtedy, ak obsahuje inferenčné či adaptívne komponenty; v takom prípade musí byť preukázané riadenie rizík, kvalita dát, technická dokumentácia, ľudský dohľad a post-market monitoring, pričom rozhranie zodpovedností poskytovateľa a používateľa má byť jasne rozdelené. Ak pôjde len o deterministické uplatnenie zákonných pravidiel bez inferencie, AI Act sa pravdepodobne neuplatní, avšak požiadavky GDPR ostávajú plne relevantné. *De lege ferenda* preto navrhujeme spresniť účel a uzavrieť rozsah údajov, zakotviť „human-in-the-loop“, odôvodnenie a odvolanie, integrovať DPIA/FRIA a zaviesť auditné a antidiscriminačné mechanizmy; až potom možno hovoriť o súlade a legitímnej automatizácii, ktorá je zároveň transparentná a verejne kontrolovateľná. Praktickým doplnkom by mala byť možnosť dotknutým domácnostiam dopomôcť smerom k energetickej efektívnosti: príjemcom poskytnúť odporúčania, energetický audit či prioritu v obnovách budov, aby sa krátkodobá cenová pomoc prirodzene premenila na dlhodobé znižovanie spotreby.

Zoznam použitej literatúry

1. CIHANOVÁ, Jana – GYURÁSZ, Zoltán: Právo duševného vlastníctva a umelá inteligencia, In: MESARČÍK, Matúš - GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s. 150-151. ISBN: 978-80-7160-715-1.
2. EDWARDS, Lilian – VEALE, Michael: Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"? In: *IEEE Security & Privacy*, 16(3), 2018. s. 46–54.
3. GYURÁSZ, Zoltán: Keď umelá inteligencia robí chyby: respondeat superior, In: Bratislavské právnické fórum 2024 . Univerzita Komenského v Bratislave. Právnická fakulta UK, 2024. 150 s. ISBN 978-80-7160-728-1, s. 85-91.
4. KUDLÍK, Leoš: Průkaz energetické náročnosti budov jako nástroj energetických úspor. In: *Acta Universitatis Carolinae Iuridica*. 2020. s. 35-43. ISSN: 0323-0619.
5. MESARČÍK, Matúš - GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 244 s. ISBN: 978-80-7160-715-1.
6. METEŇKANYČ, M. Olexij – GYURÁSZ, Zoltán: Priznanie práv a právnej subjectivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, 133 s. ISBN: 978-80-7160-667-3.
7. SARRA, Claudio: Artificial Intelligence in Decision-making: A Test of Consistency between the „EU AI Act“ and the „General Data Protection Regulation“. In: *Athens Journal of Law – Volume 11*, č.1 (2025), s.45-62.
8. VRABKO, Marián a kol.: Právo v energetike. 1. vydanie. Bratislava: Wolters Kluwer SR, 2023. 212 s. ISBN 978-80-571-0620-3.
9. VRABKO, Marián: Správne právo hmotné. Všeobecná časť, 3. vydanie. Bratislava: C.H. Beck, 2025, 344 s. ISBN 978-80-8232-068-1.
10. WALMSLEY, Joel: Artificial intelligence and the value of transparency. In: *AI & Soc*, 36, 2021. s. 585–595. Dostupné: <https://doi.org/10.1007/s00146-020-01066-z>.
11. WELLER, Adrian: Transparency: Motivation and Challenges. 2017. Dostupné: <https://arxiv.org/pdf/1708.01870.pdf>.
12. ŽATKOVÁ, Sandra – MESARČÍK, Matúš: Umelá inteligencia, profilovanie a sociálne médiá. In: MESARČÍK, Matúš - GYURÁSZ, Zoltán, a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s.223-224. ISBN: 978-80-7160-715-1.
13. ZIGO, Daniel. Register partnerov verejného sektora a odhaľovanie vlastníckych štruktúr spoločnosti. In: *Acta Facultatis Iuridicae Universitatis Comenianae*. 2021, roč. 40, č. 2, s. 221–240. ISSN 1336-6912.

Použité právne predpisy SR a EÚ

14. Dôvodová správa k zákonu č. 71/2025 Z.z. o poskytovaní údajov na účel adresnej energopomoci.
15. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).
16. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) ("GDPR").
17. Zákon č. 250/2012 Z. z. o regulácii v sieťových odvetviach v znení neskorších predpisov.
18. Zákon č. 530/2023 Z.z., ktorým sa menia a dopĺňajú niektoré zákony v súvislosti so zlepšením stavu verejných financií.
19. Zákon č. 71/2025 Z.z. o poskytovaní údajov na účel adresnej energopomoci.

Kontaktné údaje

JUDr. Kristína Slámková, PhD.

kristina.slamkova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

ARTIFICIAL INTELLIGENCE IN THE ENERGY PERFORMANCE CERTIFICATION OF BUILDINGS: OPPORTUNITIES AND LIMITS OF SLOVAK PUBLIC ADMINISTRATION¹

Ľudovít Máčaj²

Abstract: The energy certification of buildings constitutes a legally prescribed procedure for assessing their energy performance. Its normative foundation is provided by Directive 2010/31/EU, subsequently revised by Directive (EU) 2024/1275, and transposed into Slovak law by Act No. 555/2005 Coll. The outcome of this process is the energy performance certificate, a public document with binding effects vis-à-vis third parties. The certificate performs several functions: normative, by ensuring the fulfilment of EU climate and energy objectives; protective, by guaranteeing transparency and legal certainty for owners, users and consumers; and regulatory, by serving as a basis for administrative decision-making.

Certification does not constitute administrative proceedings within the meaning of Slovak Code of Administrative Procedure but is instead a specialised professional activity carried out by authorised persons, with validity limited to ten years. The revised directive introduces more stringent requirements, notably the compulsory certification of all public buildings, the introduction of building passports, and increased digitalisation.

Artificial intelligence may enhance efficiency through automated calculations, digital processing of documentation, and error detection. Nonetheless, its function remains supportive, as legal responsibility rests with authorised experts and public authorities. Consequently, the deployment of AI raises issues of transparency, procedural safeguards, and the explainability of outcomes.

Key words: energy performance of buildings, artificial intelligence, public administration.

¹ This work was supported by the Slovak Research and Development Agency under the Contract no. APVV-24-0543.

² Comenius University in Bratislava, Faculty of Law, Department of Administrative and Environmental Law.

Introduction

Energy requirements for buildings represent one of the most topical issues in contemporary efforts to combat climate change. It is widely recognised that both the construction and subsequent use of buildings generate substantial amounts of carbon dioxide, as well as other substances that adversely contribute to changes in climatic conditions. This problem affects not only newly constructed buildings, but above all older ones which lack energy efficiency, particularly in respect of heating and heat loss, cooling, electricity generation, and their impact on the local environment in the immediate vicinity of the building.

The European Union has long sought to respond to these challenges. The most prominent instrument is Directive 2010/31/EU on the energy performance of buildings, which was recently subject to a significant revision by Directive (EU) 2024/1275 (hereinafter “EPBD”). This amendment introduces numerous innovations and obligations for a wide range of actors, from public authorities to private individuals. It forms part of the EU’s broader “green agenda”, aimed at achieving so-called carbon neutrality.

This paper addresses three key themes: the nature and significance of energy certification of buildings; the challenges associated with implementing EPBD; and the potential use of artificial intelligence in this context. We argue that AI tools may provide practical and effective means of simplifying and streamlining tasks linked to energy performance obligations (for instance, the certification and subsequent “passportisation” of all publicly accessible buildings). Accordingly, the paper explores both the potential and the limitations of AI in this area. Our central research question is: *to what extent may artificial intelligence be utilised within legal decision-making processes in the field of energy certification of buildings?*

The Legal Framework of Energy Performance Certification of Buildings

The European Union, and many other organisations and states seek to achieve energy efficiency in buildings for a variety of reasons. *Greater energy efficiency helps states meet several policy goals including: reduction of greenhouse gas emissions, cost reduction while supplying electricity, and grid-reliability improvement.*³ In order to achieve these objectives, a system of energy certification has been introduced within the European Union.

The energy certification of buildings may be understood as a legally prescribed procedure for assessing the energy performance of buildings. The outcome of this process is the energy performance certificate, a public document with binding legal effects vis-à-vis third parties.

³ QIU – KAHN, 2019, p. 461.

The legal basis lies, on the one hand, in the EPBD referred to above at the level of the European Union, and, on the other, in national legislation. In the case of Slovakia, this is Act No. 555/2005 Coll. on the Energy Performance of Buildings, as amended (hereinafter "Act No. 555/2005 Coll."). The directive has been implemented into this Act in various forms in the past, and as of September 2025 the transposition of its most recent version remains the subject of the legislative process, which will be addressed in a subsequent part of this paper.

*The transition from non-zero emission buildings (hereinafter "NZEB") to zero emission buildings (hereinafter "ZEB") is crucial for achieving the EU's climate neutrality goals. While current NZEB definitions show progress, improvements are needed to meet ZEB requirements and fulfil the EU's climate and energy objectives. This shift requires revising and tightening national standards, increasing renewable energy integration, setting operational greenhouse gases emissions thresholds, and focusing on adaptable designs and sustainable materials.*⁴

From a legal perspective, the energy certification of buildings fulfils several tasks and functions, which may be divided and described as follows:

Normative function:

The normative function primarily entails ensuring compliance with the European Union's climate and energy objectives, as well as the implementation of the principle of energy efficiency as a legal principle. This principle is reflected not only in the EPBD, but also in other pieces of Union legislation in the field of energy and is subsequently transposed into national legal frameworks.

Protective function:

Certification provides a guarantee of transparency and legal certainty for the owners and users of buildings concerned, including consumers. The aim of this function is also to ensure access to information in the context of legal transactions (such as sale, lease or occupancy permits). The parties involved must have the right to know the actual condition of the building and the extent to which it complies with the energy requirements imposed upon it.

Regulatory function:

Certification further constitutes a basis for decision-making by public authorities (for instance in relation to subsidies, zoning or construction proceedings). At the same time, it serves as a control instrument for monitoring compliance with obligations imposed on builders, as well as on owners and users of the buildings concerned.

In the Slovak Republic, energy certification constitutes a distinct process regulated by law, subject to state supervision through authorised entities. This certification does not amount to administrative proceedings within the meaning of Act No. 71/1967 Coll. on Administrative Procedure as amended, nor does it qualify as

⁴ MADUTA et al., 2025, p. 12.

administrative proceedings under any special regulation. For it to do so, it would have to constitute a procedure within the sphere of public administration, resulting in the issuance of a formal decision. By contrast, it represents a specific professional activity under Act No. 555/2005 Coll. Certification is carried out by authorised persons, namely entrepreneurs holding a regulated trade licence. Professional competence is required, as specified in Section 6 of Act No. 555/2005 Coll.

The outcome of this process is the issuance of an energy performance certificate⁵, a public-law attestation valid for a maximum period of ten years. Current legislation establishes the obligation to obtain certification in cases of sale and lease, for newly constructed or substantially renovated buildings, and for public buildings exceeding 250 m² in floor area.⁶

The certificate, as a public document, also carries specific legal consequences. It is electronically recorded in the central register maintained, pursuant to Section 9 of the Act, by the Ministry of Transport of the Slovak Republic. The certificate has legal effects vis-à-vis third parties, serving as formal proof of the building's energy classification.

In this respect, the role of the state is manifested on several levels: it supervises authorised persons and monitors compliance with certification obligations. In none of these cases, however, does this amount to administrative proceedings in the sense of an individual decision-making process within public administration.

Administrative proceedings arise only at the stage of sanctions and supervision: for instance, where the owner or another obligated person fails to comply with certification duties, or where an authorised person breaches the applicable rules.

New Requirements for Energy Performance Certification

Act No. 555/2005 Coll. is expected to undergo several amendments soon, directly linked to the obligation to implement the revised text of the EPBD. These forthcoming changes bring with them a few significant challenges.⁷

First, the scope of mandatory certification will be expanded. Every publicly accessible building will be required to obtain an energy performance certificate, regardless of its primary function. Second, the introduction of building passports is envisaged as a novel supplement to certification. However, debate continues as to whether these passports will be compulsory or voluntary in practice.

Third, the requirements concerning transparency will be tightened. Certificates will need to include more detailed content and will be more closely integrated with the

⁵ § 7 of Act No. 555/2005 Coll. as amended.

⁶ § 5 par. 2 b) of Act No. 555/2005 Coll. as amended.

⁷ Legislative procedure No. PI/2025/183. Available at: <https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/PI/2025/183> (cit. 27.09.2025).

central database, thereby enhancing public accessibility of information. Finally, the process will become increasingly digitalised: certificates will be issued and maintained electronically, with the prospect of linking them to a digital building logbook.

Taken together, these developments illustrate not only the growing regulatory complexity of the field, but also the ambitious direction of the EU's broader climate and energy agenda.

In addition to the forthcoming changes already outlined, building owners and other stakeholders will also face a series of further challenges. These include the promotion of solar energy, notably through the installation of photovoltaic panels on buildings, and questions concerning industrial constructions, which remain largely exempt from the new obligations.

The responsibilities of architects and project designers may also evolve, although the precise extent of these duties has not yet been clarified. Looking ahead to the post-2030 period, further requirements for new construction are expected, though their exact scope is still under discussion. E-mobility will also play an increasingly important role: for every five parking spaces, at least one charging point will be required.

Finally, transitional provisions will apply in the short term, such as reduced obligations for renovation projects completed before 2024. Alongside these measures, the planned introduction of a digital building logbook will add an additional layer of regulatory complexity in the years to come.

In sum, the forthcoming transposition of the revised EPBD into Slovak law marks a turning point in the regulation of energy performance in the building sector. The legislative process is not only a matter of technical compliance with EU law, but also an opportunity to strengthen the domestic framework in line with broader climate and energy objectives. The success of this process will depend on balancing ambitious targets with practical feasibility, ensuring that the obligations imposed on public authorities, private actors and professionals are both proportionate and enforceable. Ultimately, the transposition is expected to contribute to greater transparency, improved energy efficiency, and the long-term sustainability of the built environment.

Artificial Intelligence and the Energy Performance Certification of Buildings

The use of artificial intelligence tools in the energy certification of buildings may be envisaged in several respects. *Adopting artificial intelligence could reduce energy consumption and carbon emissions by approximately 8% to 19% in 2050. Combining with energy policy and low-carbon power generation could approximately reduce energy*

*consumption by 40% and carbon emissions by 90% compared to business-as-usual scenarios in 2050.*⁸

In the first place, AI can support the assessment of buildings, whether existing structures or those still at the planning stage of new construction. Its potential, however, extends further. It may also concern the issuing of certificates by authorised persons, who perform this activity as a regulated trade under the relevant legal provisions.

Carrying out this activity, including the subsequent issuance of certificates, will in the coming decades represent a significant challenge for all Member States of the European Union. We therefore take the view that the appropriate integration of artificial intelligence into this process could substantially simplify and streamline the workload. In particular, opportunities for its application may be identified in the following areas:

1. Automated calculations: Artificial intelligence tools can accelerate and increase the accuracy of calculations carried out in accordance with technical standards (consumption, CO₂ emissions, categorisation of the building). This applies particularly to the certification of existing buildings, where, as noted above, the obligation will affect a much larger number of structures. For this reason, automation will be essential for achieving the objectives of the EPBD as part of the European Union's climate policy.⁹

2. Digitalisation of documentation: Especially in the case of new constructions, which will be required to meet stricter limits, digitalisation will constitute an indispensable prerequisite for the rapid and efficient processing of project documentation and measurements, without the need for manual transcription.

3. Predictive models: Such models may, for example, simulate how a building will perform following planned renovation or modernisation. Their application would be particularly justified in cases where renovation is carried out on a larger scale, for instance with buildings owned or used by local self-government.

The potential use of artificial intelligence tools may also be identified on the other side of the process, namely in the control and verification of certificates by state authorities, as well as in their application and recognition by public bodies.

4. Detection of errors and fraud: Artificial intelligence could compare the data contained in certificates with the actual energy consumption of buildings or with other databases. In this way, it would be capable of processing complex datasets that are difficult for human inspection and evaluation.

5. Verification of input data: Closely related to this is the verification of data submitted by authorised persons. The Ministry of Transport of the Slovak Republic, as the

⁸ DING et al., 2024, p. 5916.

⁹ LEUTHE et al., 2024, p. 12.

supervisory authority in this field, would thereby acquire broader powers to verify the accuracy of the information entered into the central register.

6. *Central register of certificates and its supervision:* Software supported by artificial intelligence could analyse the data contained in the register (Section 9 of Act No. 555/2005 Coll.) and identify anomalies or irregularities present within it.

The use of artificial intelligence tools in this field nevertheless has its limits. AI may serve as a form of support within these processes, but not as a substitute: either for the activities of authorised entities carrying out certification, or for the supervisory and regulatory role of the state and its authorities.

In a traditional rule-based regulatory framework, individuals retain the freedom to decide whether to comply with a given rule. By contrast, in an environment shaped by algorithmic or code-based regulation, such discretion disappears. Behaviour is determined directly by the underlying programming, leaving no room for negotiation or partial compliance. This rigidity fundamentally challenges the principle of reciprocity.¹⁰

The energy performance certificate remains a public document issued by an authorised person, who assumes responsibility for it. Both public authorities and the authorised certifier continue to bear ultimate legal responsibility. This highlights the well-known difficulty present in all debates concerning the use of artificial intelligence in administrative decision-making.

As Gyurász observes, in cases where the State employs artificial intelligence systems for the purpose of enhancing the efficiency of the exercise of public authority, while continuing to act in a position of superiority within such relationships, it shall also bear liability for any damage caused by the operation of the intelligent system under Act No. 514/2003 on State Liability for the Exercise of Public Authority as amended. The situation would be different if the State were merely to allow, for instance, authorised persons to make use of artificial intelligence systems. In such circumstances, we take the view that the State would not be liable for their potential malfunction or for any damage thereby caused, rather, liability would rest with those entities themselves.¹¹

Equally, issues arise regarding the procedural rights of affected persons, whether owners, users or others. They must be granted the opportunity to understand the functioning of the algorithm and, where appropriate, to challenge its conclusions. The fact that the revised EPBD increases the significance of certificates (particularly in relation to public buildings and building passports) may in turn result in greater administrative burdens and pressure on quantity. This, however, creates difficulties

¹⁰ GREENSTEIN, 2022, p. 317.

¹¹ GYURÁSZ, 2024a, p. 123.

in ensuring the quality, transparency and reasoned justification of individual cases in which a certificate is issued and its values determined.

Considerations regarding the introduction of artificial intelligence tools may be concluded with the following assertion: the most accurate analogy for understanding the relationship between artificial intelligence-based systems and our society is to regard them as objects under the control and direction of human entities.¹²

Conclusion

The energy certification of buildings represents one of the greatest challenges currently faced by our societies and by the European Union as a whole. We would argue that it amounts to a more profound transformation than the entire shift towards electromobility and the de facto ban on the sale of cars with combustion engines. As certification is gradually extended not only to new constructions but also to all existing buildings (subject to specified exemptions), the administrative and practical demands will be considerable.

We are convinced that artificial intelligence tools will form an indispensable part of our response to these challenges. As outlined in this paper, their role concerns both the activities of authorised persons responsible for certification and the supervisory and control functions of state authorities, particularly the Ministry of Transport of the Slovak Republic.

In response to the research question posed at the outset: *to what extent may artificial intelligence be utilised within legal decision-making processes in the field of energy certification of buildings?* We may conclude that AI can serve as a valuable support mechanism, streamlining procedures and enhancing accuracy. Nevertheless, it cannot replace the legal responsibility borne by authorised certifiers and public authorities. Its contribution must therefore be understood as complementary: increasing efficiency while leaving accountability firmly within human hands.

Bibliography

1. DING, Cheng – KE, Jiali – LEVINE, Mark – et al.: Potential of artificial intelligence in reducing energy and carbon emissions of commercial buildings at scale. In: *Nature Communications*, Vol. 15 (2024), pp. 5916. ISSN 2041-1723.
2. GREENSTEIN, Stanley: Preserving the rule of law in the era of artificial intelligence (AI). In: *Artificial Intelligence and Law*, Vol. 30, No. 3 (2022), pp. 291–323. ISSN 0924-8463.

¹² GYURÁSZ, 2024b, p. 89.

3. GYURÁSZ, Z.: Zodpovednosť umelej inteligencie. In Právo a umelá inteligencia. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2024a. ISBN 978-80-7160-715-1, pp. 116-144.
4. GYURÁSZ, Zoltán: Keď umelá inteligencia robí chyby: respondeat superior. In: *Bratislavské právnické fórum 2024: právo a technológie v 21. storočí optikou európskeho práva*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta UK, 2024b, pp. 85–91. ISBN 978-80-7160-728-1 (online).
5. LEUTHE, Daniel – ZHOU, Ying – ZHANG, Wei et al.: Leveraging explainable AI for informed building retrofit decisions: Insights from a survey. In: *Energy and Buildings*, Vol. 318 (2024), pp. 114426. ISSN 0378-7788.
6. MADUTA, Carmen – VLAICU, Ana – BĂLAN, Carmen et al.: From nearly zero-energy buildings (NZEBs) to zero-emission buildings (ZEBs): current status and future perspectives. In: *Energy and Buildings*, Vol. 328 (2025), pp. 115133. ISSN 0378-7788.
7. QIU, Yueming – KAHN, Matthew E.: Impact of voluntary green certification on building energy performance. In: *Energy Economics*, Vol. 80 (2019), pp. 461–475. ISSN 0140-9883.

Contacts

JUDr. Ľudovít Máčaj, PhD.

ludovit.macaj@flaw.uniba.sk

Comenius University in Bratislava

Faculty of Law

Department of Administrative and Environmental Law

PRÁVNE ASPEKTY VYUŽÍVANIA UMELEJ INTELIGENCIE PRI ROZHODOVANÍ VO VODNOM HOSPODÁRSTVE

LEGAL ASPECTS OF USING ARTIFICIAL INTELLIGENCE IN DECISION-MAKING IN WATER MANAGEMENT

Lenka Šutaríková¹

Abstrakt: Článok sa zaoberá komplexnou analýzou právnych aspektov využívania umelej inteligencie (AI) v rozhodovacích procesoch orgánov verejnej správy v oblasti vodného hospodárstva. Vychádza z aktuálnych trendov digitalizácie verejnej správy a z postupnej implementácie inteligentných technológií do administratívnych postupov, najmä pri povoľovaní, monitorovaní, kontrole a správe vodných zdrojov. Autori poukazujú na rastúci význam automatizovaných rozhodovacích systémov a na potrebu ich právneho a etického ukotvenia v kontexte zásad dobrej správy vecí verejných. Štúdia zdôrazňuje potenciál umelej inteligencie z hľadiska zvýšenia efektívnosti, objektívnosti, konzistentnosti a transparentnosti rozhodovania, zároveň však identifikuje významné riziká spojené s jej aplikáciou, najmä v súvislosti so ochranou osobných údajov, kybernetickou bezpečnosťou a otázkou zodpovednosti za rozhodnutia prijaté s využitím algoritmických systémov. Osobitný dôraz sa kladie na zásady vysvetliteľnosti a kontrolovateľnosti algoritmických procesov, ktoré sú nevyhnutné pre zachovanie princípov právnej istoty a dôvery verejnosti v činnosť orgánov verejnej moci. Analýza vychádza z relevantnej slovenskej a európskej legislatívy, osobitne z pripravovaného Aktu o umelej inteligencii (AI Act) a jeho dopadov na národnú právnu úpravu. Záver článku obsahuje návrhy de lege ferenda smerujúce k vytvoreniu koherentného, efektívneho a právne predvídateľného rámca pre bezpečné, transparentné a zákonné využívanie umelej inteligencie pri správe vodných zdrojov.

Kľúčové slová: umelá inteligencia, rozhodovanie vo verejnej správe, vodné hospodárstvo, ochrana údajov, digitalizácia.

Abstract: The article deals with a comprehensive analysis of the legal aspects of the use of artificial intelligence (AI) in decision-making processes of public administration bodies in the field of water management. It is based on current

¹ Univerzita Komenského v Bratislave, Právnická fakulta.

trends in the digitalization of public administration and the gradual implementation of intelligent technologies into administrative procedures, especially in permitting, monitoring, control and management of water resources. The authors point to the growing importance of automated decision-making systems and the need for their legal and ethical anchoring in the context of the principles of good governance. The study emphasizes the potential of artificial intelligence in terms of increasing the efficiency, objectivity, consistency and transparency of decision-making, but at the same time identifies significant risks associated with its application, especially in connection with the protection of personal data, cybersecurity and the issue of liability for decisions made using algorithmic systems. Special emphasis is placed on the principles of explainability and controllability of algorithmic processes, which are essential for maintaining the principles of legal certainty and public trust in the activities of public authorities. The analysis is based on relevant Slovak and European legislation, in particular the upcoming Artificial Intelligence Act (AI Act) and its impacts on national legislation. The article concludes with *de lege ferenda* proposals aimed at creating a coherent, effective and legally predictable framework for the safe, transparent and lawful use of artificial intelligence in water resources management.

Key words: artificial intelligence, decision-making in public administration, water management, data protection, digitalization.

Úvod

Cieľom tohto článku je analyzovať potenciál umelej inteligencie v oblasti správy vodných zdrojov, identifikovať právne limity jej využívania a navrhnúť kroky, ktoré by umožnili jej zodpovedné a transparentné nasadenie do rozhodovacích procesov orgánov verejnej správy.

Rozvoj informačných technológií a digitalizácie predstavuje jednu z najzásadnejších zmien v činnosti orgánov verejnej správy na Slovensku. V posledných rokoch sa osobitná pozornosť venuje využívaniu umelej inteligencie, ktorá ponúka nástroje na efektívnejšie spracovanie dát, modelovanie zložitých javov a podporu rozhodovacích procesov. V oblasti vodného hospodárstva môže umelá inteligencia priniesť výrazné zefektívnenie postupov správnych orgánov. Tu však vznikajú otázky, či právny rámec Slovenskej republiky umožňuje plnohodnotné nasadenie týchto technológií pri rozhodovaní. Zákon č. 364/2004 Z.z. o vodách (vodný zákon)² ani zákon č. 71/1967

² ZÁKON č. 364/2004 Z. z. o vodách a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon).

Zb. o správnom konaní³ neupravujú algoritmické rozhodovanie ani využívanie autonómnych nástrojov v správnom procese. Právny poriadok vychádza z predpokladu, že rozhodnutie správneho orgánu vydáva úradná osoba, ktorá zodpovedá za jeho obsah. Automatizované spracovanie podkladov alebo prípadne nahradenie časti rozhodovacieho procesu umelej inteligencie preto otvára množstvo nielen právnych ale i etických a metodických otázok.

Umelá inteligencia je rýchlo rozvíjajúca sa oblasť s potenciálom transformovať priemyselné odvetvia a náš každodenný život. Hoci existujú výzvy a etické obavy, ktoré je potreba riešiť, pokrok v technológii umelej inteligencie neustále posúva hranice toho, čo sú stroje schopné dosiahnuť. Využitím sily umelej inteligencie môžeme riešiť výzvy, ktorým čelia vodovodné a odpadové systémy, a potencionálne nás to môže priviesť na cestu kudržiateľnejšiemu a odolnejšiemu vodnému hospodárstvu.

Čo je umelá inteligencia?

Jednou z kľúčových technologických oblastí, ktorá nadobúda čoraz väčší význam, je umelá inteligencia. Nachádza uplatnenie v rôznych oblastiach spoločenského a hospodárskeho života. Umelá inteligencia predstavuje prelomový smer v informatike, ktorý sa zameriava na vývoj systémov schopných premýšľať, učiť sa a prispôbovať sa novým informáciám podobne ako ľudská myseľ. Spracúva rozsiahle množstvo údajov a používa pokročilé algoritmy na identifikáciu vzorov a vzťahov v analyzovaných dátach.⁴ Umelá inteligencia je oblasť informatiky zameraná na vytváranie systémov schopných vykonávať úlohy, ktoré by za normálnych okolností vyžadovali ľudskú inteligenciu. Zahŕňa vytváranie algoritmov, ktoré umožňujú systémom analyzovať a interpretovať obrovské množstvo údajov. Tieto algoritmy potom umožňujú počítačovým systémom napodobňovať aspekty ľudského myslenia, čo umožňuje strojom replikovať úlohy, ako je učenie, plánovanie, riešenie problémov a rozhodovanie.⁵ Hoci je umelá inteligencia stále rozvíjajúcou sa oblasťou, má potenciál poskytnúť významnú podporu v rôznych aplikáciách. Jedinečné schopnosti umelej inteligencie však vyvolávajú otázky o tom, ako ovplyvní

³ ZÁKON č. 71/1967 Zb. o správnom konaní (správny poriadok).

⁴ STAŠÍKOVÁ, A. 2023. Čo je umelá inteligencia (AI) a ako ju využiť vo svoj prospech. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.goodrequest.com/sk/blog/co-je-umela-inteligencia-ai-a-ako-ju-vyuzit-vo-svoj-prospech>.

⁵ EURÓPSKY PARLAMENT. Umelá inteligencia: definícia a využitie. [online]. [cit. 15.9.2025]. Dostupné z: <https://efcnetwork.org/ai-in-water-management-six-ways-artificial-intelligence-can-help-solve-problems-across-the-water-sector/>

rozdelenie práce a úloh medzi ľuďmi a strojmi, a tieto otázky sa čoraz viac skúmajú.⁶ Na umelú inteligenciu možno nazerať ako na nástroj relevantných informácií na realizáciu určitého rozhodnutia.⁷

Napriek skutočnosti, že umelá inteligencia so sebou prináša značné množstvo výhod, právny poriadok SR nie je na zmeny s ňou súvisiace pripravený. Vzniká tu otázka právnej subjektivity – spôsobilosť mať práva a povinnosti (de facto aj spôsobilosť na právne úkony). V zmysle slovenského právneho poriadku vzniká spôsobilosť mať práva a povinnosti u fyzických osôb narodením, pričom túto spôsobilosť majú aj právnické osoby.⁸ Vzniká však otázka, ako v uvedených intenciách vnímať umelú inteligenciu, ktorá sa postupnými krokmi blíži niektorým kognitívnym schopnostiam typickým pre človeka.⁹ Je zrejmé, že podľa platnej právnej úpravy nie je umelá inteligencia subjektom práva, nositeľom práv a povinností a tiež nie je spôsobilá realizovať právne úkony. Možno ju považovať za akúsi *sui generis* entitu, ktorá z hľadiska právnej subjektivity nie je regulovaná. Na základe uvedeného možno vyvodiť pomerne logický záver – umelá inteligencia nie je subjektom práva, a teda nemôže byť ani členom štatutárneho orgánu a nemôže autonómne prijímať rozhodnutia, prípadne inak zasahovať do rozhodovacieho procesu štatutárnych orgánov.¹⁰

Umelá inteligencia je informatická vedná disciplína, ktorá hojne využíva poznatky z iných vedných oblastí. Jednou z úloh, ktoré si umelá inteligencia kladie, je prinútiť stroje k tomu, aby ich správanie pripomínalo inteligentné správanie človeka.¹¹

Cieľom umelej inteligencie je vytvoriť, zostrojiť inteligentné objekty a porozumieť im. Metóda umelej inteligencie je vo svojej podstate spätá s použitím výpočtových

⁶ The 8th International Conference of Euro Asia Civil Engineering Forum 2022, IOP Publishing, IOP Conf. Series: Earth and Environmental Science. [online]. [cit. 15.9.2025]. Dostupné z: <https://iopscience.iop.org/article/10.1088/1755-1315/1195/1/012056/pdf>

⁷ SOKOL, M. Podstata, význam a právna subjektivita umelej inteligencie. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.) Právo – Obchod – Ekonomika XII. Zborník vedeckých prác. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2023, s. 78.

⁸ Ustanovenie § 7 ods. 1 a § 18 ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník, v znení neskorších predpisov.

⁹ SOKOL, M. Podstata, význam a právna subjektivita umelej inteligencie. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.) Právo – Obchod – Ekonomika XII. Zborník vedeckých prác. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2023, s. 344-353.

¹⁰ SOKOL, M. Digitalizácia a umelá inteligencia v obchodných spoločnostiach. 1. vydanie. Bratislava: C. H. Beck, 2024, s. 82-83., 2023, s. 82.

¹¹ KVASNIČKA, V., POSPÍCHAL, J., NÁVRAT, P., LACKO, P., TREBATICKÝ, P. Umelá inteligencia a kognitívna veda II. Edícia výskumných textov informatiky a informačných technológií. Bratislava: Slovenská technická univerzita v Bratislave, 2010, s. 376.

procesov. O definíciu toho, čo je to umelá inteligencia, sa pokúša skoro každá monografia alebo učebnica o nej. Vyšlo ich desiatky a definície v nich sa rôznia.¹²

Jednou z častých výhrad voči umelej inteligencii je, že stroje sa len ťažko môžu považovať za inteligentné, pokiaľ sa nedokážu naučiť nové vedomosti a prispôbiť sa novým situáciám.¹³

Systémy umelej inteligencie čoraz viac prenikajú aj do oblasti etiky. Tu je takisto nevyhnutná participácia človeka, ale keďže ani ľudia nie sú jednotní v etických otázkach, je potrebné premyslieť si taký systém rozhodovania, ktorý by zohľadňoval záujmy čo najväčšieho počtu jednotlivcov, ktorých sa tieto rozhodnutia dotknú. Umelá inteligencia produkuje obsah, vytvára umenie a šíri ho v oveľa väčšom rozsahu, ako by sme to dokázali sami. Algoritmy poháňané umelou inteligenciou však pracujú ako čierna skrinka a niekedy sú procesy rozhodovania v umelej inteligencii aj pred jej tvorcami.

Prediktívna schopnosť umelej inteligencie je veľmi žiadaná, napriek jej netransparentnosti a nezodpovednosti. Situácia je znepokojujúca, keďže v prípade ľudskej chyby sa možno sťažovať na človeka, ktorý sa pomýli. Ale koho viniť v prípade zlyhania alebo zaujatosti softvéru? Umelá inteligencia sa pomaly, potichu a isto dostáva do našich životov a rozhodovacích procesov.¹⁴

Verejná správa a vodné hospodárstvo

Verejná správa je ústredným pojmom správneho práva. Zabezpečuje realizáciu verejnej moci ako súčasť moci výkonnej. Snahy definovať pojem verejnej správy neboli doposiaľ uspokojivo naplnené a jej početné definície sa odvíjajú od rôznych čiastočne odlišných poňatí verejnej správy. Napriek tomu, že právna úprava ani legislatíva neponúkajú definíciu verejnej správy, často tento pojem používajú. Pojem verejná správa nájdeme v čl. 46 Ústavy Slovenskej republiky a vo viacerých právnych predpisoch.¹⁵ Verejná správa je vo svojej podstate komplex prvkov verejnej správy, ich vzťahov a vzájomných štruktúr.

¹² NÁVRAT, P., BIELIKOVÁ, M., BEŇUŠKOVÁ, Ľ., KAPUSTÍK, I., UNGER, M. Umelá inteligencia. Bratislava: Slovenská technická univerzita v Bratislave, 2002, s. 2-3.

¹³ NÁVRAT, P., BIELIKOVÁ, M., BEŇUŠKOVÁ, Ľ., KAPUSTÍK, I., UNGER, M. Umelá inteligencia. Bratislava: Slovenská technická univerzita v Bratislave, 2002, s. 141.

¹⁴ ŠNURENKO, I., MUROVANÁ, T., KUŠČU, I. Človek a umelá inteligencia. Problémy tela, slobody a kritického myslenia. Kežmarok: Vydavateľstvo TORDEN, 2023. s. 28, 76-77.

¹⁵ VRABKO, M. a kol., Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2018. s. 3-4.

Zo správnoprávneho pohľadu väčšina interpretácii pod verejnou správou rozumie správu verejných záležitostí, realizovanú ako prejav výkonnej moci v štátne. Verejnú správu vykonávajú konkrétne určené inštitúcie, t. j. orgány verejnej správy.¹⁶

Verejnú správu treba odlišovať od súkromnej správy. Verejná správa, ako správa verejných záležitostí, je správou vo verejnom záujme a subjekty, ktoré ju vykonávajú, realizujú ju ako právom uloženú povinnosť, a to zo svojho právneho postavenia verejnoprávných subjektov.¹⁷

Vodné hospodárstvo je súčasťou verejnej správy, a to aj z dôvodu lebo hospodárenie s vodnými zdrojmi má charakter verejného záujmu¹⁸. Voda je strategická surovina, bez ktorej nemôže fungovať spoločnosť ani ekonomika, a na základe toho nemôže štát nechať jej správu len na súkromný sektor.

Umelej inteligencii patrí dôležité miesto v modernizácii verejnej správy, pričom vo vodnom hospodárstve by mohla umožniť efektívnejšie riadenie a ochranu zdrojov. Verejná správa v oblasti vodného hospodárstva spracúva obrovské množstvo údajov, od hydrologických meraní cez evidenciu povolení na odber vôd, až po dáta o znečistení a environmentálnych záťažoch. Umelá inteligencia môže zefektívniť aj samotné správne konanie. Automatizované nástroje dokážu vyhodnotiť splnenie základných formálnych náležitostí, identifikovať kolízie s existujúcimi právami a upozorniť úradníkov na neštandardné prípady, ktoré si vyžadujú osobitnú pozornosť. Tým sa znižuje administratívna záťaž a urýchľuje sa vybavovanie agendy. Nesmie byť prehliadnuté, že umelá inteligencia má v oblasti vodného hospodárstva pomáhať rozhodovaciemu procesu¹⁹, nie ho plne nahrádzať.

Prečo umelá inteligencia vo vodnom hospodárstve

Vodné hospodárstvo je neoddeliteľnou súčasťou ľudskej civilizácie od vzniku stálych sídiel a poľnohospodárskych spoločností. Pojem „vodné hospodárstvo“ sa vzťahuje na systematické plánovanie, rozvoj a optimalizáciu vodných zdrojov s cieľom riešiť potreby spoločnosti a životného prostredia. Táto oblasť je kritická kvôli zásadnej úlohe vody v ekosystémoch, poľnohospodárstve, výrobe energie a ľudských potrebách. V tejto súvislosti medzi kľúčové aspekty vodného hospodárstva patrí

¹⁶ VRABKO, M. a kol., Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012. s. 6.

¹⁷ ŠKULTÉTY, P. Verejná správa a správne právo. Bratislava: Slovenská akadémia vied, 2011. s. 16.

¹⁸ K tomu pozri bližšie napríklad VRABKO, M. a kol. Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2019. s. 7.

¹⁹ „rozhodovacie procesy“ - K tomu pozri bližšie napríklad REKEN, J. – VRABKO, M. Vybrané rozhodovacie procesy vo verejnej správe. Bratislava: Právnická fakulta Univerzity Komenského, 1999. 128. ISBN 80-7160-107-1.

úprava a distribúcia pitnej vody aj odpadových vôd, kontrola zdrojov povrchových a podzemných vôd, manažment povodňových rizík a údržba hydroekosystémov.²⁰ Umelá inteligencia postupne zasahuje všetky sféry hospodárstva. Vodný sektor samozrejme nie je výnimkou. Práve v poslednom období dlhotrvajúce suchá po celom svete pripomínajú všetkým, nielen poľnohospodárom, že nedostatok vody si vyžaduje lepšie riadené vodné hospodárstvo.

Umelá inteligencia prináša revolúciu v hospodárení s vodou tým, že umožňuje efektívnejšie a udržateľnejšie využívanie tohto kritického zdroja. Systémy umelej inteligencie dokážu analyzovať obrovské množstvo údajov z rôznych dostupných zdrojov, ako sú predpovede počasia, meracie stanice, satelitné snímky a senzory, s cieľom optimalizovať distribúciu a spotrebu vody. Napríklad v oblasti hospodárenia s vodou dokážu modely riadené umelou inteligenciou lepšie predpovedať presné potreby vody používateľov, čo umožňuje prevádzkovateľom priehrad optimálnejšie alokovať vodné zdroje. Umelá inteligencia môže navyše pomôcť odhaliť únik v mestských vodovodných systémoch analýzou údajov o tlaku a prietoku v reálnom čase, čo umožňuje rýchlejšie opravy a znižuje straty vody.

Okrem hospodárenia s vodou môže umelá inteligencia zohrávať kľúčovú úlohu aj pri zabezpečovaní kvality vody. Monitorovať kvalitu vody analýzou údajov zo senzorov, ktoré detegujú znečisťujúce látky, chemikálie a iné kontaminanty vo vodných zdrojoch čo umožňuje včasné odhalenie problémov s kvalitou vody a pomáha predchádzať krízam v oblasti verejného zdravia. Umelá inteligencia bude tiež zohrávať kľúčovú úlohu pri podpore znižovania rizika katastrof zlepšením analýzy údajov, zlepšením prognóz na základe dopadov a tým podporou lepšej pripravenosti a reakcie na riziká súvisiace s vodou.²¹

Tieto údaje sú rozptýlené medzi viaceré orgány štátnej a verejnej správy a často spracúvané manuálne alebo prostredníctvom čiastočne digitalizovaných systémov. Umelá inteligencia umožňuje vytvárať integrované platformy, ktoré dokážu tieto informácie spracovať rýchlejšie a efektívnejšie.

Jednou z kľúčových možností je prediktívna analýza. Algoritmy dokážu na základe historických údajov a aktuálnych meraní predpovedať suché obdobia, povodňové riziká alebo zhoršenie kvality vôd. Tieto predikcie môžu správnym orgánom poskytnúť cenné podklady na prijímanie preventívnych opatrení, či pri povoľovaní nových vodných odberov.

Technológie umelej inteligencie prostredníctvom prediktívnej analytiky, inteligentného merania a monitorovania v reálnom čase optimalizovať hospodárenie

²⁰ Applications of AI for water management. 2025. s. 16. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>. ISBN 978-92-3-100753-8.

²¹ Applications of AI for water management. 2025. s. 8. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>.

s vodnými zdrojmi, zlepšiť prístup k nim a ich distribúciu. Niekoľko miliónov ľudí nemá bezpečne spravovaný prístup k vodným zdrojom. Systémy založené na umelej inteligencii by mohli túto medzeru riešiť predpovedaním nedostatku vody, identifikáciou únikov a zlepšením distribučných sietí. Implementáciou týchto technológií však musia riadiť etické aspekty, aby sa zabránilo prehľbovaniu nerovnosti. Marginalizované komunity tak čelia digitálnym rozdielom, ktoré by mohli brániť ich schopnosti využívať pokroky umelej inteligencie.²²

Hoci technológie umelej inteligencie majú potenciál odomknúť nové možnosti v kontexte vodného hospodárstva, tento vývoj čelí aj niekoľkým obmedzeniam. Napríklad metódy založené na dátach často vyžadujú prístup k rozsiahlym (priestorovým a časovým) a vysokokvalitným meraniam, ktoré niekedy neprezentujú extrémne hodnoty (ktoré majú pre vodné hospodárstvo zásadný význam).²³

Významným prínosom je aj kontinuálny monitoring. Sieť senzorov prepojená s algoritmami dokáže v reálnom čase sledovať dodržiavanie povolených odberov, či vypúšťanie odpadových vôd. Porušenia limitov môžu byť okamžite nahlásené príslušnému orgánu, čím sa zvyšuje efektívnosť výkonu štátneho dozoru.

Napriek týmto možnostiam nesmie byť prehliadnuté, že umelá inteligencia má v oblasti vodného hospodárstva pomáhať rozhodovaciemu procesu, nie ho plne nahrádzať.

Životné prostredie

Umelá inteligencia sa ukazuje ako dôležitý nástroj pri monitorovaní životného prostredia s víziou zvýšenia objektivity a efektivity. Je prínosná pri predpovediach prírodných katastrof (požiarov, zemetrasení či hurikánov), pri monitoringoch kvality vody a ovzdušia, či odhaľovaní znečisťujúcich látok.²⁴

Nárast populácie, zvýšené požiadavky na množstvo pitnej vody, nepostačujúce tradičné spôsoby čistenia odpadových vôd z hľadiska spotreby energie aj nákladovej neúčinnosti, sú dôvodom implementácie umelej inteligencie aj vo vodnom hospodárstve. Často je využívaná pri optimalizovaní fáz čistenia odpadových vôd,

²² Applications of AI for water management. 2025. s. 84. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>.

²³ Applications of AI for water management. 2025. s. 23. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>.

²⁴ OLAWADE, D. a kol., 2024. Artificial intelligence in environmental monitoring: Advancements, challenges, and future directions. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2773049224000278>.

ako napríklad pri detekcii rôznych látok prítomných vo vode, pri riadení procesov, zlepšovaní prevádzky či znižovaní záťaže pre životné prostredie.²⁵

Nezanedbateľnú úlohu zohráva umelá inteligencia aj pri monitoringu ovzdušia a predpovediach koncentrácie znečisťujúcich látok v ovzduší. Umožňuje skúmať ohniská znečistenia, identifikovať úroveň znečistenia či predpovedať vplyv meteorologických faktorov. Na základe toho je možné prijímať účinné rozhodnutia pri riadení kvality ovzdušia a ochrany verejného zdravia.²⁶

Technológie umelej inteligencie môžu zlepšiť starostlivosť o životné prostredie vo vodnom hospodárstve rôznymi spôsobmi. Prediktívna analýza dokáže predpovedať dopyt a ponuku vody, čo umožňuje efektívnejšie pridelovanie zdrojov a znižuje zaťaženie vodných útvarov. Umelá inteligencia môže zlepšiť presnosť hydrologických modelov, čo vedie k lepším predpovediam dostupnosti a kvality vody. To podporuje udržateľné hospodárenie s vodnými zdrojmi a zabezpečuje, aby ekosystémy dostávali dostatočné množstvo vody na udržanie svojho zdravia a biodiverzity.²⁷ Hoci umelá inteligencia môže zlepšiť monitorovanie životného prostredia, je nevyhnutné aby zavádzanie technologických riešení nenarúšalo prirodzené biotopy ani neviedlo k ekologickej nerovnováhe.

Riziká a právne limity algoritmického rozhodovania

Umelá inteligencia by mohla slúžiť na vytvorenie nových globálnych príležitostí. V čoraz búrlivejšom svete, v ktorom existujeme ako globálne spoločenstvo, však všadeprítomné a niekedy nekritické zavádzanie umelej inteligencie vytvára nové neistoty a riziká.²⁸ Nasadenie umelej inteligencie v rozhodovacích procesoch prináša riziká, ktoré si vyžadujú právnu úpravu a metodické usmernenia. Prvým zásadným problémom je netransparentnosť algoritmov. Ak systém nedokáže vysvetliť, ako k odporúčeniu dospel, môže to narušiť preskúmateľnosť rozhodnutí v správnom súdnictve.

Ďalšou výzvou je otázka zodpovednosti za škodu. Ak nesprávne rozhodnutie spôsobené algoritmom poškodí úradníka, neexistuje jasné pravidlo, kto nesie zodpovednosť, či štát, dodávateľ softvéru alebo konkrétny úradník. To je obzvlášť

²⁵ BAARIMAH, A. a kol., 2024. Artificial intelligence in wastewater treatment: Research trends and future perspectives through bibliometric analysis. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2666016424003207>.

²⁶ CHADALAVADA, S. a kol., 2025. Application of artificial intelligence in air pollution monitoring and forecasting: A systematic review. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1364815224003736>.

²⁷ Applications of AI for water management. 2025. s. 85. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>.

²⁸ ŠNURENKO, I., MUROVANÁ, T., KUŠČU, I. Človek a umelá inteligencia. Problémy tela, slobody a kritického myslenia. Kežmarok: Vydavateľstvo TORDEN, 2023. s.

citlivé v oblasti vodného hospodárstva, kde rozhodnutia môžu mať priame environmentálne a hospodárske dôsledky.

Riziko predstavuje aj spracovanie osobných údajov a citlivých informácií.

Systémy umelej inteligencie sú často prirovnávané k čiernym skrinkám, hoci sú starostlivo navrhnuté a majú vnútorné systémové procesy založené na digitálnych výpočtoch. Obrovské objemy toku dát, ktoré spracúvajú však majú rôznorodý pôvod a štruktúru. Na základe týchto údajov systémy AI vytvárajú úsudky, korigujú vlastné správanie ako sprostredkovatelia a ovládajú svoje nástroje riadiacich objektov atď.. Kvôli všetkým týmto premenným sa ich fungovanie nedá vyjadriť pevným algoritmom, a teda ani vysvetliť.

Súčasná legislatíva Slovenskej republiky neobsahuje osobitné ustanovenia pre algoritmické rozhodovanie vo verejnej správe. Hoci zákon o e-Governmente²⁹ podporuje elektronizáciu agendy, nešpecifikuje pravidlá pre autonómne rozhodovanie v citlivých sektoroch, akým je ochrana vodných zdrojov.

Umelá inteligencia sa stáva súčasťou našich životov viac ako nikdy predtým v takej miere, o akej sa nám ani nesníva. Tento trend so sebou prináša nové výzvy v oblasti mediálnej a informačnej gramotnosti. So všetkými pozitívami, ktoré vznik umelej inteligencie sprevádzajú, prichádzajú ruka v ruke aj riziká, o ktorých sa až tak nehovorí. Sú to najmä vplyv na rozhodovacie a kontrolné systémy a dehumanizácia riadenia spoločnosti. Súčasne hrozí nebezpečenstvo, že o ľudských činnostiach začnú rozhodovať stroje, ktoré nemajú žiadnu empatiu, súcitiť, morálku ani charakter.³⁰ Umelá inteligencia je už totiž latentne prítomná vo všetkých oblastiach života v podobe rôznych menších rozhodovacích procesov. Niektoré aplikácie, tvoriace základ tejto umelej inteligencie, už dnes využívajú informácie získané napríklad z pokročilých webových vyhľadávačov, systémov odpočúvania, porozumeniu ľudskej reči, alebo autonómne riadiacich systémov automobilov.

V súčasnosti sme svedkami rozsiahleho nasadzovania systémov umelej inteligencie do praxe, pričom nejde len o širokospektrálne využitie v oblasti vedy a výskumu, resp. v niektorých strategických oblastiach, ale aj o bežné používanie v spotrebnej elektronike a v systémoch, ktoré sú súčasťou nášho každodenného života.³¹

Je evidentné, že umelá inteligencia má vo veľkej miere prínos pre spoločnosť. Niektoré prínosy už pociťujeme v súčasnom období, iné prinesie budúcnosť. V spojitosti s umelou inteligenciou sa často stretávame s otázkou, či príde k potenciálnemu nahradeniu človeka pri výkone vybraných povolání, prípadne

²⁹ ZÁKON č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).

³⁰ ŠNURENKO, I., MUROVANÁ, T., KUŠČU, I. Človek a umelá inteligencia. Problémy tela, slobody a kritického myslenia. Kežmarok: Vydavateľstvo TORDEN, 2023. s. 240.

³¹ ŠANTAVÝ, P. Umelá inteligencia – dobrý sluha a zlý pán? Ľudia, stroje, spoločnosť ... Etika, hodnoty, budúcnosť ... Bratislava: Univerzita Komenského v Bratislave, 2022. s. 55.

k zániku pracovných miest pre určité profesie? Jednoznačnú odpoveď na to momentálne nemáme. Je všeobecne známe a možno aj zaužívané slovným tradovaním, že to, čo môže predstavovať pre spoločnosť prínos, môže k strate zamestnania, zániku pracovnej pozície, zneužitiu získaných informácií alebo osobných údajov, zásahu do súkromia, ohrozeniu ľudských práv a právneho štátu.

Akt o umelej inteligencii

Akt Európskej únie o AI je prvý zákon na svete o umele inteligencií. Jeho cieľom je zabezpečiť, aby boli systémy umelej inteligencie bezpečné, etické a dôveryhodné. Zákomom sa riešia riziká spojené s umelou inteligenciou, ako je skreslenie, diskriminácia a nedostatky v oblasti zodpovednosti, podporuje sa ním inovácia a zavádzanie umelej inteligencie. Keďže ide o prvý svetový právny predpis upravujúci umelú inteligenciu, pravidlami EÚ by sa mohla stanoviť globálna norma podporujúca etickú, bezpečnú a dôveryhodnú umelú inteligenciu na celom svete, ako to bolo v prípade všeobecného nariadenia o ochrane údajov (GDPR). Aktom o umelej inteligencii sa posilní nielen účinné presadzovanie platných právnych predpisov v oblasti základných práv a bezpečnosti. Jeho cieľom je tiež podporiť investície a inovácie v oblasti umelej inteligencie v celej EÚ a uľahčiť rozvoj jednotného trhu s aplikáciami umelej inteligencie. Akt o umelej inteligencii, ktorý by mal komplexne riešiť bezpečnostné otázky súvisiace s uvádzaním a využívaním umelej inteligencie.³² Akt EÚ o umelej inteligencii je významným krokom, ktorý má za cieľ stať sa celosvetovým štandardom pre reguláciu AI, podobne ako sa GDPR stalo vzorom pre ochranu údajov.

Na umelú inteligenciu možno v prvom rade nazerať ako na nástroj zberu relevantných informácií na realizáciu určitého rozhodnutia. Úlohou umelej inteligencie by teda bolo striktne iba získavanie konkrétnej skupiny dát na základe človekom vopred stanovených kritérií, pričom so sumou získaných dát by pracoval výlučne človek. Napriek skutočnosti, že umelá inteligencia so sebou prináša značné množstvo výhod a je spôsobilá pozitívnym spôsobom ovplyvniť fungovanie obchodných spoločností, je zrejmé, že právny poriadok SR nie je na zmeny s ňou súvisiace pripravený. Je na mieste uvedomenie si skutočnosti, že technológie sa vyvíjajú podstatne rýchlejšim spôsobom, než akým je na ne schopný reagovať právny poriadok. Podľa Sokola je jedným zo základných problémov ingerencie umelej inteligencie v rozhodovacích procesoch obchodnej spoločnosti kompozícia štatutárneho orgánu a otázka právnej subjektivity – spôsobilosti mať práva a povinnosti. V zmysle slovenského právneho poriadku vzniká spôsobilosť mať práva

³² EURÓPSKA RADA, RADA EURÓPSKEJ ÚNIE. Akt o umelej inteligencii. [online]. [cit. 15.9.2025]. Dostupné z: <http://www.consilium.europa.eu/sk/policies/artificial-intelligence/>

a povinnosti u fyzických osôb narodením, pričom túto spôsobilosť majú aj právnické osoby.³³

Výzvy pri implementácii umelej inteligencie

Implementácia umelej inteligencie v správnych procesoch si vyžaduje nielen legislatívne, ale aj etické opatrenia. Rozhodnutia, ktoré majú právne účinky voči občanom alebo podnikateľom, musia zostať pod ľudskou kontrolou. V opačnom prípade môže dôjsť k narušeniu legality a oslabeniu právnej istoty.

Transparentnosť algoritmov je nevyhnutná, aby bolo možné spätne posúdiť, prečo systém odporučil konkrétny postup. Len tak možno zabezpečiť, aby bolo rozhodovanie predvídateľné, kontrolovateľné a v súlade s princípmi právneho štátu. Okrem toho závislosť umelej inteligencie od údajov vyvoláva obavy o súkromie a bezpečnosť údajov. Zber a využívanie obrovského množstva údajov na optimalizáciu hospodárenia s vodou musí dodržiavať zásady transparentnosti, súhlasu a ochrany pred zneužitím. Ako zdôrazňuje všeobecné nariadenie Európskej únie o ochrane údajov³⁴ (Európsky parlament a Rada Európskej únie, 2018), postupy nakladania s údajmi musia uprednostňovať práva a slobody jednotlivcov a zabezpečiť aby hospodárenie s vodou založené na údajoch rešpektovalo súkromie a súhlas používateľov. Zákon EU o umelej inteligencii navyše stanovil spoločný rámec pre používanie a dodávky systémov umelej inteligencie podľa klasifikačného systému založeného na „prístupe založenom na riziku“. V závislosti od rizík súvisiacich s bezpečnosťou ľudí a základnými právami môžu byť systémy umelej inteligencie zakázané alebo podliehať súboru požiadaviek a povinností na získanie prístupu na trhy EÚ. Aj systémy umelej inteligencie s obmedzenými rizikami ale nedostatkom transparentnosti budú podliehať požiadavkám na informácie a transparentnosť (Európska komisia, 2024). Aplikácie umelej inteligencie zahŕňajúce rozhodovanie v oblasti kritickej infraštruktúry alebo prístup k základným službám možno zaradiť do kategórie vysoko rizikových systémov. Tieto systémy preto môžu podliehať požiadavkám na audit, ktoré zahŕňajú riadenie rizík, správu a kvalitu údajov, registráciu a posudzovanie zhody tretími stranami.

Záver

Umelej inteligencii patrí perspektívna úloha v budúcnosti správy vodných zdrojov. Slovenská právna úprava zatiaľ neobsahuje pravidlá pre algoritmické rozhodovanie, čo môže viesť k právnej neistote. Preto je nevyhnutné vytvoriť jasný právny rámec,

³³ Ustanovenie § 7 ods. 1 a 18 ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník.

³⁴ VŠEOBECNÉ NARIADENIE O OCHRANE ÚDAJOV (GDPR). An official EU website. [online] . [cit. 15.9.2025]. Dostupné z: <https://eur-lex.europa.eu/SK/legal-content/summary/general-data-protection-regulation-gdpr.html>.

ktorý stanoví napríklad povinnosť ľudskej kontroly nad rozhodnutiami, osobitný režim zodpovednosti za škody, štandardy transparentnosti algoritmov a prísne bezpečnostné opatrenia na ochranu údajov.

Využívanie umelej inteligencie pri rozhodovaní vo vodnom hospodárstve predstavuje významnú príležitosť na zrýchlenie administratívnych procesov, zvýšenie efektivity výkonu štátneho dozoru a zlepšenie prediktívneho riadenia vodných zdrojov. Súčasný právny rámec však neposkytuje dostatočné záruky pre bezpečné a transparentné nasadenie týchto technológií.

Digitalizácia právnej regulácie vodných zdrojov v Slovenskej republike predstavuje výrazný krok smerom k transparentnejšiemu a efektívnejšiemu výkonu verejnej správy. Zavádzanie elektronických nástrojov umožnilo zrýchlenie povolovacích a kontrolných procesov, zlepšilo dostupnosť údajov a podporilo implementáciu európskych environmentálnych štandardov. Zároveň však odhalilo nové riziká, ktoré nie sú v súčasnosti dostatočne riešené legislatívou ani aplikačnou praxou.

Problémy vznikajú najmä pri zabezpečení rovného prístupu účastníkov konania k elektronickým službám štátu, pri ochrane citlivých údajov o vodných zdrojoch a pri zabezpečení kybernetickej odolnosti informačných systémov. Digitalizácia navyše otvára otázku, či je možné zachovať individuálne posúdenie každého prípadu, ak sa časť rozhodovacej agendy prenáša na automatizované systémy. Absencia záväznej metodiky pre orgány štátnej správy a nejednotná prax pri elektronickej autorizácii podaní vyvolávajú neistotu a môžu viesť k narušeniu princípu právnej istoty.

Z uvedených dôvodov je nevyhnutné prijať viaceré legislatívne opatrenia *de lege ferenda*. Slovenský zákonodarca by mal výslovne stanoviť, že rozhodnutia o povoľovaní využívania vodných zdrojov musia byť vždy podrobené ľudskej kontrole. Rovnako je potrebné vytvoriť záväznú metodiku, ktorá zabezpečí rovnaké podmienky pre všetkých účastníkov konania vrátane subjektov s nižšími digitálnymi zručnosťami. Kľúčové je aj posilnenie kybernetickej bezpečnosti vodohospodárskych informačných systémov prostredníctvom pravidelných bezpečnostných auditov a zavedenia technických štandardov, ktoré zodpovedajú významu hospodárskej infraštruktúry ako súčasti kritickej infraštruktúry štátu. Napokon, legislatíva by mala presne rozlíšiť, ktoré údaje o vodných zdrojoch majú byť verejne prístupné, a ktoré si vzhľadom na svoju povahu vyžadujú obmedzený režim sprístupňovania.

Takéto opatrenia by umožnili využiť prínosy digitalizácie bez toho, aby bola ohrozená právna istota účastníkov konania, spravodlivý prístup k vodným zdrojom či bezpečnosť kritickej vodárenskej infraštruktúry. Digitalizácia práva sa tak môže stať skutočným nástrojom udržateľného rozvoja a moderného manažmentu vodných zdrojov, ktorý bude v súlade s princípmi právneho štátu a ochranou životného prostredia,

Využívanie umelej inteligencie pri rozhodovaní vo vodnom hospodárstve predstavuje významnú príležitosť na zrýchlenie administratívnych procesov, zvýšenie efektivity

výkonu štátneho dozoru a zlepšenie prediktívneho riadenia vodných zdrojov. Súčasný právny rámec však neposkytuje dostatočné záruky pre bezpečné a transparentné nasadenie týchto technológií.

Využitie umelej inteligencie vo vodnom hospodárstve je veľmi dôležité, pretože umelá inteligencia pomáha optimalizovať vodné zdroje pri každodennom používaní, ako aj predvídať zmeny životného prostredia týkajúce sa vodných zdrojov. Pokroky v umelej inteligencii môžu pomôcť zachovať zásoby vody, znížiť množstvo kontaminantov, zabezpečiť spravodlivejšie rozdelenie, zlepšiť kvalitu vody a lepšie chrániť ľudí pred povodňami a suchom.

Napriek mnohým výhodám, implementácia technológii umelej inteligencie prináša aj viaceré výzvy. Medzi najvýznamnejšie patria otázky ochrany osobných údajov, bezpečnosti systémov, etiky pri automatizovanom rozhodovaní ako aj otázky zabezpečenia digitálnej dostupnosti pre všetky skupiny obyvateľstva, pričom nevyhnutným predpokladom tohto procesu je zvyšovanie úrovne digitálnej gramotnosti a posilňovanie povedomia verejnosti o možnostiach a benefitoch využívania umelej inteligencie. Ako uvádza Šnurenko a kol. vo svojej publikácii: „Určite je potrebné zvyšovať povedomie a vzdelávať ľudí, aby sme im pomohli pochopiť, ako fungujú moderné informačné a komunikačné systémy a ako s nimi zaobchádzať, konkrétne so zameraním na umelú inteligenciu.“³⁵

Zoznam použitej literatúry

1. Applications of AI for water management. 2025. s. 8. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.unesco.org/en/articles/applications-artificial-intelligence-water-management>. ISBN 978-92-3-100753-8.
2. BAARIMAH, A. a kol., 2024. Artificial intelligence in wastewater treatment: Research trends and future perspectives through bibliometric analysis. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2666016424003207>.
3. EURÓPSKA RADA, RADA EURÓPSKEJ ÚNIE. Akt o umelej inteligencii. [online]. [cit. 15.9.2025]. Dostupné z: <http://www.consilium.europa.eu/sk/policies/artificial-intelligence/>.
4. EURÓPSKY PARLAMENT. Umelá inteligencia: definícia a využitie. [online]. [cit. 15.9.2025]. Dostupné z: <https://efcnetwork.org/ai-in-water-management-six-ways-artificial-intelligence-can-help-solve-problems-across-the-water-sector/>.
5. CHADALAVADA, S. a kol., 2025. Application of artificial intelligence in air pollution monitoring and forecasting: A systematic review. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S266601642500001>.

³⁵ ŠNURENKO, I., MUROVANÁ, T., KUŠČU, I. Človek a umelá inteligencia. Problémy tela, slobody a kritického myslenia. Kežmarok: Vydavateľstvo TORDEN, 2023. s. 156.

15.9.2025].

Dostupné

z:

<https://www.sciencedirect.com/science/article/pii/S1364815224003736>.

6. KVASNIČKA, V., POSPÍCHAL, J., NÁVRAT, P., LACKO, P., TREBATICKÝ, P. Umelá inteligencia a kognitívna veda II. Edícia výskumných textov informatiky a informačných technológií. Bratislava: Slovenská technická univerzita v Bratislave, 2010, 579 s. ISBN 978-80-227-3284-0.
7. NÁVRAT, P., BIELIKOVÁ, M., BEŇUŠKOVÁ, L., KAPUSTÍK, I., UNGER, M. Umelá inteligencia. Bratislava: Slovenská technická univerzita v Bratislave, 2002, 393 s. ISBN 80-227-1645-6.
8. OLAWADE, D. a kol., 2024. Artificial intelligence in environmental monitoring: Advancements, challenges, and future directions. [online]. [cit. 15.9.2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2773049224000278>.
9. SOKOL, M. Podstata, význam a právna subjektivita umelej inteligencie. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.) Právo – Obchod – Ekonomika XII. Zborník vedeckých prác. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2023, s. 78
10. SOKOL, M. Digitalizácia a umelá inteligencia v obchodných spoločnostiach. 1. vydanie. Bratislava: C. H. Beck, 2024, 141 s. ISBN 978-80-8232-050-6.
11. ŠANTAVÝ, P. Umelá inteligencia – dobrý sluha a zlý pán? Ľudia, stroje, spoločnosť... Etika, hodnoty, budúcnosť... Bratislava: Univerzita Komenského v Bratislave, 2022. 262 s. ISBN 978-80-88696-83-4.
12. ŠKULTÉTY, P. Verejná správa a správne právo. Bratislava: Slovenská akadémia vied, 2011. 142 s. ISBN 978-80-224-1203-2.
13. ŠNURENKO, I., MUROVANÁ, T., KUŠČU, I. Človek a umelá inteligencia. Problémy tela, slobody a kritického myslenia. Kežmarok: Vydavateľstvo TORDEN, 2023. 239 s. ISBN 978-80-8223-138-3.
14. The 8th International Conference of Euro Asia Civil Engineering Forum 2022, IOP Publishing, IOP Conf. Series: Earth and Environmental Science. [online]. [cit. 15.9.2025]. Dostupné z: <https://iopscience.iop.org/article/10.1088/1755-1315/1195/1/012056/pdf>.
15. Ustanovenie § 7 ods. 1 a § 18 ods. 1 Občiansky zákonník
16. VRABKO, M. a kol., Správne právo hmotné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2018. s. 338. ISBN 978-80-89603-68-8.
17. VRABKO, M. a kol., Správne právo procesné. Všeobecná časť. 2. vydanie. Bratislava: C. H. Beck, 2019. 232 s. ISBN 978-80-89603-76-3.
18. VRABKO, M. a kol., Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012. 480 s. ISBN 978-80-89603-03-9
19. VŠEOBECNÉ NARIADENIE O OCHRANE ÚDAJOV (GDPR). An official EU website. [online]. [cit. 15.9.2025]. Dostupné z: <https://eur->

lex.europa.eu/SK/legal-content/summary/general-data-protection-regulation-gdpr.html.

20. Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok).
21. Zákon č. 364/2004 Z. z. o vodách a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon).
22. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).
23. Zákon č. 40/1964 Zb. Občiansky zákonník, v znení neskorších predpisov.

Kontaktné údaje

JUDr. Mgr. Lenka Šutaríková, LL.M.

lenka.sutarikova@gmail.com

Univerzita Komenského v Bratislave, Právnická fakulta

KATEGORIZÁCIA PODNETOV V OBLASTI ŽIVOTNÉHO PROSTREDIA POMOCOU UMELEJ INTELIGENCIE – CESTA K EFEKTÍVNEJŠIEMU ROZHODOVANIU?

CATEGORIZING ENVIRONMENTAL COMPLAINTS USING ARTIFICIAL INTELLIGENCE – A PATH TO EFFECTIVE DECISION-MAKING?

Dominika Noskovičová¹

Abstrakt: Tento príspevok sa zaoberá možnosťami využitia nástrojov umelej inteligencie pri spracovaní environmentálnych podnetov, konkrétne ich kategorizáciu, určovaním stupňa naliehavosti a zabezpečením efektívneho a adresného postúpenia vecne príslušným orgánom verejnej správy. Vzhľadom na narastajúci počet podaní, ktoré upozorňujú na rôzne formy porušovania environmentálnych predpisov – od závažných zásahov do životného prostredia až po menej významné nedostatky – vzniká akútna potreba zavedenia systematického prístupu k ich triedeniu, prioritizácii a následnému spracovaniu. Hlavným cieľom príspevku je preto preskúmať možnosti aplikácie umelej inteligencie v oblasti kvalifikácie environmentálnych podnetov. Pozornosť sa zameriava predovšetkým na využitie umelej inteligencie pri identifikácii relevantných právnych aspektov, hodnotení závažnosti porušenia a pri návrhu automatizovaného postúpenia konkrétnemu orgánu štátnej správy. Príspevok súčasne analyzuje štatistické údaje o počte doručených podnetov a poukazuje na potrebu technickej a legislatívnej prípravy na ich efektívne spracovanie. Zároveň sa venuje aj širším súvislostiam zavádzania umelej inteligencie do praxe, predovšetkým otázkam právnej zodpovednosti, transparentnosti rozhodovacích procesov a ochrany osobných údajov. Príspevok tak poukazuje na potenciál, ale aj na riziká, ktoré tieto moderné nástroje prinášajú pre oblasť verejnej správy a ochrany životného prostredia.

Kľúčové slová: podnety, AI, umelá inteligencia, kategorizácia, životné prostredie

Abstract: This article deals with the possibilities of using artificial intelligence tools in the processing of environmental complaints, specifically their

¹ Právnická fakulta, Univerzita Komenského v Bratislave

categorization, determining their degree of urgency, and ensuring their effective and targeted referral to the relevant public authorities. Given the growing number of submissions reporting various forms of environmental violations—from serious environmental damage to minor shortcomings—there is an urgent need to introduce a systematic approach to sorting, prioritizing, and subsequently processing them. The main objective of this paper is therefore to explore the possibilities of applying artificial intelligence in the field of environmental complaint classification. The focus is primarily on the use of artificial intelligence in identifying relevant legal aspects, assessing the severity of violations, and proposing automated referral to a specific government authority. The paper also analyzes statistical data on the number of complaints received and points to the need for technical and legislative preparation for their effective processing. It also addresses the broader context of the implementation of artificial intelligence in practice, particularly issues of legal liability, transparency of decision-making processes, and personal data protection. The paper thus highlights both the potential and the risks that these modern tools bring to the field of public administration and environmental protection.

Key words: complaints, AI, artificial intelligence, categorizing, environment

Úvod

Ochrana životného prostredia patrí medzi kľúčové priority Slovenskej republiky, ako aj celého sveta. Aj napriek tejto skutočnosti však snaha o zachovanie zdravého životného prostredia v súčasnosti čelí viacerým výzvam. Práve v tejto súvislosti je na každom štáte, aby zabezpečil dostatočnú ochranu životného prostredia vo svojej krajine tými najlepšimi dostupnými prostriedkami. Pri ochrane životného prostredia však nie je dôležitá len prevencia, ale aj zabezpečenie efektívnych nástrojov na kontrolu dodržiavania predpisov práva životného prostredia. Vzhľadom na skutočnosť, že táto téma je celosvetovo intenzívne diskutovaná, verejnosti je viac a viac bližšia a základné povedomie o zákonom a nezákonnom konaní v tejto oblasti sa pomaly stáva takpovediac bežnou výbavou každého občana. Uvedené nepochybne súvisí s cieľom občanov chrániť životné prostredie a potrebou ohlásiť akúkoľvek nezákonnú činnosť v prípade, ak sa domnievajú, že sú takejto činnosti svedkom. Toto povedomie sa preto nesporne prejavuje aj v počte podnetov od občanov na možné porušenie environmentálnej legislatívy, či už ide o orez stromov susedom, objavenie skládky odpadu počas prechádzky, alebo vypúšťanie splaškových vôd na záhradu. Čo sa týka prešetrovania takehoto konania, môžeme za kľúčovú označiť činnosť orgánov verejnej správy, najmä inšpekčných orgánov, a teda

v našom prípade Slovenskej inšpekcie životného prostredia, ktorej úlohou je zabezpečovať efektívny výkon dohľadu nad dodržiavaním environmentálneho práva, predovšetkým prostredníctvom výkonu štátneho dozoru podľa jednotlivých zložkových predpisov. Okrem inšpekcie však tieto podania môžu prešetrovať aj iné orgány, ako napríklad okresný úrad, okresný úrad v sídle kraja, či obec.

Technologický pokrok je prítomný v každom aspekte nášho života, a ani výkon štátnej správy nie je v tomto smere výnimkou. V posledných desaťročiach čelí verejná správa rastúcim nárokom na efektivitu, transparentnosť a zodpovednosť voči verejnosti. Jednou z hlavných odpovedí na tieto výzvy je digitalizácia procesov a zavádzanie moderných informačných a komunikačných technológií do každodennej praxe orgánov verejnej moci. V bežnom živote už mnohí z nás okrem informačných systémov, webstránok či aplikácií využívajú aj umelú inteligenciu vo forme rôznych chatbotov. Tá môže byť každému z nás nápomocná nie len pri získavaní odpovedí na bežné každodenné otázky, ale aj pri rôznych odbornejších a komplikovaných činnostiach, ako napríklad analýzach dlhých textov, či veľkého množstva dát. Čo sa týka verejnej správy, môžeme badať opatrnejší prístup. Využívanie umelej inteligencie v rámci širokého spektra procesov a činností vedúcich k vydaniu rozhodnutia, môžeme aj dnes označiť za nie úplne bežné. Činnosť verejnej správy je totiž nepochybne komplikovaná, pričom zahŕňa aj využívanie veľkého množstva rôznych, často aj osobných, údajov. Preto je nevyhnutné, aby boli tieto systémy, ale aj údaje v nich obsiahnuté, dobre zabezpečené. Z tohto dôvodu často verejná správa nemá ambíciu využívať pri svojej činnosti bežne dostupné formy umelej inteligencie, ale skôr vyvinúť nové systémy personalizované pre daný orgán tak, aby táto umelá inteligencia bola schopná zjednodušiť jeho procesy a prispieť tak k rýchlejšiemu a efektívnejšiemu výkonu verejnej moci.

Cieľom tohto príspevku je preto preskúmať možnosti využívania umelej inteligencie pri kategorizácii týchto podaní, upozorňujúcich na protiprávne konanie v oblasti životného prostredia, ako aj posúdiť riziká, spojené s takouto činnosťou, týkajúce sa bezpečnosti či ochrany osobných údajov. Príspevok sa tiež venuje otázkam zodpovednosti, či transparentnosti rozhodovacích procesov, v prípade využívania takéhoto systému.

Kategorizácia podnetov – technologický rozmar alebo nevyhnutná potreba?

Je podnety vôbec potrebné prešetrovať? A už vôbec, nejako ich kategorizovať? Na tieto otázky existuje jednoznačná odpoveď. Aby sme ju však mohli nájsť, je potrebné ustáliť, čo za podnet považujeme. Právny poriadok Slovenskej republiky nám na túto otázku nedáva odpoveď. Legálna definícia podnetu v oblasti porušovania environmentálnej legislatívy neexistuje. Ak by sme ho však aj napriek tomu chceli nejakým spôsobom definovať, môžeme povedať, že ide o každé podanie fyzickej

alebo právnickej osoby, poukazujúce na možné porušenie predpisov v oblasti životného prostredia, inou fyzickou alebo právnickou osobou. V súčasnosti je možné tento podnet podať viacerými formami, či už listinne, ústne do zápisnice alebo elektronicky, ako predpokladá § 19 správneho poriadku.² Podnet je ale možné podať aj prostredníctvom e-mailu, či mobilnej aplikácie, čo robí nahlasovanie podnetov pre občanov veľmi jednoduchým a dostupným.

Prešetrovanie podnetov, vo viacerých prípadoch, vyplýva priamo z predpisov v oblasti životného prostredia, pričom často ide o jednu z činností, ktorá tvorí časť výkonu štátneho dozoru.³ V prípade zákona o ochrane prírody a krajiny tento jasne hovorí, že orgán ochrany prírody v rámci výkonu štátneho dozoru prešetrojú podozrenia alebo podnety poukazujúce na porušenie tohto zákona.⁴ Podobne je tomu aj v prípade zákona o ochrane ovzdušia⁵, ktorý v § 47 ods. 7 uvádza, že orgány dozoru sú oprávnené prešetrovať podozrenia a podnety, poukazujúce na porušovanie tohto zákona. Obdobnú úpravu nachádzame aj v zákone o prevencii a manažmente introdukcie a šírenia invázných nepôvodných druhov.⁶ Čo sa týka zákona o vodách, či zákona o odpadoch, tieto explicitne nespomínajú prešetrovanie podnetov, avšak k ich prešetrovaniu dochádza v rámci výkonu štátneho dozoru.⁷ Povinnosť prešetrovania podnetov pre orgány vykonávajúce štátny dozor je uvedená aj v zákone o integrovanej prevencii a kontrole znečisťovania, kde však zákon jasne uvádza, že na prešetrovanie podnetov je príslušná iba inšpekcia.⁸ V ostatných prípadoch je na výkon štátneho dozoru, a teda na prešetrovanie podnetu, príslušných viacero orgánov štátnej či verejnej správy, pričom môže ísť napríklad o inšpekciu, okresný úrad alebo obec.

Pre účely tohto príspevku sa ďalej zamierame na podnety, doručené Slovenskej inšpekcii životného prostredia (ďalej aj ako „inšpekcia“ alebo „SIŽP“) a okresným úradom. Inšpekcii bolo v minulom roku doručených 1431 podnetov.⁹ V roku 2023 to

² Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

³ K správnomu dozoru bližšie pozri: VRABKO, M. a kolektív: Správne právo hmotné všeobecná časť. Bratislava: C. H. Beck, 2018. s 193.

⁴ § 71 ods. 1 písm. b) zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov.

⁵ Zákon č. 14/2023 Z. z. o ochrane ovzdušia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

⁶ § 16 ods. 1 zákona č. 150/2019 Z. z. o prevencii a manažmente introdukcie a šírenia invázných nepôvodných druhov a o zmene a doplnení niektorých zákonov.

⁷ Zákon č. 346/2004 Z. z. o vodách o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon) v znení neskorších predpisov a zákon č. 79/2015 Z. z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

⁸ § 34 ods. 9 zákona č. 39/2013 Z. z. o integrovanej prevencii a kontrole znečisťovania životného prostredia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

⁹ Výročná správa Slovenskej inšpekcie životného prostredia za rok 2024.

bolo 1423 podnetov a v roku 2022 išlo o 1311 podnetov.¹⁰ Najčastejšie sa podnety týkali ochrany prírody a krajiny a odpadového hospodárstva. V prípade útvaru ochrany prírody a krajiny tvorilo prešetrovanie podnetov v roku 2023 až 85% kontrolnej činnosti, pričom, ak porovnáme tieto údaje s rokom 2013, môžeme skonštatovať, že počet podnetov vzrástol až o 300%.¹¹

Podnetov doručených jednotlivým okresným úradom bolo častokrát desaťnásobne, možno až stonásobne menej. Presný počet podnetov doručený jednotlivým okresným úradom zobrazuje tabuľka č. 1.

Okresný úrad	2024	2023	2022
Ružomberok	19	27	21
Lučenec	22	15	6
Topoľčany	46	52	41
Sabinov	22	8	8
Snina	7	6	6
Gelnica	5	5	6
Kežmarok	27	26	19
Tvrdošín	53	34	13
Michalovce	28	22	34
Myjava	14	18	18
Bardejov	2	2	9
Pezinok	18	23	22
Žarnovica	10	14	22
Turčianske Teplice	18	13	9
Banská Štiavnica	49	36	17
Prievidza	53	35	23
Ilava	9	7	10
Nitra	49	47	43
Zlaté Moravce	17	5	10
Humenné	9	10	10
Stará Ľubovňa	23	26	24
Medzilaborce	9	7	8
Senec	44	29	34
Čadca	56	54	50
Svidník	31	22	6
Námestovo	42	26	44

¹⁰ Vyhodnotenia plánu hlavný úloh jednotlivých útvarov inšpekcie za roky 2023 a 2022.

¹¹ Vyhodnotenie plánu hlavných úloh útvaru ochrany prírody a krajiny za rok 2023.

Trnava	16	12	27
Rožňava	38	61	62
Poprad	62	82	46
Medzilaborce	4	6	2
Púchov	10	3	5
Senica	6	6	4
Sobrance	6	4	5
Zvolen	59	17	42
Malacky	34	22	11
Kysucké Nové Mesto	16	25	17
Hlohovec	15	17	22
Skalica	15	19	16
Komárno	30	16	20
Detva	15	17	16
Rimavská Sobota	17	13	32
Krupina	8	5	13
Veľký Krtíš	18	10	16
Trenčín	6	3	43
Bánovce nad Bebravou	6	7	10
Šaľa	17	21	13
Levoča	20	14	12

Tabuľka č. 1

Počet podnetov, doručených jednotlivým okresným úradom v rokoch 2022, 2023 a 2024¹²

Na základe uvedeného je možné konštatovať jednoznačný nepomer medzi počtom podnetov doručených na jednotlivé okresné úrady a počtom podnetov doručených na inšpekciu, ako aj jasnú potrebu kategorizácie doručených podnetov podľa stupňa ich závažnosti.

Aj vzhľadom na skutočnosť, že inšpekcia je podľa zákona č. 525/2003 Z. z.¹³ odborným kontrolným orgánom vykonávajúcim štátny dozor vo veciach starostlivosti o životné prostredie, je zrejmé jej postavenie a kompetencia na

¹² Údaje poskytnuté okresnými úradmi. Okresné úrady, ktoré nie sú uvedené v tabuľke č. 1 zahrnuté požadované údaje neposkytli z dôvodu, že nimi nedisponujú. Považujeme za potrebné doplniť, že okresné úrady nemajú od roku 2013 povinnosť zostavovať výročnú správu okresného úradu za daný rok na základe smernice Ministerstva vnútra z 1. októbra 2013 o organizácii činnosti okresného úradu.

¹³ § 9 ods. 1 písm. a) zákona č. 525/2003 Z. z. o štátnej správe starostlivosti o životné prostredie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

prešetrovanie predovšetkým závažnejších správnych deliktov. Možnosť postúpenia podnetov, poukazujúcich na menej závažné konanie potencióálne porušujúce environmentálnu legislatívu na miestne príslušný okresný úrad, sa preto javí ako vhodné riešenie aj z hľadiska efektívnosti a hospodárnosti konania. Nie je tomu tak len z dôvodu nadmerného zaťaženia inšpekcie podnetmi, a tým spôsobeným predĺžením reakčného času na prešetrovanie daného podnetu, ale aj z logistického hľadiska, nakoľko územná pôsobnosť jednotlivých inšpektorátov je častokrát pomerne rozsiahla, a preto sa na základe skúseností z aplikačnej praxe preukazuje ako neefektívne, aby daný podnet prešetroval inšpektor, ktorý musí do tejto oblasti vycestovať, namiesto zamestnanca príslušného okresného úradu, ktorý je, takpovediac, priamo na mieste.

Potreba určitej diferenciacie medzi dôležitejšími a „menej dôležitými úlohami“ inšpekcie vyplýva aj z odporúčania Európskeho parlamentu a Rady č. 2001/331/ES¹⁴, ktoré poukazuje na dôležitosť vykonávania takzvanej analýzy rizík, ktorá by mala jasne a presne stanoviť priority jednotlivých útvarov v rámci inšpekčnej činnosti, teda najmä výkon systematických kontrol vo veľkých priemyselných podnikoch, ktoré majú najväčší potenciál znečistenia životného prostredia.

Riešením tohto problému malo byť zavedenie Komplexného systému environmentálneho dohľadu (KSED). KSED je informačný systém, prevádzkovaný inšpekciou, ako orgánom štátnej správy. Vzhľadom na túto skutočnosť sa na neho vzťahujú špecifické požiadavky, ustanovené v zákone č. 95/2019 Z. z., ako aj v zákone č. 305/2013 Z. z.¹⁵ Práve tento právny predpis tvorí základ pre vykonávanie štátnej moci elektronickými prostriedkami.¹⁶ Samotná elektronizácia verejnej správy v širšom zmysle však môže predstavovať napríklad aj proces spracovania podnetov a vyhľadávanie informácií z rôznych registrov.¹⁷

Ako teda mal tento informačný systém vyriešiť problém s veľkým množstvom podnetov? KSED má aj v súčasnosti modul podnetov, ktorý je zodpovedný za správu podnetov, podaných prostredníctvom neho alebo prostredníctvom jeho mobilnej aplikácie. Tento modul mal byť však pôvodne navrhnutý omnoho komplexnejšie. Vzhľadom na prepojenosť tohto systému so všetkými ostatnými systémami

¹⁴ Odporúčanie 2001/331/ES, ktorým sa ustanovujú minimálne kritériá environmentálnych inšpekcií v členských štátoch.

¹⁵ Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.

¹⁶ § 17 zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.

¹⁷ ANDRAŠKO, J. a kolektív: Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021. s. 16.

inšpekcie mal obsahovať určitý druh umelej inteligencie, ktorá by automaticky vykonávala vyššie uvedenú analýzu rizík a posudzovala podnety podľa závažnosti. Takto kategorizované podnety mal systém automaticky postupovať na okresný úrad, alebo v prípade vyhodnotenia ich vyššej závažnosti, prideliť inšpekcii. Tento ambiciózny plán však nakoniec nebol zrealizovaný, najmä vzhľadom na chýbajúcu právnu úpravu, ktorá by umožňovala inšpekcii postúpiť podnet okresnému úradu. Ide totiž o prípady, kedy aj sama inšpekcia je na konanie príslušná, a preto neexistuje zákonný dôvod podľa § 20 správneho poriadku, na základe ktorého by mohla tieto podania postúpiť na vybavenie inému orgánu. Z uvedeného dôvodu nemôže ísť ani o postúpenie veci podľa § 8 správneho poriadku, nakoľko v tomto prípade by muselo ísť o postúpenie na orgán rovnakého druhu a stupňa, pričom jediné, čo by sa líšilo, by bola miestna príslušnosť.¹⁸ O takomto postupe by sme mohli uvažovať v prípade postúpenia medzi dvoma okresnými úradmi, nie však v prípade okresného úradu a inšpekcie.

Použitie umelej inteligencie – utópia alebo reálna možnosť?

Vzhľadom na vyššie uvedené skutočnosti, kategorizácia environmentálnych podnetov doručovaných inšpekcii sa stáva skutočnou nevyhnutnosťou. Dôležité je sa vyhnúť prípadom, kedy sa budú inšpektori zaoberať „orezom jedného konára na susedovom strome“, a z dôvodu krátkosti času a obmedzených personálnych kapacít, nepríde k včasnému prešetreniu závažnejšieho protiprávneho konania.

Umelá inteligencia sa preto stále javí ako vhodný nástroj. Koniec koncov, správne právo je jedno z najvhodnejších odvetví na využívanie umelej inteligencie, práve kvôli veľkému množstvu údajov, s ktorými pracuje, a ktoré sú už teraz uchovávané elektronicky, v rôznych registroch.¹⁹ Takýto systém by mal v ideálnom prípade posudzovať doručené podnety a kategorizovať ich podľa stupňa závažnosti. Taktiež je možnosť zavedenia ich automatického preposielania. Tento systém by však pravdepodobne nepatril medzi vysokorizikové systémy podľa Nariadenia o AI,²⁰ nakoľko je určený len na výkon čiastkovej, aj keď podstatnej úlohy, a nenapĺňa definičné znaky a podmienky stanovené na posudzovanie systémov ako

¹⁸ POTASCH, P., HAŠANOVÁ, J., VALLOVÁ, J., MILUČKÝ, J., MEDŽOVÁ, D.: Správny poriadok komentár. Praha: CH Beck, 2022. s. 87-90.

¹⁹ PARYCEK, P., SCHMID, V., NOVAK, A.-S: Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. In: Journal of the Knowledge Economy. Berlín: Springer, 2024.

²⁰ Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

vysokorizikových. Aj napriek uvedenému, by však bolo nepochybne potrebné, zachovať istú mieru ľudského dohľadu ako aj transparentnosti vo vzťahu k občanom. Pravdepodobne by teda išlo o systém strojového učenia, ktorý by na základe podnetov a ich posúdení, vložených do tohto systému, vedel automaticky vyhodnocovať budúce doručené podnety. Takýto typ programu je totiž schopný sa učiť na základe skúseností, úloh a miery výkonnosti.²¹

Takýto systém so sebou prináša množstvo výhod, napríklad už skôr uvedenú rýchlosť a efektívnosť konaní, rýchlejšiu reakciu príslušných orgánov, či lepšie a racionálnejšie využívanie personálnych kapacít inšpekcie a okresných úradov. Môže zároveň aj zlepšiť komunikáciu s verejnosťou, nakoľko v súčasnosti sa často stáva, že občania kontaktujú príslušný orgán ohľadom stavu šetrenia podnetu, pričom v tomto prípade ešte ani nebolo začaté šetrenie.²² Proces sa zefektívni, čo so sebou automaticky nesie aj rýchlejšiu reakciu, rýchlejšie rozhodnutie vo veci a v konečnom dôsledku aj rýchlejšie upovedomenie podávateľa o stave jeho podnetu. Pri snahe o dosiahnutie najvyššej možnej miery efektivity však vždy musia byť zachované aj ostatné princípy správneho konania, ktoré by na úkor efektivity nemali byť potláčané.²³

Takýto systém so sebou nesie aj radu rizík, či problematických oblastí. Jedným z takýchto problémov je zodpovednosť za nesprávne alebo nezákonné rozhodnutie. Dôležité je posúdenie, že daný subjekt bude v tomto prípade vystupovať ako orgán verejnej moci, nakoľko rozhoduje o právach a právom chránených záujmoch fyzických a právnických osôb. Ak pri procese rozhodovania využíva umelú inteligenciu, tá by mala byť využívaná na zodpovednosť daného orgánu, a teda v prípade nesprávneho alebo nezákonného postupu vznikne škoda, spôsobená pri výkone verejnej moci podľa zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov, v znení neskorších predpisov.²⁴ V tomto prípade však nepôjde o rozhodnutie vo veci, a preto jeho následky zjavne nebudú také rozsiahle ako v prípade meritórneho rozhodnutia, avšak aj napriek tomu by malo byť v najlepšom záujme daného orgánu, aby tento systém rozhodoval správne.

Ďalšou kategóriou sú otázky transparentnosti takéhoto rozhodovania, ktoré by mali byť zaručené za každých okolností. Podávateľ podnetu by mal byť upovedomený o skutočnosti, že o jeho podnete rozhodovala umelá inteligencia a taktiež by mal byť

²¹ MESARČÍK, M., GYURÁSZ, Z.: Právo a umelá inteligencia. Bratislava: Právnická fakulta univerzity Komenského v Bratislave, 2024. s. 3

²² Informácie získané riadeným rozhovorom so zamestnancami SIŽP.

²³ WEITZENBOECK, E. M.: Simplification of Administrative Procedures through Fully Automated Decision-Making: The Case of Norway. In: Administrative Sciences. Bazilej: Multidisciplinary Digital Publishing Institute (MDPI), 2021.

²⁴ MESARČÍK, M., GYURÁSZ, Z.: Právo a umelá inteligencia. Bratislava: Právnická fakulta univerzity Komenského v Bratislave, 2024. s. 125.

schopný požiadať o preskúmanie takéhoto rozhodnutia človekom. Okrem tohto ponímania transparentnosti by však mal byť tento systém aj predvídateľný vo svojich rozhodnutiach, teda by malo byť zrejmé, ako a na základe čoho, rozhoduje. Uvedené do veľkej miery súvisí aj s dôverou občanov v takéto rozhodovanie. Transparentnosť takéhoto AI systému by preto nemala byť založená len na procese získavania výsledku, či naopak na výsledku samotnom, ale na celej škále hodnôt, ktoré chceme do tohto daného systému pretaviť.²⁵

V neposlednom rade, každý AI systém čelí aj otázke zachovania kybernetickej bezpečnosti a ochrany osobných údajov, pričom systémy verejnej správy nie sú výnimkou. Tento systém musí byť preto zabezpečený tak, aby bol odolný voči akýmkoľvek neoprávneným prístupom tretích osôb, či akýmkoľvek útokom na tieto systémy. Samotná umelá inteligencia, samozrejme v inej forme ako v našom nastavenom programe, sa už v súčasnosti využíva na zlepšenie zabezpečenia iných systémov pred kybernetickými útokmi. Sama však môže byť aj napriek tomu zraniteľná. Problémom je okrem dátovej a výkonnostnej náročnosti, aj potreba neustáleho prispôsobovania novým druhom potencionálnych hrozieb.²⁶

Tak, ako každý iný informačný systém, aj tento by bol nepochybne naplňaný osobnými údajmi, ktoré by však s najväčšou pravdepodobnosťou nemali povahu citlivých osobných údajov.²⁷ Aj napriek tomu však musí byť zabezpečená ich náležitá ochrana pred zneužitím. Výhodou, no aj problémom, môže byť tiež nezaujatosť či zaujatosť takéhoto systému. Často sa o AI hovorí ako o objektívnej, avšak jej výstupy do veľkej miery záležia od vstupných údajov, ktoré môžu byť skreslené. Vytvára sa tu teda priestor na vznik nespravodlivých, či zaujatých rozhodnutí.²⁸

Záver

Kategorizácia podnetov v oblasti životného prostredia sa v dnešnej dobe stáva nevyhnutnou činnosťou. Vzhľadom na rýchly rozvoj vedy a techniky sa ako vhodné javí využiť na túto činnosť náležité technologické nástroje a postupy tak, aby bola činnosť orgánov verejnej správy čo najviac zjednodušená, čo zároveň zabezpečí efektívnejšie a rýchlejšie rozhodovanie. Jednou z takýchto možností je nepochybne kategorizácia podnetov pomocou umelej inteligencie.

²⁵ BUIJSMAN, S.: Transparency for AI systems: a value-based approach. In: Ethics and Information Technology, 26, 34. Berlín: Springer Science and Business Media LLC, 2024.

²⁶ SALEM, A.H., AZZAM, S.M., EMAM, O.E., ABOHANY, A. A.: Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. In: Journal Big Data 11, 105, Berlín: SpringerOpen, 2024.

²⁷ K citlivým osobným údajom pozri bližšie: MESARČÍK, M.: Ochrana osobných údajov. Bratislava: C.H. Beck, 2020. s. 49 – 50.

²⁸ PINTÉROVÁ, D. Právna regulácia umelej inteligencie (perspektívy a výzvy). In: Právny obzor, 107, č. 4, Bratislava: Wolters Kluwer, 2024. s.363.

V takomto prípade by išlo o systém, ktorý by na základe vložených podnetov a ich výsledkov, vedel posúdiť závažnosť daného podnetu, a prípadne ho aj priradiť príslušnému orgánu. K aplikácii takéhoto postupu by však muselo prísť k zmene časti legislatívy, nakoľko v prípade príslušnosti daného orgánu, nie je možné postúpiť podnet na iný príslušný orgán len kvôli jeho menšej závažnosti.

Tento systém by bol nie len pomerne náročný na vytvorenie, ale aj na údržbu, nakoľko by musel byť výborne zabezpečený pred možnými kybernetickými hrozbami a s tým spojeným únikom osobných údajov, ktorými by bol napĺňaný. Pri jeho prevádzke by museli byť zachované všetky zásady ochrany osobných údajov, ako napríklad zásada minimalizácie údajov, zásada obmedzenia účelu, či zásada integrity a dôvernosti.

Všeobecne sa s otázkou využívania AI vo verejnej správe spája aj otázka vyvodzovania zodpovednosti za prípadné nesprávne alebo nezákonné rozhodnutie správneho orgánu. Je však možné konštatovať, že ak orgán využíva pri svojej činnosti umelú inteligenciu, za nesprávne rozhodnutie, urobené týmto systémom, alebo prostredníctvom neho by voči občanovi zodpovedal tento orgán a teda štát. Otázkou však zostáva subsidiárna zodpovednosť dodávateľa tohto AI systému voči orgánu verejnej moci. V takomto prípade by už nešlo o zodpovednosť pri výkone verejnej moci, ale o súkromnoprávny typ zodpovednosti.

V neposlednom rade je veľmi dôležité zachovanie transparentnosti, nie len pri prevádzke AI systému, ale aj pri výkone verejnej moci. Preto je o to dôležitejšie, aby sme poznali, na základe čoho umelá inteligencia rozhoduje a ako rozhoduje. Táto otázka je kľúčová aj z hľadiska objektivity rozhodovania. Podávateľ podnetu by mal byť taktiež informovaný o tom, že jeho podnet spracovala umelá inteligencia, nakoľko práve transparentnosť je kľúčovým faktorom, ktorý napomáha k postupnému budovaniu dôvery občanov v takéto formy rozhodovania.

Vytvorenie a využívanie takéhoto systému má potenciál prispieť k rýchlejšiemu a efektívnejšiemu prešetrovaniu podnetov, rýchlejšiemu rozhodovaniu a v konečnom dôsledku aj k vyššej miere ochrany životného prostredia. Otázkou však zostáva, či je naša spoločnosť a najmä naša verejná správa pripravená na využívanie takýchto systémov.

Zoznam použitej literatúry

1. ANDRAŠKO, J. a kol.: Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021. ISBN: 9788097383725. 324 s.
2. BUIJSMAN, S.: Transparency for AI systems: a value-based approach. In: Ethics and Information Technology, 26, 34. Berlín: Springer Science and Business Media LLC, 2024. <https://doi.org/10.1007/s10676-024-09770-w>

3. MESARČÍK, M.: Ochrana osobných údajov. Bratislava: C.H. Beck, 2020. ISBN: 9788089603923. 320 s.
4. MESARČÍK, M., GYURÁSZ, Z.: Právo a umelá inteligencia. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. ISBN: 978-80-7160-715-1. 244 s.
5. PARYCEK, P., SCHMID, V., NOVAK, A.-S.: Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. In: Journal of the Knowledge Economy. Berlín: Springer, 2024. s. 8390–8415. <https://doi.org/10.1007/s13132-023-01433-3>
6. PINTÉROVÁ, D. Právna regulácia umelej inteligencie (perspektívy a výzvy). In: Právny obzor, 107, č. 4, Bratislava: Wolters Kluwer, 2024. s. 361 – 383 <https://doi.org/10.31577/pravnyobzor.2024.4.02>
7. POTASCH, P., HAŠANOVÁ, J., VALLOVÁ, J., MILUČKÝ, J., MEDŽOVÁ, D.: Správny poriadok komentár. Praha: CH Beck, 2022. ISBN: 978-80-7400-908-2. 688 s.
8. SALEM, A.H., AZZAM, S.M., EMAM, O.E., ABOHANY, A. A.: Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. In: Journal Big Data 11, 105, Berlín: SpringerOpen, 2024. <https://doi.org/10.1186/s40537-024-00957-y>
9. VRABKO, M. a kolektív: Správne právo hmotné všeobecná časť. Bratislava: C. H. Beck, 2018. ISBN: ISBN: 978-80-89603-68-8. 361 s.
10. WEITZENBOECK, E. M.: Simplification of Administrative Procedures through Fully Automated Decision-Making: The Case of Norway. In: Administrative Sciences. Bazilej: Multidisciplinary Digital Publishing Institute (MDPI) 11(4), 149, 2021. <https://doi.org/10.3390/admsci11040149>
11. Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)
12. Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov
13. Zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov
14. Zákon č. 14/2023 Z. z. o ochrane ovzdušia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
15. Zákon č. 150/2019 Z. z. o prevencii a manažmente introdukcie a šírenia invázných nepôvodných druhov a o zmene a doplnení niektorých zákonov
16. Zákon č. 346/2004 Z. z. o vodách o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon) v znení neskorších predpisov

17. Zákon č. 79/2015 Z. z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
18. Zákon č. 39/2013 Z. z. o integrovanej prevencii a kontrole znečisťovania životného prostredia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
19. Zákona č. 525/2003 Z. z. o štátnej správe starostlivosti o životné prostredie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
20. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
21. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
22. Odporúčanie 2001/331/ES, ktorým sa ustanovujú minimálne kritériá environmentálnych inšpekcií v členských štátoch
23. Informácie získané riadeným rozhovorom so zamestnancami SIŽP.
24. Údaje poskytnuté okresnými úradmi na základe žiadostí podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
25. Výročná správa Slovenskej inšpekcie životného prostredia za rok 2024
26. Vyhodnotenia plánu hlavný úloh jednotlivých útvarov inšpekcie za roky 2023 a 2022

Kontaktné údaje

Mgr. Dominika Noskovičová

noskovicova13@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

MOŽNOSTI A LIMITY VYUŽÍVANIA UI PRI ROZHODOVANÍ O NÁHRADE ŠKODY SPÔSOBENEJ URČENÝMI ŽIVOČÍCHMI

POSSIBILITIES AND LIMITS OF USING AI DECIDING ON COMPENSATION FOR DAMAGE CAUSED BY SPECIFIC ANIMALS

Viktória Sokolová¹

Abstrakt: Príspevok analyzuje možnosti a limity využívania umelej inteligencie pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi podľa zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov. Autorka v úvode analyzuje platnú právnu úpravu procesu vyplácania náhrad škôd a identifikuje jeho jednotlivé fázy. V ďalšej časti príspevku načrtáva možnosti použitia nástrojov umelej inteligencie – od oznámenia o vzniku škody až po vydanie rozhodnutia orgánom ochrany prírody. Na základe analýzy legislatívneho rámca a komparácie s úpravou v Poľsku a v Českej republike príspevok poukazuje na absenciu právneho základu umožňujúceho využívanie umelej inteligencie v správnom rozhodovaní v podmienkach Slovenskej republiky. Diskutuje tiež etické, technické a vzdelávacie aspekty implementácie AI do verejnej správy. Prínosom príspevku je aj návrh doplnenie znenia zákona o ustanovenie umožňujúce využívanie AI pri monitorovaní, spracovaní dát a príprave rozhodnutí, pričom zdôrazňuje potrebu zachovania princípu „human-in-the-loop“. Cieľom príspevku je iniciovať odbornú diskusiu o možnostiach integrácie umelej inteligencie do procesov ochrany prírody a zefektívnenia rozhodovacej činnosti štátnej správy. Zároveň však autorka príspevku hľadá odpoveď vedeckú otázku či je možné využívanie UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi. V závere príspevku nájde čitateľ odpoveď.

Kľúčové slová: náhrada škody, umelá inteligencia, možnosti právnej úpravy, limity

Abstract: The paper analyses the possibilities and limits of using artificial intelligence (AI) in administrative decision-making concerning compensation for damage caused by designated animal species under Act No. 543/2002 Coll. on the Protection of Nature and Landscape, as amended. The author first

¹ Právnická fakulta, Univerzita Komenského v Bratislave

examines the existing Slovak legal framework regulating the process of compensation payments and identifies its individual procedural phases. The following section outlines potential applications of AI tools in each stage of this process – from the notification of damage and on-site investigation to the issuance of a final decision by the competent nature protection authority. Based on a comparative analysis with the legislation of Poland and the Czech Republic, the paper highlights the absence of a clear legal basis allowing the use of AI in administrative decision-making in Slovakia. It also addresses the ethical, technical, and educational aspects of implementing AI in the public sector, with particular emphasis on the environmental administration. The contribution further proposes the introduction of a new legislative provision enabling the use of AI for monitoring, data processing, and the preparation of draft decisions, while ensuring compliance with the “human-in-the-loop” principle and fundamental rights protection. The aim of the paper is to stimulate academic and professional discussion on the integration of AI into nature protection processes, its potential to increase the efficiency of public administration, and to provide an informed answer to the research question of whether AI can be lawfully and effectively used in deciding on compensation for damage caused by protected wildlife.

Key words: compensation for damage, artificial intelligence, limits, possibilities

Úvod

Umelá inteligencia dnes už nie je našou budúcnosťou ale je prítomnosťou. Súčasný rozvoj umelej inteligencie prináša nové možnosti asi vo všetkých oblastiach života. Medzi oblasti s priaznivou perspektívou využívania umelej inteligencie patrí aj ochrana životného prostredia. Mnohé štáty už dnes dokážu využívať umelú inteligenciu pri kontrole, monitorovaní či ukladaní pokút za porušovanie ochrany životného prostredia. Využívanie umelej inteligencie však ponúka aj iné oblasti v ktorých by mohla nájsť uplatnenie. Tento príspevok približuje proces vyplácania náhrad za škody spôsobené určenými živočíchmi a zároveň prepája možnosti, limity a výzvy vo vzťahu k využívaniu umelej inteligencie pri rozhodovaní o náhrade škody. Príspevok vo svojej prvej časti využíva deskriptívnu metódu bádania, ktorá má detailne popísať stav vecí alebo prebiehajúceho procesu náhrady škody spôsobenej určenými živočíchmi. V ďalšej časti príspevku budeme využívať metódy analýzy, syntézy, právnej komparatistiky a prognostickej metódy v závere príspevku. Hlavnou vedeckou otázkou, ktorú sa pokúsime týmto príspevkom zodpovedať je: Či je možné využívanie UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi.

Pričom v prvej časti sa budeme venovať aktuálnej právnej úprave a jej detailnému opisu do ktorej v druhej podkapitole príspevku navrhujeme využívanie UI. A v poslednej časti príspevku navrhujeme doplnenie aktuálnej právnej úpravy s ohľadom na dodržiavanie zásad využívania UI vo verejnej správe. Cieľom príspevku nie je vytvorenie komplexnej právnej legislatívy v skúmanej oblasti ale len načrtnutie a nadchnutie tejto právnej a etickej témy k širšiemu vedeckému bádaniu, ktoré sa, v ideálnom prípade, pretaví do legislatívnej zmeny.

Proces vyplácania náhrady škody spôsobenej určenými živočíchmi

Vyplácanie náhrady škody spôsobenej určenými živočíchmi nájdeme upravené v zákone č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov (ďalej len „ZoOPaK“. Ide o stav *de lege lata*, ustanovenia § 97 a nasledujúce, ktoré upravujú predmet za ktorý je náhrada škody vyplácaná, podmienky, ktoré musia byť splnené a aj rozsah a procesný postup vyplácania škôd. Živočíchy za ktoré štát zodpovedá za škodu sú taxatívne vymedzené v prílohe č. 39 vyhlášky č. 170/2021 Z. z. ktorou sa vykonáva zákon o ochrane prírody a krajiny. Náhrada škody je súčasťou environmentálneho práva. Vývoj náhrady škody spôsobenej určenými živočíchmi na našom území sa spája s jeho vznikom už od 20. storočia ale aj skôr.²

Náhradu škody za určené živočíchy je možné vyplatiť len na predmetoch, ktoré sú v zmysle zákona taxatívne vymedzené. Ide najmä o domestikované živočíchy, včelstvá, poľné plodiny, dreviny či život a zdravie fyzickej osoby.³ Podmienky nároku na náhradu škody v základných rámcoch určuje zákon, no presnejšie vymedzenie podmienok, ktoré musia byť splnené, aby mohla byť náhrada škody vyplatená vymedzuje vyhláška v ustanovení § 45. Ide konkrétne o podrobnosti o primeraných preventívnych opatreniach na ochranu vybraných domestikovaných živočíchov, včelstiev a včelárskych zariadení pred určeným živočíchom. Rozsah náhrady škody je určený v ustanovení § 99 a to pri škode na živote alebo zdraví ako jednorazové odškodnenie a náhrada primeraných nákladov spojených s pohrebom alebo účelne a preukázateľne vynaložených nákladov spojených s liečením v súvislosti so vznikom škody. Pri škode na zdraví sa poškodenému poskytuje odškodnenie za bolesť a sťažené spoločenské uplatnenie. Pri ostatných druhoch škôd sa uhradí v zmysle zákona skutočná škoda. Tu je potrebné odlišovať od škôd spôsobených na domestikovaných zvieratách a napríklad rybách pri ktorých sa vychádza zo zaznamenatej početnosti výskytu určených živočíchov pri vodnej ploche.

²K tomu pozri: MICHALOVIČ, Matúš a Michal MASLEN. Advocating for environmental law – grounds for its status as an independent branch of law in Slovak legal doctrine. *Prawne Problemy Górnictwa i Ochrony Środowiska*, 2024, č. 2, s. 2 a nasl. DOI: 10.31261/PPGOS.2024.02.06.

³ § 97 Zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov.

Vznik škody oznámi poškodený alebo pozostalá osoba. Zákon určuje lehoty v ktorých je potrebné vykonať takéto oznámenie. Podľa ustanovenia § 100 má pozostalá osoba 60 dní na oznámenie vzniku škody. V ostatných prípadoch je lehota kratšia a to 48 hodín odo dňa jej zistenia. Vznik škody sa oznamuje orgánu ochrany prírody, v ktorého územnom obvode došlo ku škode. Orgán ochrany prírody po oznámení vzniku škody do troch dní uskutoční miestne zisťovanie. Na tomto miestnom zisťovaní alebo aj obhliadke miesta kde škoda vznikla sa zúčastnia zamestnanci orgánu ochrany prírody, teda zamestnanci príslušného okresného úradu, ďalej zamestnanci organizácie ochrany prírody, ktorou je Štátna ochrana prírody SR a poškodený. Miestna obhliadka slúži ako hlavný podklad pre rozhodnutie o náhrade škody. Zisťujú sa na nej, kto alebo čo mohlo škodu spôsobiť, zaisťujú sa dôkazy a fotodokumentácia. Zamestnanci Štátnej ochrany prírody SR pritom zabezpečujú odbornosť, teda to, aby bolo spoľahlivo a odborne zistené, či vzniknutú škodu spôsobilo niektoré z určených živočíchov. Z miestneho zisťovania sa následne spíše protokol, ktorý slúži ako podklad k rozhodnutiu. Poškodený si ďalej musí uplatniť právo na náhradu škody v zmysle ustanovenia § 100 ods. 2 a to písomnou žiadosťou doloženou dokladmi a podkladmi potrebnými na posúdenie nároku. Žiadosť musí obsahovať predpísané náležitosti, ktoré upravuje zákon a aj vyhláška.

Posledným procesným krokom je rozhodnutie orgánu ochrany prírody. Ten v zmysle ustanovenia § 100 ods. 7 môže na preukázanie skutočnosti, že škoda vznikla, ako i na preukázanie rozsahu škody vyzvať poškodeného v prípade pochybností na doplnenie predložených dokladov. Môže tiež dať vypracovať odborný posudok alebo znalecký posudok. Pri posudzovaní žiadosti o náhradu škody vychádza okresný úrad zo všetkých predložených podkladov a dokladov, ako aj z preukázaných majetkových práv, prípadne iných vzťahov k predmetu vzniknutej škody. V prípade vzniku škody na zdraví alebo živote fyzickej osoby posudzuje škodu na základe lekárskej správy. Môže tiež využiť údaje o monitorovaní určených živočíchov, ktoré poskytuje ministerstvo alebo organizácia ochrany prírody.⁴ Ak orgán ochrany prírody, v ktorého územnom obvode ku škode došlo, zistí, že škodu spôsobil určený živočích, sú splnené podmienky určené zákon a nie sú iné pochybnosti, zaplatí náhradu škody poškodenému najneskôr do štyroch mesiacov. O svojom rozhodnutí nahradiť škodu spôsobenú určeným živočíchom informuje poškodeného.

Taxatívne vymedzenie určených voľne žijúcich živočíchov má za cieľ chrániť tieto druhy živočíchov aj napriek tomu, že môžu spôsobovať škody. Ich voľný pohyb v prírode je však veľmi dôležitý. Hovorí o tom aj Envirostratégia 2030 v zmysle ktorej, je potrebné minimalizovanie straty biodiverzity, pre ktorú sú aj určené živočíchy

⁴ § 101 ods. 2 zákona č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov.

potrebné vo voľnej prírode.⁵ Určenými živočíchmi sú v zmysle prílohy č. 39 k vyhláške č. 170/2021 Z. z. los mokradňový, beluša veľká, volavka popolavá, zubor hôrny, vlk dravý, bobor vodný, krkavec čierny, vydra riečna, rys ostrovid, kormorán veľký, medveď hnedý. Pre porovnanie uvádzame počet určených živočíchov podľa ustanovenia § 126 Zákona zo 16. apríla 2004 o ochrane prírody v Poľsku (poľ. *Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody*). Ide o zubry, vlky, rysy, medvede a bobry. V Poľsku zákonodarca obmedzil v niektorých prípadoch potencionálnym poškodeným stranám v preventívnych opatreniach (napr. je zakázané preventívne usmrtiť takéto zviera, aby sa predišlo ujme).⁶ Vidíme teda istej forme rovnaký úmysel zákonodarcu ochraňovať tieto živočíchy. V Českej republike sú určené živočíchy definované v zákone č. 115/2000 Sb., o poskytovaní náhrad škod spôsobených vybranými zvlášť chránenými živočíchmi. Podľa ustanovenia § 3 ide o bobra európskeho, vydra riečnu, losa európskeho, medveďa hnedého, rysa ostrovida a vlka. Za príklad ochrany v Česku môžeme uviesť bobra európskeho. V roku 2013 bola prijatá Koncepcia Programu péče, ktorá je založená na tzv. zonácii diferencovanej ochrany.⁷ Zabezpečuje ochranu pohybu a pobytu bobra v jeho prirodzenom prostredí s ohľadom na škody, ktoré tento živočích môže spôsobiť.

Akým spôsobom by sa dala využiť umelá inteligencia pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi?

Ak by sme mala autorka tohto príspevku za úlohu vymyslieť systém alebo lepšie povedané vymyslieť možnosti využívania UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi mohli by sme hovoriť o nasledovnom.

V prvej časti sa príspevok zaoberá aktuálnou právnou úpravou náhrady škody spôsobenej určenými živočíchmi. Proces vyplácania náhrady škody by sme mohli zadefinovať v zmysle uvedeného do piatich procesných fáz:

1. vznik škody
2. oznámenie o vzniku škody orgánu ochrany prírody
3. miestne zisťovanie
4. žiadosť o vyplatenie náhrady škody
5. rozhodnutie o vyplatení alebo nevyplatení náhrady škody.

⁵ Zelenšie Slovensko. *Stratégia environmentálnej politiky Slovenskej republiky do roku 2030*. Bratislava : Ministerstvo životného prostredia SR, 2019. s. 11. Dostupné z: https://www.minzp.sk/files/iep/03_vlastny_material_envirostrategia2030_def.pdf [cit. 2025-09-27].

⁶ RAKOCZY, Bartosz. *Odpowiedzialność skarbu państwa za szkody spowodowane przez zwierzęta na podstawie art. 126 ustawy o ochronie przyrody*. Acta Universitatis Carolinae – Iuridica, 2015, roč. 61, č. 2, s. 144. [cit. 2025-09-27].

⁷ DAMOHORSKÝ, Milan a Petr ŠEDINA. *Ochrana bobra evropského v českém právu*. Acta Universitatis Carolinae. Iuridica. Praha : Univerzita Karlova, Právnická fakulta, 2015, roč. 61, č. 2, s. 57.

Pri jednotlivých fázach procesu náhrady škody by sme UI mohli využiť nasledovne. Ministerstvo alebo organizácia ochrany prírody, ktorou je Štátna ochrana prírody SR v rámci svojej činnosti monitoruje určené živočíchy. Tento monitoring by sa v prvej fáze dal využiť na účinné zabezpečenie ochrany pred určenými živočíchmi, ktoré žijú vo voľnej prírode. Umelá inteligencia by mohla v tejto fáze vyhodnocovať dáta z dronov a fotopascí a zasielať upozornenia či už samotným vlastníkom napríklad oviec alebo kôz či včelstiev, ktoré sa v danej lokalite nachádzajú. Taktiež by tieto údaje mohli byť neskôr využité na jednoduchšie a rýchlejšie rozhodnutie o vyplatení náhrady škody.

V ďalšej fáze procesu náhrady škody, teda v oznámení o vzniku škody, zákon nestanovuje presne, ktoré informácie má oznámenie obsahovať. Vo vzore oznámenia, ktoré je dostupné na stránke Ministerstva vnútra SR⁸ sa uvádza adresa alebo lokalita kde ku škode došlo, dátum zistenia škody a opis jej rozsahu, označenie určeného živočicha, ktorý podľa poškodeného škodu spôsobil a opis opatrení žiadateľa, ktoré vykonal na zabránenie vzniku škody, výpočet hodnoty poškodenia a jeho detailný rozsah. Poškodený zároveň má uviesť aj uplatňovanú výšku náhrady v eurách. Momentálne sa tento krok vykonáva v papierovej forme. Aj keď má orgán ochrany prírody povinnosť vykonať miestnu obhliadku do troch dní v zmysle ustanovenia § 101 ods. 1 zákona, v praxi sa môže (a aj často stáva), že miestne zisťovanie je vykonané až po piatich dňoch. Je tak z dôvodu, že do týchto dní prípadne víkend, ktorý túto lehotu predĺži. Zníži sa tým možnosť spoľahlivo zistiť pôvodcu škody a zároveň tým môže byť znížená aj celková výška vyplatenej škody. Štátna ochrana prírody SR na svojej web stránke uvádza, že: Odporúčanie mimo citovaný zákon: najideálnejšie je škodu písomne nahlásiť príslušnému okresnému úradu, bezprostredne po zistení škody a zároveň telefonicky kontaktovať zamestnanca Štátnej ochrany prírody SR. Prečo uvádzame toto odporúčanie? Ak poškodený splní vrchnú lehotu nahlásenia škody do dvoch dní a okresný úrad do troch dní od ohlásenia škody zvolá šetrenie, prebehnúť môže celkovo až 5 dní. Vo veľa prípadoch nie je možné po 5 dňoch od vzniku škody objektívne posúdiť, či ide o škodu spôsobenú chráneným živočíchom, resp. veľkou šelmou (štádium rozkladu riešených zvierat, nepriaznivé poveternostné podmienky, vďaka ktorým zanikne možnosť prípadného stopovania pôvodcu škôd a pod.)“.⁹ V tomto kroku by využívanie UI mohlo prebiehať prostredníctvom platformy alebo univerálneho celoslovenského systému podobného ako je portál Slovensko.sk. Poškodený by mohol oznámenie o vzniku škody zasielať online. Zamedzilo by sa tým aj zmienenému predĺženiu

⁸ Oznámenie o vzniku škody. Ministerstvo vnútra Slovenskej republiky [online]. Dostupné z: <https://www.minv.sk/?okresne-urady-klientske-centra&urad=32&odbor=10&subor=311212> [cit. 2025-09-27].

⁹ Ako nahlásiť škodu spôsobenú určeným živočíchom? Štátna ochrana prírody SR, 2018 [online]. Dostupné z: <https://www.sopsr.sk/web/?cl=20352> [cit. 2025-09-27].

lehoty na vykonanie obhliadky. Doručovanie online by mohlo mať výhodu aj v tom smere, že prostredníctvom automatizácie by mohli byť informovaní zamestnanci okresných úradov ako aj Štátnej ochrany prírody SR o vzniku škody, čo by urýchlilo ich informovanosť. Okrem toho takéto využitie umelej inteligencie môžeme preniesť aj do protokolu, ktorý sa spisuje v ďalšej fáze procesu náhrady škody pri vykonaní miestneho zisťovania. UI by mohla informácie, ktoré poškodený zadal do systému jednoducho prekopírovať aj do protokolu či neskôr už do samotného rozhodnutia o vyplatení alebo nevyplatení náhrady škody. Ak by sme do tohto procesu ešte pridali aj pohotovosť zamestnancov okresných úradov a Štátnej ochrany prírody SR, aby sa zabezpečila ešte skoršia a rýchlejšia obhliadka vzniknutých škôd, mohlo by dôjsť k úplnému naplneniu zmyslu tejto časti zákona.

Žiadosť o vyplatenie náhrady škody musí vyplniť poškodený momentálne v písomnej papierovej forme a tú doručiť na príslušný okresný úrad. Aj tu by mohol prebiehať proces automatizácie, kedy by v konkrétnom konaní cez portál verejnej správy vedel poškodený pokračovať v procese náhrady škody. Portál verejnej správy by mohol na základe použitia UI použiť informácie z oznámenia a z protokolu, ktoré by už boli nahraté v systéme a na základe nich predpripraviť žiadosť o náhradu škody. Súčasťou žiadosti by mal byť aj kompletný výpočet náhrady škody podľa toho, aká bola zistená skutočná škoda pri miestnej obhliadke.

Následne v poslednej fáze by UI mohla zamestnancovi okresného úradu predpripraviť rozhodnutie na základe všetkých informácií, ktoré boli do systému vložené. Zamestnanec okresného úradu by tieto informácie skontroloval a vydal rozhodnutie o vyplatení náhrady škody spôsobenej určenými živočíchmi.

Právna úprava využívania umelej inteligencie pri rozhodovaní o náhrade škody v podmienkach SR

Pojem náhrady škody sa v krajinách strednej Európy líši podľa toho, kto škodu platí a komu, ale aj v aspektoch rozsahu zodpovednosti (aké škody sú kryté, pre aký druh zveri) a posúdenia zodpovednosti (akú úlohu zohráva zavinenie).¹⁰ V krajinách EÚ nájdeme už dnes prvé právne úpravy¹¹, ktoré hovoria o využívaní UI pri rozhodovaní. V niektorých prípadoch ide o automatické rozhodovanie UI bez zásahu fyzickej osoby¹² v iných slúži využívanie UI len ako podklad na rozhodnutie¹³.

¹⁰ VOMÁČKA, Vojtěch a Josef BÁRTŮ. Damage caused by game and its compensation in Central European countries: A comparative perspective. *Central European Journal of Comparative Law* [online]. 2023, 4(2), s. 198 [cit. 2025-09-26]. Dostupné z: <https://doi.org/10.47078/2023.2.123-141>.

¹¹ Príkladom môže byť Taliansko.

¹² Príkladom môže byť Holandsko.

¹³ Napríklad Estónsko.

Využívanie umelej inteligencie pri rozhodovaní o právach alebo povinnostiach fyzických a právnických osôb v štátnej alebo verejnej správe je na Slovensku zatiaľ istým spôsobom tak povediac sci-fi. Na využívanie umelej inteligencie pri rozhodovaní nemáme zatiaľ právnu úpravu, aj keď určitý návrh právnej úpravy je aktuálne v medzirezortnom pripomienkovom konaní.¹⁴ Vedeckou otázkou, ktorú sme si stanovili v úvode práce je, či je možné využívať UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi. Vzhľadom na fakt, že v ZoOPaK nenájdeme ustanovenie umožňujúce takéto využívanie UI môžeme z tohto pohľadu na vedeckú otázku odpovedať, že v aktuálnej právnej úprave platnej a účinnej v podmienkach SR, nie je možné využívanie UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi.

Je však nevyhnutné dodať, že ani prijatie základného právneho rámca na úrovni EÚ toto rozhodovanie neumožní. A neumožní to ani národná právna úprava. Možnosťou ako využívať UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi vidíme len v zmene ustanovení o náhrade škody, teda ZoOPaK.

Zmena legislatívy a samotné využívanie UI pri rozhodovaní však musí byť jednoznačne v zmysle základných zásad pre využívanie UI. AI predstavuje „ideálnu technológiu, ktorá sa má aplikovať v kontexte verejného sektora, kde sa environmentálne prostredie neustále mení a predprogramovanie nemôže zohľadniť všetky možné prípady“.¹⁵ Čo sa však, na rozdiel od iných individuálnych správnych aktov, netýka náhrady škôd pretože samotný proces, ako aj výpočty sú presne stanovené. Kľúčovou je v tomto smere miestna obhliadka, ktorú však vykonávajú odborníci, aby bol skutočný pôvodca škody starostlivo zistený.

Okrem základných princípov dôležitých pri rozhodovaní¹⁶, ktorými sú princíp zákonnosti, rovnosti, nestrannosti a objektívnosti či hospodárnosti konania¹⁷, sú dôležité aj princíp transparentnosti, princíp human-in- the-loop, teda zodpovednosť a kontrola človekom a v neposlednom rade ochrana súkromia a dátová bezpečnosť. Tie nájdeme upravené v rôznych dokumentoch napríklad v Etických usmerneniach

¹⁴ Legislatívny proces LP/2025/401. [online]. Bratislava: Slov-Lex, 2025. Dostupné z: <https://www.slov-lex.sk/elegislativne-procesy/SK/LP/2025/401>.

¹⁵ SUN, T. Q. a MEDAGLIA, R. *Mapovanie výziev umelej inteligencie vo verejnom sektore: dôkazy z verejného zdravotníctva*. Government Information Quarterly, 2019, 36(2), s. 370. DOI: [10.1016/j.giq.2018.09.008](https://doi.org/10.1016/j.giq.2018.09.008). [cit. 2025-09-27].

¹⁶ K tomu pozri aj: Vrabko, M. a kol. *Správne právo hmotné. Všeobecná časť*. 3. vyd. Bratislava: C. H. Beck, 2025. s. 144 a nasl.

¹⁷ K tomu pozri: Cepek, B. a kol. *Environmentálne právo: všeobecná a osobitná časť*. Plzeň: Aleš Čeněk, 2015. s. 28 a nasl.

Európskej komisie pre dôveryhodnú AI¹⁸, OECD AI Principles¹⁹ či UNESCO Recommendation on the Ethics of Artificial Intelligence²⁰. No asi najdôležitejším je Európsky akt o umelej inteligencii (AI Act).²¹

Napriek tomu, že pri zavádzaní UI do praxe môžeme naraziť na problém nie len pri ukotvení princípov a zásad pri používaní UI do právnej úpravy ale aj pri vzdelávaní zamestnancov v štátnej a verejnej správe. Všeobecný nedostatok pochopenia fungovania umelej inteligencie medzi občanmi môže viesť k ich váhaniu s používaním umelej inteligencie verejnými orgánmi, čo obmedzuje možnosti orgánov používať tieto technológie. Samotní štátni zamestnanci tiež nemusia úplne chápať príležitosti a dôsledky umelej inteligencie, keďže vo verejnom sektore všeobecne chýbajú zručnosti súvisiace s umelou inteligenciou.²² Vzdelávanie zamestnancov v štátnej správe starostlivosti o životné prostredie upravuje vyhláška č. 462/2004 Z. z. ktorou sa ustanovujú podrobnosti o osobitných kvalifikačných predpokladoch na výkon niektorých činností na úseku starostlivosti o životné prostredie. Tá je však zastaralá a z autorkiných výskumov momentálne neprebíha odborná príprava v zmysle tejto vyhlášky v oblasti využívania UI. Okrem toho sa môžeme pri zavádzaní UI do aplikácie vo verejnej správe stretnúť aj s problémami akými sú napríklad etické, technické, spoločenské a právne problémy.

Na práve posledné spomínané, teda právne problémy, už tento príspevok priblížil. Príspevok priblížil ako by mohlo vyzeráť rozhodovanie o náhrade škody teoreticky. V tejto časti však chce autorka uviesť aj niekoľko návrhov k samotnej legislatíve v tejto oblasti.

Využívanie umelej inteligencie procese náhrady škody spôsobenej určenými živočíchmi by sme mohli doplniť do aktuálneho znenia zákona o nové ustanovenie § 99a. Ustanovenie by mohlo umožňovať využívanie UI na účely:

- a) monitorovania pohybu určených živočíchov,
- b) vyhodnocovania dát z automatizovaných senzorov (napr. drony, fotopasce),

¹⁸ EURÓPSKA KOMISIA. *Ethics Guidelines for Trustworthy AI*. [online]. Dostupné z: https://ec.europa.eu/digital-strategy/our-policies/ethics-guidelines-trustworthy-ai_en [cit. 2025-09-27].

¹⁹ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Recommendation on Artificial Intelligence*. [online]. Dostupné z: <https://oecd.ai/principles/> [cit. 2025-09-27].

²⁰ UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. [online]. [cit. 2025-09-27]. Dostupné z: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>.

²¹ EURÓPSKA KOMISIA. *Návrh nariadenia Európskeho parlamentu a Rady o ustanovení právnych predpisov týkajúcich sa umelej inteligencie (Akt o umelej inteligencii)*. COM/2021/206 final. Brusel : Európska komisia, 2021. [cit. 2025-09-27].

²² VAN NOORDT, Colin, MEDAGLIA, Rony a TANGI, Luca. *Politické iniciatívy pre artific sociálnu inteligenciu vo vláde: Analýza národných stratégií v Európe*. Public Policy and Administration, 2025, 40(2), s. 220. DOI: 10.1177/09520767231198411. [cit. 2025-09-27].

- c) automatického zasielania výstrah dotknutým subjektom,
- d) elektronického spracovania údajov potrebných na podanie oznámenia o vzniku škody,
- e) predvyplnenia žiadosti o náhradu škody,
- f) prípravy návrhu rozhodnutia o vyplatení alebo nevyplatení náhrady škody.

Ministerstvo životného prostredia SR by pritom muselo zriadiť centrálny informačný systém náhrad škôd spôsobených určenými živočíchmi. Systém by pritom musel pracovať s dátovými vstupmi z monitorovacích zariadení (drony, senzory, fotopasce). Taktiež by mal viesť spracovať jednotný elektronický formulár na podanie oznámenia o vzniku škody, elektronickú prípravu a podanie žiadosti o náhradu škody. V poslednej fáze náhrady škody by mal systém viesť vypracovať návrh rozhodnutia o vyplatení alebo nevyplatení náhrady škody a výpočtom výšky náhrady škody. Do tohto ustanovenia by bolo vhodné aj zakomponovať odsek, ktorý by znel, že *výstupy zo systému za použitia UI majú iba odporúčací charakter. Rozhodnutie musí vždy schváliť človek. Využívanie UI nesmie obmedziť právo poškodeného na podanie odvolania alebo iného opravného prostriedku.*

Záver

Podľa štúdie Univerzity v Queenslande a spoločnosť KPMG, ktoré sa spojili na vypracovanie globálnej štúdie s cieľom pochopiť dôveru a postoje k umelej inteligencii výskum uvádza, že traja z piatich ľudí sú buď ambivalentní alebo nie sú ochotní dôverovať umelej inteligencii.²³ Táto štúdia skúmala správanie ľudí v 17 štátoch sveta. Môžeme predpokladať, že podobné výsledky by sme mohli očakávať aj vo výskume na Slovensku. Používanie UI pri rozhodovaní o právach a povinnostiach je v našej právnej úprave ešte len na svojom začiatku. No o to viac je dôležité rozprávať a vedecky pracovať s touto problematikou na akademickej úrovni. Príspevok priblížil vo svojej úvodnej časti aktuálnu právnu úpravu prostredníctvom dôkladnej analýzy. Dôležitou časťou je však práve nasledujúca **podkapitola s názvom** Akým spôsobom by sa dala využiť umelá inteligencia pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi? V tejto časti teoreticky približuje autorka príspevku možnosti využívania umelej inteligencie pri špecifickej právnej a správnej oblasti náhrady škôd spôsobovaných určenými živočíchmi. Autorka rozdelila proces náhrady takýchto škôd do piatich procesných fáz. Sú nimi vznik škody, oznámenie o vzniku škody, miestne zisťovanie, žiadosť o náhradu škody

²³ GILLESPIE, Nicole, LOCKEY, Steve, CURTIS, Caitlin a POOL, Javad. *Trust in Artificial Intelligence: A Global Study*. Brisbane: The University of Queensland & KPMG, 2023. 82 s. DOI: 10.14264/ood3c94. Dostupné z: https://ai.uq.edu.au/files/6161/Trust%20in%20AI%20Global%20Report_WEB.pdf.

a rozhodnutie o vyplatení alebo nevyplatení náhrady škody. V tejto časti nájde čitateľ aj detailne priblíženie možného využívania UI v jednotlivých fázach procesu náhrady škody. Samozrejme, že slovenská právna úprava momentálne neobsahuje žiadne ustanovenia o využívaní UI a nová právna úprava je ešte len v procese jej tvorby. Na európskej úrovni je vypracovaný základný dokument, ktorým je Nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá pre umelú inteligenciu (akt o umelej inteligencii). V poslednej časti príspevku sa autorka teda zaoberá princípmi a zásadami, ktoré musia byť dodržiavané pri procese rozhodovania o náhrade škody spôsobenej určenými živočíchmi, ako aj návrhom ustanovení *de lege ferenda*, týkajúcich sa najmä spomínaných procesných fáz náhrady škody.

V úvode si autorka položila vedeckú otázku na ktorú hľadala prostredníctvom vedeckých metód odpovede. A aká je teda odpoveď na stanovenú otázku? Zložitá. V podmienkach aktuálnej právnej úpravy nie je možné využívanie UI pri rozhodovaní o náhrade škody spôsobenej určenými živočíchmi. Ak by sa ale prijala právna úprava, ktorá by legislatívu na tomto úseku doplnila, bolo by využívanie UI pri takýchto rozhodnutiach veľmi prínosné. Na rozdiel od iných individuálnych správnych aktov je rozhodovanie o náhrade škody v podstate proces veľmi tabuľkový. Tým chceme povedať, že vyplácanie a výpočet náhrady škody je už dnes presne daný. Využívanie UI pri tomto procese náhrady škôd spôsobených živočíchmi, by mohlo zamestnancom okresných úradov významným spôsobom zjednodušiť a zefektívniť výkon ich práce.

Zoznam použitej literatúry

1. CEPEK, B. a kol. *Environmentálne právo: všeobecná a osobitná časť*. Plzeň: Aleš Čeněk, 2015. 442 s. ISBN 978-80-7380-560-9.
2. DAMOHORSKÝ, Milan a Petr ŠEDINA. *Ochrana bobra evropského v českém právu*. Acta Universitatis Carolinae. Iuridica. Praha : Univerzita Karlova, Právnická fakulta, 2015, roč. 61, č. 2, s. 51–58. ISSN 0323-0619.
3. GILLESPIE, Nicole, LOCKEY, Steve, CURTIS, Caitlin a POOL, Javad. *Trust in Artificial Intelligence: A Global Study*. Brisbane : The University of Queensland & KPMG, 2023. 82 s. DOI: 10.14264/00d3c94. Dostupné z: https://ai.uq.edu.au/files/6161/Trust%20in%20AI%20Global%20Report_WEB.pdf [cit. 2025-09-27].
4. MICHALOVIČ, Matúš a Michal MASLEN. Advocating for environmental law – grounds for its status as an independent branch of law in Slovak legal doctrine. *Prawne Problemy Górnictwa i Ochrony Środowiska*, 2024, č. 2, s. 1–26. DOI: 10.31261/PPGOS.2024.02.06.

5. RAKOCZY, Bartosz. *Odpowiedzialność skarbu państwa za szkody spowodowane przez zwierzęta na podstawie art. 126 ustawy o ochronie przyrody*. Acta Universitatis Carolinae – Iuridica, 2015, roč. 61, č. 2, s. 141–150. ISSN 0323-0619. [cit. 2025-09-27].
6. SUN, T. Q. a MEDAGLIA, R. *Mapovanie výziev umelej inteligencie vo verejnom sektore: dôkazy z verejného zdravotníctva*. Government Information Quarterly, 2019, 36(2), s. 368–383. ISSN 0740-624X. DOI: 10.1016/j.giq.2018.09.008. [cit. 2025-09-27].
7. VAN NOORDT, Colin, MEDAGLIA, Rony a TANGI, Luca. *Politické iniciatívy pre artific sociálnu inteligenciu vo vláde: Analýza národných stratégií v Európe*. Public Policy and Administration, 2025, 40(2), s. 215–253. ISSN 0952-0767, e-ISSN 1749-4192. DOI: 10.1177/09520767231198411. [cit. 2025-09-27].
8. VRABKO, M. a kol. *Správne právo hmotné. Všeobecná časť. 3. vyd.* Bratislava: C. H. Beck, 2025. 344 s. ISBN 978-80-8232-068-1.
9. VOMÁČKA, Vojtěch a Josef BÁRTŮ. *Damage caused by game and its compensation in Central European countries: A comparative perspective*. Central European Journal of Comparative Law [online]. 2023, 4(2), 183–199. ISSN 2732-9938. DOI: 10.47078/2023.2.123-141. [cit. 2025-09-27]. Dostupné z: <https://doi.org/10.47078/2023.2.123-141>.
10. *Zelenšie Slovensko. Stratégia environmentálnej politiky Slovenskej republiky do roku 2030*. Bratislava : Ministerstvo životného prostredia SR, 2019. 60 s. Dostupné z: https://www.minzp.sk/files/iep/03_vlastny_material_envirostrategia2030_def.pdf [cit. 2025-09-27].
11. *Oznámenie o vzniku škody*. Ministerstvo vnútra Slovenskej republiky [online]. Dostupné z: <https://www.minv.sk/?okresne-urady-klientske-centra&urad=32&odbor=10&subor=311212> [cit. 2025-09-27].
12. *Ako nahlásiť škody spôsobené určeným živočíchom?* Štátna ochrana prírody SR, 2018 [online]. Dostupné z: <https://www.sopsr.sk/web/?cl=20352> [cit. 2025-09-27].
13. *Zákon č. 115/2000 Sb., o poskytovaní náhrad škod spôsobených vybranými zvlášť chránenými živočíchmi*.
14. *Zákon č. 543/2002 Z. z. o ochrane prírody a krajiny v znení neskorších predpisov*.
15. *Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody*. (Dziennik Ustaw z 2024 r., poz. 1785).
16. *Vyhláška č. 462/2004 Z. z., ktorou sa ustanovujú podrobnosti o osobitných kvalifikačných predpokladoch na výkon niektorých činností na úseku starostlivosti o životné prostredie*.

17. *Legislatívny proces LP/2025/401*. [online]. Bratislava : Slov-Lex, 2025. Dostupné z: <https://www.slov-lex.sk/elegislativne-procesy/SK/LP/2025/401> [cit. 2025-09-27].
18. EURÓPSKA KOMISIA. *Návrh nariadenia Európskeho parlamentu a Rady o ustanovení právnych predpisov týkajúcich sa umelej inteligencie (Akt o umelej inteligencii)*. COM/2021/206 final. Brusel : Európska komisia, 2021. [cit. 2025-09-27].
19. EURÓPSKA KOMISIA. *Ethics Guidelines for Trustworthy AI*. [online]. Dostupné z: https://ec.europa.eu/digital-strategy/our-policies/ethics-guidelines-trustworthy-ai_en [cit. 2025-09-27].
20. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Recommendation on Artificial Intelligence*. [online]. Dostupné z: <https://oecd.ai/principles/> [cit. 2025-09-27].
21. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. [online]. Dostupné z: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> [cit. 2025-09-27].

Kontaktné údaje

Mgr. Viktória Sokolová

novotna92@uniba.sk

Právnická fakulta, Univerzita Komenského v Bratislave

VYUŽITIE UMELEJ INTELIGENCIE PRI VYBAVOVANÍ ŽIADOSTÍ O SLOBODNOM PRÍSTUPE K INFORMÁCIÁM

USING ARTIFICIAL INTELLIGENCE IN HANDLING FREEDOM OF INFORMATION REQUESTS

Lenka Hmírová¹

Abstrakt: AI (umelá inteligencia) nie je priamo spojená so slobodným prístupom k informáciám ako právnym konceptom, ale skôr s jeho využitím a spracovaním. Slobodný prístup k informáciám je legislatívna kategória upravujúca právo občanov na informácie od povinných osôb. AI je technológia, ktorá však môže pomôcť s analýzou a sprístupnením týchto informácií, ale aj vytvoriť nové informácie (napr. analýzy, prognózy), na ktoré sa právo na slobodný prístup nevzťahuje. Účelom príspevku a jeho obsahovým zameraním je načrtnúť možnosti využitia umelej inteligencie pri vybavovaní žiadostí o slobodnom prístupe k informáciám. Ako AI súvisí s agendou slobodného prístupu k informáciám? Jednak ako nástroj na spracovanie informácií. AI môže byť použitá na rýchlejšie a efektívnejšie spracovanie a sprístupnenie rozsiahlych súborov informácií, ktoré sú už v databázach. Ďalej môže poslúžiť pri tvorbe nových informácií. AI dokáže totiž generovať nové výstupy (napr. analýzy, prognózy, vysvetlenia). Tie nie sú ale automaticky predmetom práva na slobodný prístup k informáciám, pretože nie sú "k dispozícii" v pôvodnej forme. V neposlednom rade môže umelá inteligencia prispieť k zvyšovaniu efektivity. Pomocou AI môžu orgány verejnej moci zlepšiť spôsob, akým sú verejné informácie spracovávané a sprístupňované občanom, napríklad prostredníctvom sofistikovanejších vyhľadávacích nástrojov.

Kľúčové slová: základné právo na informácie, slobodný prístup k informáciám, umelá inteligencia, verejná správa, rozhodovanie vo verejnej správe

Abstract: AI (artificial intelligence) is not directly related to free access to information as a legal concept, but rather to its use and processing. Free access to information is a legislative category regulating the right of citizens to information from obligated persons. AI is a technology that can, however, help with the analysis and disclosure of this information, but also create new

¹ Katedra správneho a environmentálneho práva Právnickej fakulty Univerzity Komenského v Bratislave.

information (e.g. analyses, forecasts) that is not covered by the right to free access. The purpose of the contribution and its content focus is to outline the possibilities of using artificial intelligence in handling requests for free access to information. How does AI relate to the free access to information agenda? Firstly, as a tool for processing information. AI can be used to process and make available large sets of information that are already in databases and on the internet faster and more efficiently. It can also be used to create new information. AI can generate new outputs (e.g. analyses, forecasts, explanations). However, these are not automatically subject to the right to free access to information, because they are not "available" in their original form. Last but not least, artificial intelligence can contribute to increasing efficiency. With the help of AI, public authorities can improve the way in which public information is processed and made available to citizens, for example through more sophisticated search tools.

Key words: fundamental right to information, free access to information, artificial intelligence, public administration, decision-making in public administration

Úvod

Slobodný prístup k informáciám v kontexte umelej inteligencie nie je priamo definovaný v zákone č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov (ďalej len „ZoSI“). ZoSI sa vzťahuje primárne na informačné povinnosti povinných osôb, ktorými sú

štátne orgány, obce, vyššie územné celky, právnické osoby a fyzické osoby, ktorým zákon zveruje právomoc rozhodovať o právach a povinnostiach v oblasti verejnej správy, právnické osoby zriadené zákonom a právnické osoby zriadené štátnym orgánom, vyšším územným celkom alebo obcou, zdravotné poisťovne, ďalej aj právnické osoby, ak v nich povinné osoby majú samostatne alebo spoločne aspoň väčšinovú priamu alebo nepriamu účasť a kontrolu a aj mimovládne neziskové organizácie ustanovené zákonom a prípadne aj ďalšie právnické osoby alebo fyzické osoby podľa osobitného zákona.

V oblasti AI ide skôr o diskusie o otvorenom prístupe k dátam, modelom a algoritmom, o transparentnosti ich fungovania, o demokratizácii ich vývoja a používania, ako aj o etických a regulačných otázkach spojených s umelou inteligenciou a právom na informácie. ZoSI umožňuje občanom kontrolovať činnosť povinných osôb. V kontexte umelej inteligencie sa slobodný prístup k informáciám stáva dôležitou oblasťou pre jej rozvoj, pretože AI často potrebuje prístup k

rozsiahlym datasetom, modelom a algoritmom, pričom sa zároveň stretáva s otázkami etiky, ako aj právnymi otázkami týkajúcimi sa ochrany osobnosti, súkromia, duševného vlastníctva a osobných údajov a tiež aj aspektov možného zneužitia dát alebo vzniku škody spôsobenej nezákonným rozhodnutím alebo nesprávnym úradným postupom. Je potrebné nájsť rovnováhu medzi transparentnosťou a potrebnou právnou ochranou, teda aby boli dáta dostupné v zrozumiteľnej forme a aby boli zároveň jasne definované pravidlá ich využívania. Takýto prístup totiž umožní zabezpečiť v praxi vybudovanie dôvery a zodpovedné využívanie AI.

V súvislosti s pojmami umelá inteligencia a slobodný prístup k informáciám je dôležité rozlišovať dva obsahové kontexty. Jedným je ústavné právo občana na prístup k informáciám podľa ZoSI a druhým je prístup k informáciám generovaným alebo spracovaným AI. ZoSI zaručuje právo získať informácie od povinných osôb, ale nevzťahuje sa na všetky typy informácií v kontexte zákonných obmedzení prístupu k informáciám (napr. ochrana utajovaných skutočností, limitovaná informácia, bankové tajomstvo, daňové tajomstvo, obchodné tajomstvo, ochrana osobnosti a osobných údajov, ochrana pred ujmom v hospodárskej súťaži). Prístup k dátam, modelom a algoritmom AI je komplexnejšia otázka, ktorá závisí od toho, či sú dáta verejne dostupné, na aký účel boli zozbierané a či nie sú chránené v medziach tzv. zákonných licencií a podmienok obmedzenia prístupu k informáciám podľa § 8 až § 13 ZoSI. Téma je predmetom odborných diskusií a vedeckého bádania či už z pohľadu etiky, práva, bezpečnosti, ale aj monopolizácie na trhu vrátane ochrany práv duševného vlastníctva a práv priemyselného vlastníctva.

Vymedzenie umelej inteligencie vo vede a v legislatíve

„V minulosti sa výskumníci zaoberali viacerými rôznymi verziami umelej inteligencie (artificial intelligence, AI). Niektorí definovali inteligenciu podľa podobnosti k úrovni ľudských schopností, zatiaľ čo iní uprednostňujú abstraktnú, formálnu definíciu inteligencie nazývanú racionalita, teda voľne povedané, konanie "správnych vecí". Samotný predmet sa tiež líši.“²

Niektorí považujú inteligenciu za vlastnosť vnútorných myšlienkových procesov a uvažovania, zatiaľ čo iní sa zameriavajú na inteligentné *správanie*, vonkajšiu charakteristiku.³

² MESARČÍK, M., GYURÁSZ, Z. a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 1, ISBN: 978-80-7160-715-1.

³ RUSSELL, S., NORVIG, P.: Artificial Intelligence: A Modern Approach (4th Edition). Pearson 2020, s. 669, ISBN 9780134610993.

Podľa iných autorov je AI odvetvie informatiky, ktoré sa zaoberá vytváraním algoritmov a systémov schopných vykonávať úlohy, ktoré by obvykle vyžadovali ľudskú inteligenciu.⁴

Podľa vedeckej doktríny neexistuje jednotne uznávaná definícia AI. Definícia pojmu AI nie je vymedzená ani ako terminus technicus v oblasti umelej inteligencie ako vedeckej disciplíny a ani v oblasti právnej regulácie neexistuje legálna definícia AI. Z dôvodu nejestvujúcej jednotnej definície by sa pojem „AI“ nemal používať v právnych predpisoch regulačnej povahy. Absencia jeho legálnej definície môže totiž znejasniť predmet a účel dotknutej právnej úpravy, ako aj jej samotný obsah.

Podľa čl. 3 ods. 1 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) č. 2018/858, (EÚ) č. 2018/1139 a (EÚ) č. 2019/2144, smernice č. 2014/90/EÚ, smernice č. 2016/797/EÚ a smernice č. 2020/1828/EÚ (ďalej len „AIA“), ktorý obsahuje len definíciu pojmu „systém AI“ je „systém AI“ *„strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie.“*

Pojem „model AI na všeobecné účely“ je definovaný v čl. 3 ods. 63 AIA ako *„model AI, a to aj model AI trénovaný veľkým množstvom údajov s použitím samokontroly vo veľkom rozsahu, ktorý má významnú všeobecnú povahu a je schopný kompetentne vykonávať širokú škálu odlišných úloh bez ohľadu na spôsob, akým sa model uvádza na trh, a ktorý možno integrovať do rôznych nadväzujúcich systémov alebo aplikácií, s výnimkou modelov AI, ktoré sa využívajú na účely výskumných, vývojových a prototypových činností pred ich uvedením na trh.“*

Na základe aktuálnych vedeckých poznatkov možno AI definovať na základe rôznych klasifikačných kritérií.

1. AI môžeme z technického hľadiska definovať ako:

- 1.1 strojovú inteligenciu tvoriacu pododvetvie počítačovej vedy,
- 1.2 technológiu, softvér aplikovaný v počítačových systémoch, ktoré sú spôsobilé fungovať spôsobom podobným ľudskej inteligencie; v dôsledku toho takéto počítačové systémy rozumejú ľudskej reči, sú schopné riešiť problémy, učiť sa z nadobudnutých skúseností, adaptovať sa, seba klasifikovať a zlepšovať,
- 1.3 stroj, ktorý je spôsobilý vykonať úlohy, ktoré pokiaľ by boli vykonávané ľuďmi by vyžadovali inteligenciu,

⁴ ŠTĚDRŮ, B., JAŠEK, R., SVÍTEK, M. a kol. Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024, s. 13, ISBN-978-80-7380-947-8.

- 1.4 koncepcia strojov, ktoré technológiami AI sledujú dosiahnutie určitého cieľa.⁵
2. AI môžeme definovať z pohľadu informačných a komunikačných technológií ako:
- 2.1 schopnosť digitálneho počítača alebo počítačom riadeného robota vykonávať úlohy bežne spojené s inteligentnými bytosťami,
 - 2.2 teóriu a vývoj počítačových systémov schopných plniť úlohy, ktoré si obvykle vyžadujú ľudskú inteligenciu, ako je vizuálne vnímanie, rozpoznávanie reči, rozhodovanie a preklad medzi jazykmi,
 - 2.3 program, ktorý si v ľubovoľnom svete dokáže poradiť s úlohami nie horšie ako človek.⁶
3. AI môžeme definovať tiež v kontexte využívania poznatkov z iných vedných odborov (napr. matematika, logika, štatistika, informatika), v rámci ktorých sa vychádza pri definovaní AI zo štyroch kategórií podľa toho, na akom princípe AI pracuje, respektíve o čo sa AI snaží ako vedeckú multidisciplínu alebo určité procesy alebo schopnosti, ktorými disponujú alebo ich vykonávajú počítače, respektíve ich softvér takto:
- 3.1 AI sa snaží myslieť ako ľudia „*think like humans, thinking humanly*“,
 - 3.2 AI sa snaží konať ako ľudia „*act like humans, acting humanly*“,
 - 3.3 AI sa snaží myslieť racionálne „*think rationally, thinking rationally*“,
 - 3.4 AI sa snaží konať racionálne „*act rationally, acting rationally*“.⁷
- Existujú dve široké triedy systémov AI na základe ich schopností, a to: prediktívna AI (PredAI) a generatívna AI (GenAI). Predikatívna AI sa využíva v počítačovom videní na detekciu a klasifikáciu objektov. Generatívna AI je neoddeliteľnou súčasťou jazykových modelov, avšak zďaleka to nie je jediná doména generatívnej AI.⁸
- Pri právnej úprave a právnej regulácii AI a jej používania je potrebné zohľadňovať premisu, podľa ktorej „*samotná regulácia AI nie je účelom, ale prostriedkom*“.⁹ Právne aspekty AI sa stali nosnou časťou výskumov až začiatkom posledného desaťročia. Najdiskutovanejšími témami sa stali: a) právna subjektivita, b) zodpovednosť, c) transparentnosť, d) ochrana (osobných) údajov, e) ochrana súkromia, f) práva duševného vlastníctva, g) práva priemyselného vlastníctva a h) možnosť regulácie

⁵ KLUČKA, J., Medzinárodné právo, umelá inteligencia a vice versa, Časopis pro právní vědu a praxi, XXIX, 3/2021, s. 553-555.

⁶ ANDRAŠKO, J. a kol., Právo informačných a komunikačných technológií 2, Bratislava: TINCT, 2021, s. 283.

⁷ VOJTUŠ, F., KORDÍK, M., DRAŽOVÁ, P., Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia, časopis Právnik 6/2023, s. 551-552.

⁸ VASSILEV, A. a kol., *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artificial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023. s. 3. 2024. Dostupné na: <https://doi.org/10.6028/NIST.AI.100-2e2023>.

⁹ ANDRAŠKO, J. a kol., Právo informačných a komunikačných technológií 2, Bratislava: TINCT, 2021, s. 288.

zariadení spracúvajúcich (osobné) údaje ako výrobkov a nosičov softvéru najmä z pohľadu ústavnosti, kybernetickej bezpečnosti a technickej normalizácie.¹⁰

Zaujímavou je aj otázka zodpovednosti za vady alebo škodu spôsobenú prevádzkovaním zariadení AI ako výrobku a softvéru a nevynímajúc ani zodpovednosť štátu za škodu spôsobenú pri výkone verejnej moci alebo nesprávnym úradným postupom podľa zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov v znení neskorších predpisov. Citovaný zákon vychádza síce z ústavnoprávnej úpravy, konkrétne čl. 46 ods. 3 Ústavy Slovenskej republiky,¹¹ podľa ktorého má každý právo na náhradu škody spôsobenej nezákonným rozhodnutím súdu, iného orgánu či orgánu verejnej správy alebo nesprávneho úradného postupu. Avšak nejde o „komplexné poňatie verejnej moci, pretože vymedzenie pojmu verejná moc je zamerané iba na tie prípady, keď orgán verejnej moci rozhoduje o individuálnych právach a povinnostiach v právno-aplikačnom procese a obchádza normotvorbu, riadiacu a organizátorskú činnosť, postup pri uzatváraní verejnoprávných zmlúv, uskutočňovanie rôznych bezprostredných zázkrokov a iných opatrení obdobnej povahy.“¹²

V súčasnosti nie je AI a jej používanie v právnom poriadku Slovenskej republiky upravené žiadnym všeobecne záväzným právnym predpisom ustanoveným v § 1 ods. 1 zákona č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Aktuálne jediným všeobecne záväzným právnym predpisom, ktorý používa pojem „AI“ je vyhláška Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky č. 244/2019 Z. z. o sústave študijných odborov Slovenskej republiky v znení vyhlášky Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky č. 26/2023 Z. z., ktorou sa mení a dopĺňa vyhláška Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky č. 244/2019 Z. z. o sústave študijných odborov Slovenskej republiky. Citovaná vyhláška terminologicky používa pojem „AI“ len v prílohe č. 1, a to v súvislosti s určením obsahu študijných odborov, v ktorých môžu vysoké školy v Slovenskej republike poskytovať vysokoškolské vzdelávanie, a to v študijných odboroch Informatika a Kybernetika.

Jediným právnym aktom upravujúcim problematiku AI v Slovenskej republike je AIA ako sekundárny legislatívny právny akt (prameň práva) Európskej únie (pozri čl. 288 prvú a druhú alineu a čl. 297 ods. 1 a ods. 2 prvú alineu Zmluvy o fungovaní Európskej

¹⁰ MESARČÍK, M., GYURÁSZ, Z. a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 103, ISBN: 978-80-7160-715-1.

¹¹ SVÁK, J. In. OROSZ, L., SVÁK, J. a kol. Ústava Slovenskej republiky. Komentár. 1. zväzok (základné princípy a ľudské práva). Bratislava : Wolters Kluwer, 2021, s. 623 – 625.

¹² ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. In. Mílniky práva v stredoeurópskom priestore 2008. Bratislava : VO PraF UK, 2008, s. 651 a nasledujúce.

únie). AIA bol uverejnený v Úradnom vestníku Európskej únie 12. júla 2024 (Ú. v. EÚ L, 2024/1689, 12.7.2024). AIA nadobudol účinnosť 1. augusta 2024 a bude sa uplatňovať od 2. augusta 2026, avšak niektoré jeho kapitoly a články sa uplatňujú postupne od 2. februára 2025, 2. augusta 2025, resp. od 2. augusta 2027 (pozri čl. 113). AIA má všeobecnú platnosť, je záväzný v celom rozsahu a priamo uplatniteľný vo všetkých členských štátoch. AIA sa stal súčasťou právneho poriadku Slovenskej republiky dňom jeho uverejnenia v Úradnom vestníku Európskej únie (12. júla 2024) a má prednosť pred zákonmi Slovenskej republiky (pozri čl. 7 ods. 2 druhú vetu Ústavy Slovenskej republiky). AIA ako sekundárny legislatívny právny akt (prameň práva) Európskej únie môže byť predmetom výkladu len zo strany Súdneho dvora Európskej únie v prejudiciálnom konaní podľa čl. 267 prvej aliney písm. a) a ods. 2 Zmluvy o fungovaní Európskej únie. V súvislosti s aplikáciou AIA v Slovenskej republike sa uplatňuje *zásada prednosti práva Európskej únie*.

Základná filozofia AIA ustanovuje týchto šesť konkrétnych dôvodov pre prijatie AIA na úrovni Európskej únie, ktoré sú relevantné aj vo vzťahu k ZoSI, a to:

1. využívanie AI predstavuje zvýšené riziko pre bezpečnosť jednotlivcov,
2. využívanie AI predstavuje zvýšené riziko porušovania základných práv a slobôd,
3. dozorné orgány nemajú právomoci, procesné rámce a zdroje na zabezpečenie a monitorovanie súladu vývoja a používania umelej inteligencie s platnými pravidlami,
4. právna neistota ohľadom uplatnenia súčasného právneho rámca na systémy AI,
5. nedôvera k AI by znížila inovatívnosť a konkurencieschopnosť Európskej únie v globálnom meradle,
6. fragmentované opatrenia predstavujú prekážky pre ďalší vývoj jednotného digitálneho trhu a suverenity.¹³

Podľa čl. 1 AIA je cieľom harmonizovať pravidlá systémov AI pri uvádzaní a používaní v EÚ, zakázať určité systémy AI, upraviť špecifické požiadavky pre vysokorizikové systémy AI, zakotviť požiadavky transparentnosti pre špecifické systémy AI a harmonizovať pravidlá dohľadu a monitorovania trhu.

AIA je horizontálna regulácia založená na skúmaní rizika. V praxi to znamená, že vymedzuje systémy AI v kontexte rôznych typov rizík pre základné ľudské práva a slobody¹⁴ a následne upravuje špecifické právne požiadavky pre tieto systémy v danej

¹³ EURÓPSKA KOMISIA. *Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

¹⁴ Napríklad AIA, recitál 15: „Využívanie umelej inteligencie má síce mnoho výhod, túto technológiu však možno zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky v oblasti sociálnej kontroly. Takéto praktiky sú mimoriadne škodlivé a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej

kategórii. AIA rozlišuje systémy AI, ktoré predstavujú a sú relevantné aj pre agendu slobodného prístupu k informáciám ako ústavného práva podľa čl. 26 Ústavy Slovenskej republiky v nadväznosti aj na čl. 46 Ústavy Slovenskej republiky, ktorý upravuje ústavné právo na súdnu inú právnu ochranu:

1. neakceptovateľné riziko (zakázané praktiky),
2. vysoké riziko,
3. nízke riziko,
4. žiadne riziko.

Možnosti využitia AI v agende slobodného prístupu k informáciám z pohľadu povinných osôb a žiadateľov o informácie

Niektorí autori načrtli potenciál využitia umelej inteligencie pri vybavovaní žiadostí o informácie najmä pri automatizácii procesov, formulovaní textu odpovedí či rozhodnutí o nesprístupnení informácie a podpore rozhodovacieho procesu.¹⁵

Kľúčové aspekty slobody informácií v kontexte AI z pohľadu povinných osôb a žiadateľov o informácie sú:

1. AI systém ako nástroj na vyhľadávanie, filtrovanie, spracovanie a sprístupnenie informácií. AI datasety, modely a algoritmy môžu byť použité na rýchlejšie a efektívnejšie vyhľadávanie, filtrovanie, spracovanie a sprístupnenie rozsiahlych súborov informácií, ktoré sú už v databázach prípadne na internete (napr. povinné zverejňovanie informácií podľa § 5 ZoSI, povinne zverejňované zmluvy v Centrálnom registri zmlúv podľa § 5a ZoSI, informačné systémy verejnej správy, objednávky a faktúry za tovary, služby a práce zverejnené na webovom sídle povinných osôb, ak ho majú zriadené podľa § 5b ZoSI, odkaz na zverejnenú informáciu podľa § 7 ZoSI, opakované použitie informácií podľa § 21b až § 21l ZoSI).
2. AI systém ako tvorca nových informácií. AI datasety, modely a algoritmy dokážu totiž generovať nové výstupy (napr. výkladové stanoviská, rozbor, analýzy, referáty, prognózy). Avšak hoci podľa § 3 ods. 1 ZoSI má každý právo na prístup k informáciám, ktoré majú povinné osoby k dispozícii, tak právo na prístup k informáciám sa nevzťahuje na informácie, ktoré nie sú k dispozícii, najmä na vytváranie výkladových stanovísk, rozborov, analýz, referátov, odborných stanovísk, politických stanovísk, prognóz a výkladov právnych predpisov a na vytváranie názorov. Citované informácie nie sú totiž podľa § 3 ods. 1 ZoSI „k dispozícii“ u povinných osôb v pôvodnej forme.

dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv Únie vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa. "

¹⁵ JÄGER, P. kol. Svobodný přístup k informacím. Zákon č. 106/1999 Sb. Plzeň : Aleš Čeněk, 2025, 258 s., s. 195 a nasledujúce. ISBN 978-80-7380-964-5.

3. AI systém ako nástroj na zvyšovanie efektivity. Pomocou AI datasetov, modelov a algoritmov môžu povinné osoby zlepšiť spôsob, akým sú verejné informácie spracovávané a sprístupňované občanom prostredníctvom sofistikovanejších vyhľadávacích nástrojov nastavených na tréningové údaje, strojové učenie, hĺbkové učenie, stratové funkcie, tréningové algoritmy a gradientový zostup, hlboké neurónové siete, spracovanie prirodzeného jazyka, počítačové videnie, robotiku, prediktívnu a generatívnu umelú inteligencia, odporúčacie systémy, kolaboratívne filtrovanie, explicitnú a implicitnú spätnú väzbu, veľké jazykové modely.¹⁶

4. AI systém ako nástroj na automatizáciu procesov. Prostredníctvom AI datasetov, modelov a algoritmov môžu povinné osoby zjednodušiť a zjednotiť procesy v rámci konania o sprístupňovaní informácií na žiadosť podľa § 14 až § 21 ZoSI (napr. jednotný formulár žiadosti o sprístupnenie informácií, štandardizované vzory rozhodnutia o čiastočnom sprístupnení informácie, rozhodnutia o nesprístupnení informácie a fiktívneho rozhodnutia, triedenie žiadostí o informácie, sledovanie zákonných lehôt, posudzovanie formálnych náležitostí jednotlivých žiadostí o informácie, identifikácia kľúčových slov, predbežné vyhodnotenie obsahu žiadosti o informácie, anonymizovanie osobných údajov alebo údajov podliehajúcich zákonným licenciám obmedzujúcich právo na informácie, evidencia žiadostí o informácie, formulovanie textu odpovedí alebo rozhodnutia o čiastočnom sprístupnení informácie a rozhodnutia o nesprístupnení informácie, vyznačovanie vybavených žiadostí v spise).

5. AI systém ako pomocník a sprievodca občana. AI nástroje môžu pomôcť občanom pri príprave a formulácii žiadosti o sprístupnenie informácie, čím sa zvýši ich úspešnosť.

Quo vadis systémy AI a slobodný prístup k informáciám

Nasadzovanie AI do vysoko regulovaných sektorov, ktorým je aj verejná správa prináša nové výzvy v oblasti ochrany základných práv a slobôd. Práve preto zavádza AIA povinnosť vykonať hodnotenie vplyvu na základné práva a slobody (FRIA) pri využívaní vysokorizikových systémov AI. Tento proces má zabezpečiť, že umelá inteligencia funguje v súlade s princípmi demokracie, právneho štátu a ochrany jednotlivcov. Aj napriek uvedenému otvára téma systémov AI a slobodného prístupu k informáciám aj tieto otázky:

1. Aké systémy AI sa aktuálne používajú v rámci rozhodovacích procesov vo verejnej správe pri sprístupňovaní informácií v rámci členských štátov Európskej únie?
2. Aké sú legislatívne podmienky a procesné postupy na používanie týchto systémov AI pri sprístupňovaní informácií?

¹⁶ MESARČÍK, M., GYURÁSZ, Z. a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 7 a nasledujúce, ISBN: 978-80-7160-715-1.

3. Akým spôsobom sa pri používaní systémov AI zabezpečuje ochrana práva na informácie ako jedného zo základných práv a slobôd a splnenie podmienok dôveryhodnosti, etickosti a transparentnosti takéhoto postupu?

4. Do pôsobnosti akých orgánov verejnej moci patrí nasadzovanie systémov AI a kontrola ich používania pri sprístupňovaní informácií?

5. Aké sú pozitíva a negatíva (riziká) v prípade použitia systémov AI na účely sprístupňovania informácií povinnými osobami?

Medzi pozitíva systémov AI použitých v agende slobodného prístupu k informáciám možno už v súčasnosti považovať: a) rýchlosť vyhľadávania, filtrovania a spracovanie množstva informácií, b) objektívna analýza dát bez predsudkov, c) identifikácia vzorcov a vzájomných súvislostí a d) podpora rozhodovania. Medzi negatíva (riziká) systémov AI použitých pri vybavovaní žiadosti o sprístupnenie informácie patria: a) hypertrofia povinných osôb, b) mega obsiahlosť a rôznorodosť skutkových podstat a životných situácií, ktoré riešia povinné osoby pri sprístupňovaní informácií vrátane používaných informačných systémov dosiaľ vzájomne neprepojených aj napriek digitalizácii vo verejnej správe, c) nepriehľadnosť, zložitost' a nezrozumiteľnosť AI datasetov, modelov a algoritmov, d) závislosť systémov AI na kvalite vstupných dát a informácií a e) etické a právne dilemy, ak by sa systémy AI používali bez ľudskej kontroly.

Záver

1. AIA ako sekundárny právny akt práva EÚ s priamym účinkom a zásadou prednosti pred vnútroštátnym právom obsahuje komplexnú hmotnoprávnú úpravu používania AI v Slovenskej republike.

2. AIA upravuje požiadavky a podmienky na používanie AI orgánmi verejnej správy aj na účely rozhodovacích procesov vo verejnej správe, avšak vzhľadom na zaužívanú prax bude aj v Slovenskej republike žiaduca pravdepodobne novelizácia Správneho poriadku prípadne aj ďalších procesných predpisov a zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov v znení neskorších predpisov.

3. V rozhodovacích procesoch v oblasti slobodného prístupu k informáciám je možné z hľadiska typu používať dva systémy AI, a to vysokorizikový systém AI a systém AI, ktorý nie je považovaný za vysokorizikový. Systém AI, ktorý nie je považovaný za vysokorizikový, je systém AI určený na: a) vykonávanie úzko vymedzenej procedurálnej úlohy alebo b) systém AI určený na zlepšenie výsledku predtým dokončenej ľudskej činnosti alebo c) systém AI určený na zisťovanie vzorcov rozhodovania alebo odchýlok od vzorcov predchádzajúceho rozhodovania a nie je určený na to, aby bez riadneho ľudského preskúmania nahradil alebo ovplyvnil predtým dokončené ľudské posúdenie alebo d) systém AI určený na vykonávanie

prípravnej úlohy v oblasti využitia vysokorizikovej AI na účely presadzovania práva podľa čl. 6 ods. 3 AIA.

4. Používanie vysokorizikového systému AI v agende slobodného prístupu k informáciám musí byť povolené podľa právnych predpisov Európskej únie a aktuálne žiadny právny akt Európskej únie ani vnútroštátny právny predpis neustanovujú konkrétny postup povinnej osoby pri používaní vysokorizikovej AI v oblasti slobodného prístupu k informáciám (napr. pri posudzovaní obmedzení prístupu k informáciám).

5. Používanie vysokorizikového systému AI v agende slobodného prístupu k informáciám je možné len vtedy, ak sú splnené objektívne podmienky ustanovené v § 8 až § 13 ZoSI a technické požiadavky na bezpečnosť informačných systémov prípadne aj kybernetickú bezpečnosť podľa § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, prílohy č. 2 vyhlášky Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach, § 31 písm. j) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a § 3 ods. 4 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

6. Používanie vysokorizikového systému AI na úseku slobodného prístupu k informáciám je možné len vtedy, ak subjekt nasadzujúci do používania taký systém spĺňa podmienky ustanovené v čl. 26 AIA a ide o systém registrovaný v databáze Európskej únie.

7. Používanie vysokorizikového systému AI v rámci rozhodovacích procesov vo verejnej správe ohľadom sprístupňovania informácií na žiadosť je možné len vtedy, ak systém spĺňa podmienky dôveryhodnosti, etickosti a transparentnosti.

8. Na základe aktuálnych vedecko-technických poznatkov by v rámci rozhodovacích procesov vo verejnej správe vo veci sprístupňovania informácií na žiadosť bolo možné však nasadiť také systémy AI, ktoré nevykazujú žiadne riziko a sú vyvinuté ako generatívna AI, teda také, ktoré sú po zadaní textového pokynu používateľom určené na generovanie (vytvorenie) nového obsahu (výstupu) vo forme písaného textu, zvuku, obrázkov, zdrojového kódu alebo obrazovo-zvukového záznamu, pričom vygenerovaný výstup je jedinečný a k používaniu takýchto systémov AI by bolo potrebné pozitívne stanovisko Úradu na ochranu osobných údajov Slovenskej republiky a Stálej komisie pre etiku a reguláciu umelej inteligencie (CERAI).

9. Z pohľadu hypertrofie povinných osôb je preferované centrálné (spoločné, súčasné) používanie systémov AI na úseku slobodného prístupu k informáciám všetkými povinnými osobami.

10. Zachovanie ľudskej kontroly pri vybavovaní žiadostí týkajúcich sa slobodného prístupu k informáciám (napr. posudzovanie zákonných licencií obmedzenia prístupu k informáciám, odvolania, rozklady, fiktívne rozhodnutia) v súvislosti s budúcim používaním systémov AI je nevyhnutné pre to, aby táto technológia slúžila verejnému záujmu, chránila základné práva a slobody, podporovala spravodlivosť a rovnosť, interpretovala výsledky činnosti týchto systémov v súlade s právom, judikatúrou a ďalšími výstupmi aplikačnej praxe a akademickej obce a pre morálny úsudok vo vzťahu k prijatým rozhodnutiam.

Pokiaľ ide o aspekty používania AI či už občanmi alebo povinnými osobami pro futuro, tak pri využívaní systémov AI je nevyhnutné rešpektovať tieto komponenty: a) dôvera, b) transparentnosť, c) etika a zodpovednosť, d) právna regulácia AI a e) odborná príprava a praktický výcvik na používanie AI. Zastávame názor, že systémy AI môžu slúžiť len ako podpora rozhodovacieho procesu vo verejnej správe pre povinné osoby a akékoľvek rozhodnutie nimi vydané v konaní o sprístupnení/čiasťočnom sprístupnení/nesprístupnení informácie na žiadosť, musí byť výsledkom ľudskej činnosti, prejavom ľudskej autonómie a prieskumu súdom alebo iným orgánom.

Zoznam použitej literatúry

Knižné publikácie

1. ANDRAŠKO, J. a kol., Právo informačných a komunikačných technológií 2. Bratislava: TINCT, 2021, 234 s. ISBN 9788097383725.
2. JÄGER, P. kol. Svobodný přístup k informacím. Zákon č. 106/1999 Sb. Plzeň: Aleš Čeněk, 2025, 258 s. ISBN 978-80-7380-964-5.
3. MESARČÍK, M., GYURÁSZ, Z. a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, 244 s. ISBN: 978-80-7160-715-1.
4. RUSSELL, S., NORVIG, P.: Artificial Intelligence: A Modern Approach (4th Edition). Pearson 2020, s. 669, ISBN 9780134610993.
5. ŠTĚDRŮŇ, B., JAŠEK, R., SVÍTEK, M. a kol.: Umělá inteligencia a právo. Plzeň: Aleš Čeněk, 2024, 233 s. ISBN-978-80-7380-947-8.

Príspevky v neperiodických publikáciách (príspevky, kapitoly) a zborníky

1. SVÁK, J. In. OROSZ, L., SVÁK, J. a kol. Ústava Slovenskej republiky. Komentár. 1. zväzok (základné princípy a ľudské práva). Bratislava: Wolters Kluwer, 2021, s. 623 – 625. ISBN 978-80-571-0381-3.
2. ŠKROBÁK, J. Kategória verejnej moci a jej význam vo verejnej správe a vo vede správneho práva. In. Míľníky práva v stredoeurópskom priestore 2008. Bratislava : VO PraF UK, 2008, s. 651 a nasledujúce.

Články v periodickej tlači (časopisecké články)

1. KLUČKA, J. - Medzinárodné právo, umelá inteligencia a vice versa, Časopis pro právní vědu a praxi, XXIX, 3/2021, s. 553-555.
2. VOJTUŠ, F., KORDÍK, M., DRAŽOVÁ, P. - Umelá inteligencia, jej využívanie a trestnoprávna zodpovednosť – výzvy, problémy a možné riešenia, časopis Právnik 6/2023, s. 551-552.

Iné zdroje

1. EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.
2. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) č. 2018/858, (EÚ) č. 2018/1139 a (EÚ) č. 2019/2144, smernice č. 2014/90/EÚ, smernice č. 2016/797/EÚ a smernice č. 2020/1828/EÚ.
3. VASSILEV, A., a kol. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artificial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023. s. 3. 2024. Dostupné na: <https://doi.org/10.6028/NIST.AI.100-2e2023>.
4. Zákon č. 211/2000 Z.z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

Kontaktné údaje

JUDr. Mgr. Lenka Hmírová, RSc.

hmirova5@uniba.sk

Katedra správneho a environmentálneho práva Právnickej fakulty Univerzity Komenského v Bratislave

DOSTATKY DIGITÁLNÍ KOMUNIKACE S VEŘEJNOPRÁVNÍM PRVKEM

DEFICIENCIES OF DIGITAL COMMUNICATION WITH A PUBLIC-LAW ELEMENT

Sandra Konečná¹

Abstrakt: Tento příspěvek publikuje výsledky projektu „Nedostatky digitální komunikace s veřejnoprávním prvkem“ vedeného pod záštitou Právnické fakulty Univerzity Palackého v Olomouci. Stěžejním problémem je fikce podpisu při užívání datových schránek právníckými osobami, která je nekonzistentní s nařízením eIDAS a způsobuje právní nejistotu, neboť oprávnění jednat bývá přičítáno bez jasné identifikace fyzické osoby. Další právní nedostatky datových schránek představuje směšování soukromoprávních a veřejnoprávních úkonů, např. u obcí, a rovněž absence rozlišení hmotněprávní nebo procesněprávní povahy jednání. Mezi systémové nedostatky digitální veřejnoprávní komunikace patří nedostatečná autentizace jednající soukromoprávní osoby, roztržitost komunikačních portálů a chybějící centrální přehled požadavků občana, což vede k nedostatečné transparentnosti. Kritizován je i "lidský faktor" neochoty ve veřejné správě a omezení asistované služby pro digitálně slabé jedince. Navrhovány jsou legislativní změny, adaptace na eIDAS 2.0 a jednotné řízení digitalizace pro zajištění jasnějšího právního rámce.

Klíčová slova: digitální komunikace, veřejná správa, datové schránky, autentizace, autorizace, eGovernment ČR

Abstract: This paper publishes the results of the project "Deficiencies of Digital Communication with a Public Law Element" led under the Faculty of Law, Palacký University in Olomouc. The main problem is the fiction of signature when legal entities use data boxes, which is inconsistent with the eIDAS regulation and causes legal uncertainty, as the authority to act is often attributed without clear identification of the physical person. Further legal shortcomings of data boxes include the mixing of private law and public law acts, for example by municipalities, and also the absence of distinguishing between the substantive law or procedural law nature of the act. Systemic

¹ Univerzita Palackého v Olomouci, Právnická fakulta, Institut pro právo a pokročilé technologie

shortcomings of digital public law communication include inadequate authentication of the acting private law person, the fragmentation of communication portals, and the missing central overview of citizen requests, which leads to insufficient transparency. The "human factor" of reluctance in public administration and the limitations of assisted service for digitally vulnerable individuals are also criticized. Legislative changes, adaptation to eIDAS 2.0, and unified management of digitalization are proposed to ensure a clearer legal framework

Key words: digital communication, public administration, data boxes, authentication, authorization, eGovernment of the Czech Republic

Úvod

Tento článek si klade za cíl seznámit čtenáři s provedenou analýzou digitální komunikace veřejné správy v České republice a popsat klíčové právní a systémové bariéry, které narušují principy řádné správy. Závěrem autorka formuluje konkrétní doporučení a možnosti využití moderních technologií, včetně umělé inteligence, k nápravě těchto zjištěných nedostatků.

Principy řádné správy a požadavky na digitální komunikaci

Dodržování principů řádné správy a splnění specifických požadavků na digitální komunikační kanály je základním stavebním kamenem pro budování důvěry lidí v e-Government. Nejedná se pouze o technickou funkčnost, ale především o kvalitu služeb poskytovaných jejich adresátům.

Principy dobré správy v digitální sféře vyžadují, aby veškeré jednání veřejné správy, včetně provozu digitálních služeb, striktně probíhalo v souladu s platným právním řádem (princip zákonnosti). Digitální systémy musí zajistit, že ke všem uživatelům bude přistupováno stejně, bez jakékoli formy diskriminace (principy nestrannosti a rovného zacházení). Zároveň se očekává, že služby budou rychlé a efektivní, eliminují průtahy a minimalizují administrativní zátěž (principy rychlého vyřízení věci a efektivity).² Uživatelé musí legitimně očekávat konzistentní fungování digitálních služeb a stabilní rozhodovací praxi (princip předvídatelnosti).³ Informace a pokyny

² *Služební předpis nejvyššího státního tajemníka č. 3 ze dne 3. října 2023 o pravidlech etiky státních zaměstnanců.* Online. In: MINISTERSTVO VNITRA. Ministerstvo vnitra. 2023. Dostupné z: file:///C:/Users/uzivatel/Downloads/Sluzebni_predpis_a_oduvodneni_v_grafickem_zpracovani_-_20231013.pdf. [cit. 2025-09-25].

³ MINISTERSTVO VNITRA. *Etický kodex úředníků a zaměstnanců veřejné správy.* Online. Český úřad pro zkoušení zbraní a střeliva. 2014. Dostupné

musí být přesvědčivé, srozumitelné a psané jednoduchým jazykem, aby uživatelé nebyli uvedeni v omyl. Veřejná správa smí digitálně vyžadovat pouze nezbytně nutné údaje (princip přiměřenosti), přičemž orgány veřejné moci musí nést odpovědnost za funkčnost a bezpečnost systémů a aktivně přijímat nápravná opatření.⁴ Digitální prostředí by mělo zvyšovat otevřenost a transparentnost fungování správy, například snadným přístupem k informacím.⁵ I v tomto prostředí se musí projevovat vstřícnost a ochota pomoci, což zahrnuje kvalitní uživatelskou podporu.

Klíčové požadavky na digitální komunikační kanály veřejné správy jsou rozděleny do několika kritérií.

Základem je Přístupnost, která zajišťuje, že internetové stránky a aplikace jsou vnímatelné, ovladatelné a stabilní pro všechny uživatele, včetně osob se zdravotním postižením. S tím souvisí Dostupnost, jež požaduje spolehlivý a technologicky neutrální přístup, nevyžadující specifický placený software, a zajištěnou lidskou podporu.⁶ Kritérium Ekvity a nediskriminace sleduje, jak jsou zohledněny potřeby zranitelných skupin a zda jsou služby dostupné v cizích jazycích pro komunikaci s cizinci.

Z hlediska důvěry a právního rámce je klíčová Bezpečnost, která vyžaduje splnění nároků na kybernetickou bezpečnost a ochranu dat dle národních i evropských předpisů (včetně GDPR), s důrazem na princip Technologické neutrality⁷ a principy *Privacy & Security by design and by default*. Přesnost ověřuje obsahovou správnost informací a jejich soulad s platnou právní úpravou. Transparentnost zkoumá průhlednost procesů, poskytování otevřených dat, možnost sledovat stav vyřízení požadavku a vizuální identifikovatelnost orgánu veřejné moci.

z: https://cuzzs.gov.cz/userfiles/documents/Legislativa/Etický_kodex_uredniku_a_zamestnancu_ver_ejne_spravy.pdf. [cit. 2025-09-26].

⁴ Veřejný ochránce práv. *Principy dobré správy*. Online. In: Ombudsman - Veřejný ochránce práv. 2025. Dostupné z: <https://www.ochrance.cz/dokument/principy-dobre-spravy/principy-dobre-spravy.pdf>. [cit. 2025-09-25].

⁵ *Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration*. Online. In: Council of Europe, s. 6 - 9. Dostupné z: <https://rm.coe.int/cmrec-2007-7-of-the-cm-to-ms-on-good-administration/16809foo7c>. [cit. 2025-09-25]

⁶ *Informační koncepce České republiky: Koncepce budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zák. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů*. On-line. 2023. *Informační koncepce České republiky*. Online. In: Digitální česko. Strana 24 – 25. Dostupné z: https://digitalnicesko.gov.cz/media/files/Informa%C4%8Dn%C3%AD_koncepce_%C4%8Cesk%C3%A9_republiky_2024.docx.pdf. [cit. 2025-09-26].

⁷ RAMEŠOVÁ, Kristina; LECHNER, Tomáš; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Právní regulace kybernetické bezpečnosti a její meze: komentář*. Právní instituty. V Praze: C. H. Beck, 2023, a. 44-46. ISBN 978-80-7400-931-0.

Pro právní platnost úkonů je nezbytná Autentizace uživatele, prověřující spolehlivé ověření identity jednatelky osoby⁸, a Stvrzení projevu vůle adresáta veřejné moci, které cílí na zanechání platného a závazného potvrzení prostřednictvím uznávaného elektronického podpisu či datové schránky.⁹¹⁰ Konečně, kritérium Právo na digitální službu a práva související analyzuje, zda je naplněno právo uživatele garantované zákonem č. 12/2020 Sb. (např. právo na předvyplnění elektronických formulářů nebo na technologickou neutralitu¹¹). Tyto služby musí být veřejnosti dostatečně představeny skrze kritérium Seznámení veřejnosti (publicita), které monitoruje informovanost o nabízených službách a jejich výhodách, což je nutné pro jejich reálné využití.

Výsledky testování vybraných komunikačních kanálů

Právě na základě těchto principů a specifických požadavků bylo provedeno testování vybraných komunikačních kanálů, kdy řešitelka projektu cílila na zastoupení co nejširšího spektra možností komunikace, tj. datovou schránku, e-mail i na centrální, agendové a územní portálová řešení. Výsledky analýzy a zjištěné nedostatky jsou předmětem následující kapitoly. Celkově komunikační kanály vykazují značné rozdíly v implementaci definovaných požadavků. Některé kanály jsou uživatelsky přívětivé, ale vykazují nedostatky v transparentnosti nebo autentizaci, zatímco jiné excelují v transparentnosti, ale selhávají v přístupnosti nebo rychlosti.

- **Datové schránky (Digitální a informační agentura)**

Datové schránky jsou jedním z nejznámějších a nejoblíbenějších nástrojů digitální komunikace s veřejnoprávním prvkem. Prostředí je celkově uživatelsky přátelské a velmi jednoduché na ovládání. Systém disponuje technickou podporou a výpadky sítě nejsou časté. Systém je transparentní ve vztahu k odeslané a přijaté zprávě. Adresát veřejné moci však nemůže svůj požadavek spojit s označením u orgánu veřejné moci, nezná odpovědnou osobu, ani nemůže sledovat stav vyřizování požadavku. Systém neumožňuje třídění přijatých zpráv ani výmaz dle volby uživatele. Zásadním nedostatkem je to, že adresátovi zprávy není umožněno

⁸ KORBEL, František a KOVÁŘ, Dalibor. Právní úprava tzv. bankovní identity. Online. *Advokátní deník*. 2021. Dostupné z: <https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/>. [cit. 2025-04-13].

⁹ JAREŠ, Adam a KORBEL, František. Vztah elektronického podpisu a elektronické identifikace. *Právní rozhledy*. 2025, roč. -, č. 13-14, s. 444.

¹⁰ LECHNER, Tomáš; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Nařízení eIDAS a české adaptační zákony: komentář*. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2023, s. 138-140. ISBN 978-80-7598-924-6.

¹¹ MATEJKA, Ján; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Zákon o právu na digitální služby: komentář*. Komentátor. Praha: Leges, 2022, s. 46. ISBN 978-80-7502-607-1.

jednoznačně určit a ztotožnit jednající fyzickou osobu. Navíc je ztížen přístup cizím státním příslušníkům. Úroveň zabezpečení se odvíjí od nejslabšího článku, kterým je verifikace přístupu jménem a heslem. Projev vůle může být potvrzen buď elektronickým podpisem nebo fikcí podpisu, jejíž právní konstrukce však vykazuje klíčové nedostatky ve vztahu k identitě jednající osoby.

- **Portál občana (Digitální a informační agentura)**

Portál občana je dle správce plně v souladu se zákonem o přístupnosti. Životní situace jsou popsány srozumitelně.

Hlavním nedostatkem je nemožnost vyhledávání a filtrování v nabídce služeb a systém předpokládá pokročilou orientaci uživatele. Při přetíženosti sítě se nelze přihlásit identitou občana. Portál občana je transakční částí Portálu veřejné správy¹², ale právní úprava tento vztah obou portálů nijak nedefinuje a slučuje je pod jedním pojmem „Portál veřejné správy“. Systém není dostatečně transparentní - je uvedeno datum odeslání, ale nikoli datum doručení, ani číslo označení. Věc je vedena jako vyřízená ihned po odeslání žádosti. Systém běží jen v českém jazyce. Odeslání je možno provést datovou schránkou bez identifikace jednajícího.

- **Portál „Moje daně“ (Ministerstvo financí)**

Portál splňuje požadavky na přístupnost a dokonce byl testován za přispění nevidomých a slabozrakých. Portál je návodný. Umožňuje tři možnosti přihlášení. Funguje vyhledávání a řazení podle typu daně je předvídatelné. Portál je transparentní, neboť obsahuje jak údaj o odeslání, tak o doručení, čísla jednací, odpovědný úřad a stav vyřízení. Dochází k předvyplnění základních údajů ve formulářích.

Do systému se lze přihlásit identitou občana nebo datovou schránkou. Autentizace je možná jen při přihlášení identitou občana, nikoli prostřednictvím datové schránky, ale odeslání je možno provést i datovou schránkou bez identifikace jednajícího.

- **Portál „Jenda“ (Ministerstvo práce a sociálních věcí)**

Komunikační kanál je přehledný a srozumitelný, s jednoduchou nabídkou služeb a je přizpůsoben pro použití osobním počítačem i mobilním telefonem. Systém využívá kvalitní propojení s údaji ze základních registrů, včetně údajů o partnerovi/manželovi a dítěti. Systém je dobře komunikován vůči veřejnosti. Systém plní požadavky na transparentnost, včetně aktuálního stavu dávky, data podání a čísla jednací. Systém obsahuje přehledně sled jednotlivých učiněných kroků a jejich změn. Systém neobsahuje údaj o doručení, ale zajišťuje vystavení osvědčení. Portál plní požadavky na autentizaci i autorizaci.

¹² DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Na čem pracujeme - Portál občana*. Online. DIGITÁLNÍ A INFORMAČNÍ AGENTURA. Digitální a informační agentura. -. Dostupné z: <https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme>. [cit. 2025-04-16].

Stránky nejsou plně v souladu s požadavky na přístupnost. Podání může učinit pouze osoba ověřená přes identitu občana. Systém běží jen v českém jazyce.

- **Portál dopravy (Ministerstvo dopravy)**

Portál dopravy dle správce plní požadavky na přístupnost. Systém je propojen se základními registry, registrem vozidel a dalšími agendovými systémy. Help desk je nápomocný, nabízí kontakt jak na technickou podporu (kontaktní formulář), tak non-stop na věcnou podporu (telefonní číslo, email). Přihlášení je možné pouze identitou občana, tudíž autentizace je zaručena a autorizace může využít fikce podpisu dle zákona o informačních systémech veřejné správy.

Systém postrádá obecnou kolonku pro podání žádosti a neobsahuje vyhledávání, čímž nutí uživatele přijmout logiku správce. Cesta pro vrácení do předchozího kroku je špatně viditelná, systém využívá na některých místech velmi malé písmo. Informace o podaných žádostech nejsou shromážděny na jednom místě. Systém běží jen v českém jazyce.

- **Portál stavebníka (Ministerstvo pro místní rozvoj)**

Portál plní požadavky na autentizaci i autorizaci.

Ačkoli správce tvrdí plný soulad s přístupností, řešitelka pochybuje o správnosti prohlášení, jelikož stránky jsou přehlceny obrázky a kolonka "nová žádost" splývá s pozadím. Systém je pomalý, mívá výpadky a vykazuje chyby (např. neumožňuje vyhledání pozemků z mapy bez zadání obce). Podání nelze přenechat jiné osobě pro pokračování ve zpracování nebo podpisu, a proto má značné nedostatky v uživatelské přívětivosti a nejde vstříc stavební praxi. Název „Portál stavební správy“ neodpovídá zákonnému termínu „Portál stavebníka“. Nedostatek je zmírněn tím, že internetový vyhledávač nabízí po zadání obou možností správný odkaz. Požadavek na transparentnost systému je na nízké úrovni - systém informuje o odeslání podání, nikoli o doručení ani o označení u orgánu veřejné moci. Stav vyřízení se zobrazuje pouze zjednodušeně - jako vyřízená/ nevyřízená věc. Systém běží jen v českém jazyce.

- **Elektronická podatelna (Ministerstvo spravedlnosti)**

Systém je spojený pro všechny české soudy. Prostředí je uživatelsky vstřícné a jednoduché na ovládání. Na úvodní straně jsou návody a příručky; aktuální informace o technologických odstávkách a změnách v systému. Systém informuje o doručení požadavku orgánu veřejné moci a o označení, pod nímž lze požadavek u orgánu veřejné moci nalézt.

Odkazy a informace o možnosti využití ePodatelny jsou u některých soudů obtížně dohledatelné (schované nebo ve Word dokumentech). Pro jakékoli podání je vyžadován uznávaný elektronický podpis. Přesto není uživatel autentizován – systém přejímá informace uvedené žadatelem. Stránky neobsahují informace o přístupnosti - prohlášení je umístěno na stránkách justice.cz, podle nichž nejsou stránky plně v souladu.

- **Moje VZP (Veřejná zdravotní pojišťovna)**

Systém je cíleně budován i pro neslyšící a podporuje český a anglický jazyk. VZP má kvalitní helpdesk i prostřednictvím telefonní linky, kdy pracovníci jsou schopni informace zjistit dodatečně a volají klientovi zpět.

Stránky jsou přehledné pouze omezeně; nabídka je velmi rozvětvená a informace nelze nalézt na jednom místě. Klienti užívají aplikace zejména za účelem získání příspěvků a podmínky pro získání příspěvku jsou poměrně složitě popsány. Stránky jsou v souladu se zákonem o přístupnosti pouze částečně. Autentizace je možná pouze při přihlášení identitou občana, ačkoli způsobů přihlášení nabízí systém více, včetně datových schránek. Z toho důvodu je i autorizace validní pouze tehdy, je-li identifikována jednáající osoba.

- **Portál Pražana (Magistrát hlavního města Prahy)**

Systém poskytuje přehledný seznam služeb a je adekvátně propagován. Systém obsahuje přehled učiněných podání a stav aktuálně učiněného kroku, např. odesláno. Při přihlášení prostřednictvím identity občana je umožněna autorizace úkonu. Při přihlášení pomocí datové schránky systém identifikuje zastupující osobu.

Systém informuje o okamžiku odeslání požadavku ze strany adresáta, nikoli o okamžiku doručení ani o označení u orgánu veřejné moci. Vystavené osvědčení neidentifikuje obsah úkonu, který adresát učinil. Není zřejmé, zda portál splňuje požadavky zákona o přístupnosti v plném rozsahu.

Analýza a zjištěné nedostatky digitální komunikace

Navzdory nepopiratelnému pokroku v digitalizaci veřejné správy odhalil výzkum řadu systémových i praktických nedostatků, které brání plnému využití potenciálu e-Governmentu.

Jedním z nejzásadnějších zjištění je, že technologický pokrok naráží na bariéry v podobě lidského faktoru. U některých orgánů veřejné moci byla zaznamenána neochota ke spolupráci a alibistický přístup.¹³ Tento problém nelze vyřešit pouze digitalizací, ale vyžaduje změnu v kultuře a řízení veřejné správy.

Povědomí veřejnosti o dostupných digitálních službách je stále nízké.¹⁴ Ačkoli existují kvalitní informační zdroje, chybí systematická osvěta a marketingové aktivity. Situaci dále komplikuje pojmová nejednoznačnost, například zaměňování Portálu veřejné

¹³ NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST. Odpověď k dotazu dle zákona č. 106/1999 Sb. ze dne 23. 5. 2025 č. j. 4285/2025-NÚKIB-E/210, sp. zn. 210-460/2025-E k žádosti o poskytnutí informací dle zákona č. 106/1999 Sb.

¹⁴ Průzkum: Digitalizace státu má velké rezervy. Co lidem a firmám chybí? Online. *BusinessInfo.CZ*. 2025, roč. -, č. -, s. -. Dostupné z: <https://www.businessinfo.cz/clanky/pruzkum-digitalizace-statu-ma-velke-rezervy-co-lidem-a-firmam-chybi/>. [cit. 2025-07-29].

správy a Portálu občana, což působí na uživatele matoucím dojmem a narušuje principy srozumitelnosti a předvídatelnosti.

Každý portál a informační systém veřejné správy má často odlišný vzhled a logiku ovládání. Tato nejednotnost ztěžuje orientaci, snižuje intuitivnost a narušuje důvěru v to, že uživatel komunikuje s oficiálním orgánem státu. Implementace nedávno schváleného jednotného vizuálního stylu je proto klíčová.¹⁵

Digitální služby jsou roztržštěné do velkého množství samostatných a často nepropojených portálů. Uživatel nemá k dispozici centrální místo pro sledování stavu všech svých podání, což vede k duplicitám a porušuje princip Transparentnosti. Namísto propojování systémů dochází k budování nových, což fragmentaci dále prohlubuje.

Složitá a nejednoznačná zákonná definice informačního systému veřejné správy ztěžuje orgánům i uživatelům orientaci v tom, jaká práva a povinnosti se k danému systému vážou. Tato nejasnost komplikuje praktickou aplikaci norem, například uplatnění fikce podpisu.

V některých případech digitalizace paradoxně vytváří duplicitní procesy. Příkladem je povinnost orgánu veřejné moci vystavit osvědčení o digitálním úkonu, i když jiné mechanismy, jako je doručenko z datové schránky, již plní podobnou funkci. Taková duplicita je v rozporu s principem efektivity a měla by být eliminována.

Ačkoli Zákon o právu na digitální služby primárně zakotvuje *právo*¹⁶, jeho subsidiární povaha umožňuje speciálním zákonům nařídit *povinnost* jednat elektronicky. V kombinaci s absencí ústavně garantovaného práva na nedigitální komunikaci vzniká riziko digitálního vyloučení, které je v rozporu s principem rovného zacházení.

Potenciál kontaktních míst Czech POINT jako klíčového nástroje pro digitálně vyloučené občany omezuje legislativní bariéra, která jim brání vydávat výpisy z neveřejných evidencí. Občan si tak tentýž výpis může sám obstarat online přes Portál občana, ale na přepážce mu jej vydat nelze. To je nelogické a v přímém rozporu s několika principy řádné správy.

Autentizace prostřednictvím datové schránky je systémově problematická, neboť často ověřuje pouze držitele schránky, nikoli konkrétní fyzickou osobu, která úkon činí. Tím je zpochybněna platnost fikce podpisu a narušena právní jistota, jelikož adresát nemůže zjistit, kdo za právnickou osobu skutečně jednal. Problematiku dále

¹⁵ Česko představilo nový jednotný vizuální styl státu. Přináší důvěru, srozumitelnost a lepší prezentaci v zahraničí. Online. In: MINISTERSTVO ZAHRA NIČNÍCH VĚCÍ. Ministerstvo zahraničních věcí České republiky. -, 16.07.2025. Dostupné z: https://mzv.gov.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/cesko_predstavilo_novy_jednotny_vizualni.html. [cit. 2025-07-22].

¹⁶ ZAJÍČEK, Zdeněk; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Zákon o právu na digitální služby: komentář*. Beckovy komentáře. V Praze: C.H. Beck, 2021, s. 35. ISBN 978-80-7400-822-1.

komplikuje stanovisko Nejvyššího soudu (Pls. 1/2015), které obsahuje řadu nesprávností.¹⁷ Systém také nerozlišuje mezi veřejnoprávní a soukromoprávní rolí obce, což působí nedůvodné rozdíly pro adresáty zejména v oblasti pracovněprávních vztahů.

Centrální, agendové i územní portály jsou uživatelsky velmi oblíbeným, ale jen jednosměrným komunikačním kanálem. Současná právní úprava, zejména správní řád a zákon o elektronických komunikacích, neumožňují, aby orgán veřejné moci odpověděl adresátovi stejným způsobem, jakým žadatel svůj podnět učinil.¹⁸ Odpovědi jsou doručovány výlučně do datové schránky, což ubírá na přehlednosti a flexibilitě komunikace.

Doporučení pro aplikaci výsledků s využitím umělé inteligence

Na základě zjištění prezentovaných v předchozí kapitole lze definovat několik klíčových oblastí vyžadujících systematickou pozornost. Některé z identifikovaných problémů mohou být řešeny za použití umělé inteligence. Cílené nasazení umělé inteligence může vést k efektivnější a uživatelsky přívětivější veřejné správě.¹⁹ Úspěch však vyžaduje jasnou strategii, etický rámec a investice.

Inteligentní chatboti a virtuální asistenti, jaké již pilotuje většina orgánů veřejné moci, mohou poskytovat občanům okamžité odpovědi, navigovat je složitými procesy a pomáhat s vyplňováním formulářů. Tím se snižuje zátěž úředníků, kteří se mohou orientovat na odborné procesy. Současně by měla být umělá inteligence schopná vyvíjet samostatně marketingové aktivity a pomáhat s řešením problému nedostatečné informovanosti veřejnosti.

Technologie AI je ideálním nástrojem pro vytěžování dat z nestrukturovaných dokumentů. Může tak výrazně zrychlit zpracování podání, která nejsou ve strojově čitelném formátu, a snížit manuální práci na straně úřadů. Současně je schopná vyhledávat duplicity procesů a možnosti snižování administrativní zátěže.

Využití AI při tvorbě legislativy, jak bylo testováno již při vzniku Zákona o právu na digitální služby, může pomoci odhalovat konflikty mezi předpisy a přispět k odstranění nejasností. Jak ukazuje projekt Ministerstva financí v oblasti regulace hazardu, umělá inteligence může být využita k analýze velkých objemů dat a k

¹⁷ KMENT, Vojtěch; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Právní monografie. Praha: Wolters Kluwer, 2018., s. 322. ISBN 978-80-7552-815-5.

¹⁸ JEMELKA, Luboš; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Správní řád: komentář*. 7. vydání. Beckova edice komentované zákony. V Praze: C.H. Beck, 2023, s. 163. ISBN 978-80-7400-932-7.

¹⁹ JAREŠ, Adam. Umělá inteligence, automatizace a kódování v právu. *Bulletin advokacie*. 2025, č. 1-2, s. 33.

identifikaci anomálií. Umělá inteligence by tak mohla být použita například pro kontrolu digitálních nástrojů orgánů veřejné moci, například souladu s pravidly přístupnosti.

Některé problémy s autentizací osob a autorizací jednání odstraní, nebo alespoň *zmírní elektronická peněženka (EUDI Wallet)*.²⁰ „Pro zastupování je klíčový Registr zastupování – jeho důsledná implementace významně omezí nejasnosti, kdo za koho a v jaké agendě jedná.“²¹

Závěr

Projekt poskytl komplexní a kritický pohled na současný stav digitální komunikace v prostředí českého e-Governmentu. Analýza odhalila, že navzdory existenci pokročilých technologií a ambiciózní legislativy přetrvává v Česku řada systémových nedostatků, které brání naplnění vize efektivní, transparentní a uživatelsky přívětivé digitální veřejné správy.

Mezi nejdůležitější zjištění patří přetrvávající fragmentace systémů, která vede k uživatelské nepřehlednosti. Klíčovým problémem je také nedostatečná autentizace uživatelů, zejména v kontextu datových schránek, což vyvolává právní nejistotu. Nízká informovanost veřejnosti způsobuje, že potenciál digitálních služeb zůstává nevyužit. V neposlední řadě, roztržitost právní úpravy a legislativní bariéry komplikují maximální využitelnost digitálního prostředí.

Přínos projektu spočívá v pojmenování a analýze stěžejních nedostatků a tedy ve vypracování podkladu pro jejich další rozpracování. Klíčové může být využití potenciálu moderních technologií, včetně umělé inteligence za účelem nápravy nežádoucího stavu. Ačkoli trend společnosti je směřovat kupředu, dle autorky to není možné bez nápravy stěžejních systémových chyb. Cesta k tomuto cíli je náročná, ale předložená analýza ukazuje, že je dosažitelná.

Seznam použité literatury

1. *Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration*. Online. In: Council of Europe. Dostupné z: <https://rm.coe.int/cmrec-2007-7-of-the-cm-to-ms-on-good-administration/16809foo7c>. [cit. 2025-09-25].

²⁰ PIFFL, Robert. *Dopady novely nařízení eIDAS 2.0; 1. díl Evropské peněženky digitální identity*. Online. CCB, SPOL. S R. O. SystemOnlineCz. 10/2024. Dostupné z: <https://www.systemonline.cz/sprava-dokumentu/dopady-novely-narizeni-eidas-2.0.htm>. [cit. 2025-04-16].

²¹ KONEČNÁ, Sandra a PETR, Jan. *Závěrečná zpráva SUP2-2024-2: „Nedostatky digitální komunikace s veřejnoprávním prvem v ČR“*. Akademická práce. Olomouc: Univerzita Palackého v Olomouci, Právnická fakulta, 2025, s. 47.

2. *Služební předpis nejvyššího státního tajemníka č. 3 ze dne 3. října 2023 o pravidlech etiky státních zaměstnanců.* Online. In: MINISTERSTVO VNITRA. Ministerstvo vnitra. 2023. Dostupné z: file:///C:/Users/uzivatel/Downloads/Sluzebni_predpis_a_oduvodneni_v_grafickem_zpracovani_-_20231013.pdf. [cit. 2025-09-25].
3. Veřejný ochránce práv. *Principy dobré správy.* Online. In: Ombudsman - Veřejný ochránce práv. 2025. Dostupné z: <https://www.ochrance.cz/dokument/principy-dobre-spravy/principy-dobre-spravy.pdf>. [cit. 2025-09-25].
4. MINISTERSTVO VNITRA. *Etický kodex úředníků a zaměstnanců veřejné správy.* Online. Český úřad pro zkoušení zbraní a střeliva. 2014. Dostupné z: https://cuzzs.gov.cz/userfiles/documents/Legislativa/Etický_kodex_uredniku_a_zamestnancu_verejne_spravy.pdf. [cit. 2025-09-26].
5. KORBEL, František a KOVÁŘ, Dalibor. *Právní úprava tzv. bankovní identity.* Online. *Advokátní deník.* 2021. Dostupné z: <https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/>. [cit. 2025-04-13].
6. *Informační koncepce České republiky: Koncepce budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zák. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.* On-line. 2023. *Informační koncepce České republiky.* Online. In: Digitální česko. Dostupné z: https://digitalnicesko.gov.cz/media/files/Informa%C4%8Dn%C3%AD_koncepce_%C4%8Cesk%C3%A9_republiky_2024.docx.pdf. [cit. 2025-09-26].
7. JAREŠ, Adam a KORBEL, František. *Vztah elektronického podpisu a elektronické identifikace.* *Právní rozhledy.* 2025, roč. -, č. 13-14, s. 441-445.
8. DIGITÁLNÍ A INFORMAČNÍ AGENTURA. *Na čem pracujeme - Portál občana.* Online. DIGITÁLNÍ A INFORMAČNÍ AGENTURA. Digitální a informační agentura. -. Dostupné z: <https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme>. [cit. 2025-04-16].
9. *Česko představilo nový jednotný vizuální styl státu. Přináší důvěru, srozumitelnost a lepší prezentaci v zahraničí.* Online. In: MINISTERSTVO ZAHRANIČNÍCH VĚCÍ. Ministerstvo zahraničních věcí České republiky. -, 16.07.2025. Dostupné z: https://mzv.gov.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/cesko_predstavil_o_novy_jednotny_vizualni.html. [cit. 2025-07-22].
10. PIFFL, Robert. *Dopady novely nařízení eIDAS 2.0; 1. díl Evropské peněženky digitální identity.* Online. CCB, SPOL. S R. O. SystemOnlineCz. 10/2024. Dostupné z: <https://www.systemonline.cz/sprava-dokumentu/dopady-novely-narizeni-eidas-2.0.htm>. [cit. 2025-04-16].
11. *Průzkum: Digitalizace státu má velké rezervy. Co lidem a firmám chybí?* Online. *BusinessInfo.CZ.* 2025, roč. -, č. -, s. -. Dostupné

z: <https://www.businessinfo.cz/clanky/pruzkum-digitalizace-statu-ma-velke-rezervy-co-lidem-a-firmam-chybi/>. [cit. 2025-07-29].

12. LECHNER, Tomáš; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Nařízení eIDAS a české adaptační zákony: komentář*. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2023. ISBN 978-80-7598-924-6.
13. RAMEŠOVÁ, Kristina; LECHNER, Tomáš; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Právní regulace kybernetické bezpečnosti a její meze: komentář*. Právní instituty. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-931-0.
14. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST. Odpověď k dotazu dle zákona č. 106/1999 Sb. ze dne 23. 5. 2025 č. j. 4285/2025-NÚKIB-E/210, sp. zn. 210-460/2025-E k žádosti o poskytnutí informací dle zákona č. 106/1999 Sb.
15. JEMELKA, Luboš; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Správní řád: komentář*. 7. vydání. Beckova edice komentované zákony. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-932-7.
16. JAREŠ, Adam. Umělá inteligence, automatizace a kódování v právu. *Bulletin advokacie*. 2025, č. 1-2, s. 33-37.
17. KMENT, Vojtěch; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Právní monografie. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-815-5.
18. MATEJKA, Ján; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Zákon o právu na digitální služby: komentář*. Komentátor. Praha: Leges, 2022. ISBN 978-80-7502-607-1.
19. ZAJÍČEK, Zdeněk; ŠIMKA, Karel; POSTRÁNECKÝ, Josef; POMAHAČ, Richard; HOSTAŠ, Petr et al. *Zákon o právu na digitální služby: komentář*. Beckovy komentáře. V Praze: C.H. Beck, 2021. ISBN 978-80-7400-822-1.
20. KONEČNÁ, Sandra a PETR, Jan. *Závěrečná zpráva SUP2-2024-2: „Nedostatky digitální komunikace s veřejnoprávním prvkem v ČR“*. Akademická práce. Olomouc: Univerzita Palackého v Olomouci, Právnická fakulta, 2025.

Kontaktní údaje

JUDr. Sandra Konečná

sandra.konecna01@upol.cz

Univerzita Palackého v Olomouci, Právnická fakulta, Institut pro právo a pokročilé technologie

PŘEKÁŽKY ŠIRŠÍHO VYUŽITÍ UMĚLÉ INTELIGENCE VE SPRÁVNÍM ROZHODOVÁNÍ V ČESKÉ REPUBLICE

THE OBSTACLES OF THE USE OF AN ARTIFICIAL INTELLIGENCE IN ADMINISTRATIVE DECISION-MAKING IN THE CZECH REPUBLIC

Kateřina Ištuková¹

Abstrakt: Článek se zaměřuje na hlavní překážky, které brání širšímu využívání umělé inteligence v rozhodovací činnosti správních orgánů v České republice a na možnosti jejich překonání. Tyto překážky lze rozdělit do tří oblastí: právní, technické a organizační.

Z právního hlediska je překážkou nestabilita legislativního prostředí. Nedostatkem je také absence právního zakotvení možnosti využití umělé inteligence s ohledem na specifika správního práva. Novela správního řádu umožňující využití automatizace už neprojde legislativním procesem.

Technické bariéry souvisí především s prací s daty, která jsou pro AI klíčová. ČR se dlouhodobě potýká s jejich roztržitostí, problematickou kvalitou i omezenou dostupností pro správní orgány. Další otázkou je, zda využívat komerční nástroje s AI či vytvořit vlastní systém připravený na míru českému správnímu řízení. Situaci také komplikuje pomalé zavádění digitalizovaných agend, nedostatečné využívání datových schránek a Portálu občana a chybějící standardizované formuláře pro podání.

Organizační překážky spočívají zejména v nedostatku kvalifikovaného personálu. Nabídka odpovídajících školení a metodik je zatím omezená. Významnou roli hraje i nedůvěra úředních osob v samotné výstupy, obavy z nedostatečné garance ochrany osobních údajů a nevyjasněná odpovědnost úředních osob.

Cílem příspěvku je představit některé z překážek, a ukázat, že pro zavedení AI je potřeba změna systémového přístupu zahrnující změny ve všech zmíněných odvětvích.

Klíčové slova: Správní rozhodování, Odpovědnost, Umělá inteligence, Práce s daty, Legislativní prostředí

Abstract: This article addresses the main obstacles that have so far prevented the wider use of artificial intelligence in the decision-making processes of the

¹ Katedra správní vědy a správního práva Právnické fakulty Masarykovy univerzity v Brně

administrative bodies in the Czech Republic and the possible solution. These barriers can be divided into three categories: legal, technical and organizational.

From a legal perspective, the main concern is the instability of the legislative environment. Another shortcoming is the absence of the regulation governing the use of AI in administrative law. The planned amendment to the Administrative Code, intended to allow such regulation, will not pass the legislative process.

Technical barriers relate mainly to data, which is crucial for AI. The Czech Republic has a long-standing problem with fragmentation, low-quality and poorly accessible data for the administrative bodies. Authorities must also decide whether to rely on commercial AI tools or create a system tailored to the Czech administrative field. Slow digitalization, limited use of data boxes and the Citizen Portal, and the lack of standardized forms further complicate the situation.

Organizational obstacles stem from shortage of qualified personnel, insufficient training and methodologies, distrust of AI outputs, concerns about data protection and unclear responsibility for automated decisions.

Overall, introducing AI requires a systemic approach involving legal, technical, and organizational reforms.

Key words: Administrative decision-making, Responsibility, Artificial Intelligence, Use of Data, Legislation

Úvod

Umělá inteligence (dále také „AI“) se v české veřejné správě často prezentuje jako nástroj, který může zásadně zvýšit efektivitu činností veřejné správy a současně snížit administrativní zátěž úředních osob.² Tento důraz na pozitivní přínosy umělé inteligence však opomíjí skutečnost, že existuje celá řada bariér, které širšímu zapojení této technologie do rozhodovací činnosti správních orgánů brání.

Jejich systematické shrnutí s důrazem na českou veřejnou správu dosud chybí, a to i přes existenci řady strategických dokumentů orgánů ústřední správy³ či množství

² NEJEDLÝ, Matěj: AI v české státní správě? Když zaspíme, ekonomika neporoste, varují experti. In: Seznam Zprávy [online] [cit. 27.09.2025]. Dostupné na: <https://www.seznamzpravy.cz/clanek/domaci-ai-v-ceske-statni-sprave-kdyz-zaspime-ekonomika-neporoste-varuji-experti-263061>

³ Viz VLÁDA ČR: Národní strategie umělé inteligence České republiky 2030. [online] [cit. 1. 9. 2025]. Dostupné na: <https://www.mpo.gov.cz/assets/cz/podnikani/2024/9/Narodni-strategie-umele-intelligence-CR-2030.pdf> či MINISTERSTVO VNITRA: Analýza a zhodnocení

odborných článků. A z toho důvodu jsem si toto téma vybrala jako téma svého příspěvku.

Tyto bariéry lze rozdělit do tří kategorií: na technické, právní a organizační. Každou z nich představím v samostatné části článku. Je však nutné zdůraznit, že na tyto oblasti nelze nahlížet izolovaně, protože mezi překážkami existují vazby a ke kvalitnímu provedení implementace AI je bude nutné překonávat systematicky.

Cílem tohoto článku je nejen představit tyto překážky, ale také nastínit způsoby jejich řešení, což provedu na závěr mého příspěvku. Namísto pouhého konstatování, že česká veřejná správa není na využívání AI dostatečně připravena, se pokusím ukázat, že řadu bariér lze vhodnými opatřeními zmírnit či zcela eliminovat. Což může usnadnit postupnou implementaci umělé inteligence do správních řízení, potažmo správního rozhodování a naplno využít přínosy této technologie.

Ačkoli mé poznatky a závěry se budou primárně vztahovat k českému právnímu a institucionálnímu prostředí, tak lze tyto závěry aplikovat i v dalších státech, například na Slovensku, které se s využíváním umělé inteligence nachází rovněž v počátcích.

Umělá inteligence v české veřejné správě

Umělá inteligence představuje komplexní fenomén, který není snadné jednoznačně definovat.⁴ Pod tímto pojmem se mohou skrývat jak jednoduché, tzv. rules-based modely založené na předem daných pravidlech s prvky autonomie, které využívají rozsáhlé databáze,⁵ tak i pokročilé modely využívající strojové učení, které se učí z poskytnutých dat a zpětné vazby.⁶

AI lze definovat různě, ale pro oblast veřejné správy a práva je klíčová definice obsažená v nařízení o umělé inteligenci⁷. Podle něj je systém AI: „*strojový systém navržený tak, aby po zavedení fungoval s různými úrovněmi autonomie, a který po zavedení může vykazovat adaptabilitu, a který za explicitními nebo implicitními účely z*

potenciálu využití automatizace a umělé inteligence v agendách veřejné správy. Praha: Ministerstvo vnitra ČR, 2023. 80 s. [online] [cit. 1. 9. 2025]. Dostupné na: <https://www.mvcr.cz/soubor/analiza-a-zhodnoceni-potencialu-vyuziti-automatizace-a-umele-inteligence-v-agendach-verejne-spravy.aspx>.

⁴ WIRTZ, Bernd W. – WEYERER, Jan C. – GEYER, Carolin: Artificial Intelligence and the Public Sector—Applications and Challenges. In: International Journal of Public Administration, Roč. 42, č. 7 (2019), s. 600.

⁵ PARYCEK, Peter – SCHMID, Verena – NOVAK, Anna-Sophie: Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. In: Journal of the Knowledge Economy, Roč. 15, č. 2 (2024), s. 8400.

⁶ SURDEN, Harry: Machine Learning and Law: An Overview. In: Research Handbook on Big Data Law. Stanford: Edward Elgar Publishing, 2021, s. 171. ISBN 978-1-78897-282-6.

⁷ Nařízení Evropského Parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (dále také „akt o umělé inteligenci“ či „AI akt“).

*obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická nebo virtuální prostředí.*⁸ Tato definice je zásadní, protože od ní se budou odvíjet budoucí právní úpravy umělé inteligence.

Je rovněž nezbytné od AI odlišovat automatizaci, i přesto, že v praxi se tyto nástroje často směřují. Automatizované nástroje vykonávají pouze předem naprogramované úkony bez jakékoliv autonomie či schopnosti adaptace, a výsledku se dosahují bez zásahu člověka.⁹

V České republice se zatím využívají převážně automatizované systémy než skutečná AI. Přesto již existuje několik systémů s umělou inteligencí, která se v praxi využívají. Nově jejich přehled tvoří Digitální a informační agentura, která pro tento účel vytvořila „katalog využití AI ve veřejném sektoru“¹⁰. V praxi se jedná například o „AI systém Emil“, využívaný v předprocesní fázi na Městském úřadě v Praze 8 v oblasti dopravní přestupků¹¹, či systém DROMAS, který zpracovává satelitní data a průběžně monitoruje plnění dotačních podmínek v zemědělství.¹² Tyto nástroje se však zatím uplatňují mimo oblast správního rozhodování.

Na základě Aktu o AI bylo jako gestor pro tuto oblast vybráno Ministerstvo průmyslu a obchodu, které bude odpovědné za koordinaci implementace. Vykonávat dozor v této oblasti bude Český telekomunikační úřad (ČTÚ), Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) a Česká agentura pro standardizaci (ČAS).¹³

Z uvedeného vyplývá, že česká veřejná správa se nachází spíše ve fázi pilotních projektů a přípravných strategií než v plošném zavádění umělé inteligence do správního rozhodování.

⁸ Článek 3 aktu o umělé inteligenci.

⁹ FIALOVÁ, Eva – MATEJKA, Ján – GÜTLER, Vojen: Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod. Praha: Ústav státu a práva AV ČR, v. v. i., 2020. s. 13. ISBN 978-80-87439-42-5.

¹⁰ DIGITÁLNÍ A INFORMAČNÍ AGENTURA: Katalog využití umělé inteligence ve veřejném sektoru. In: Digitální a informační agentura [online] [cit. 27.09.2025]. Dostupné na: <https://egovai.dia.gov.cz/>

¹¹ MĚSTSKÁ ČÁST PRAHA 8: Úřad MČ Praha 8: Informace z úřadu – V Praze 8 řeší přestupky za špatné parkování softwarový robot. In: Městský úřad Praha 8 [online] [cit. 27.09.2025]. Dostupné na: <https://m.praha8.cz/v-praze-8-resi-prestupky-za-spatne-parkovani-softwarovy-robot-1.html>

¹² EVROPSKÁ VESMÍRNÁ AGENTURA: DROMAS | ESA Space Solutions. In: European Space Agency [online] [cit. 27.09.2025]. Dostupné na: <https://business.esa.int/projects/dromas>

¹³ ODBOR KOMUNIKACE MPO: Další krok k rozvoji umělé inteligence v Česku. Vláda schválila návrh na zajištění implementace AI Aktu, novým gestorem je MPO. In: Ministerstvo průmyslu a obchodu [online] [cit. 27.09.2025]. Dostupné na: <https://mpo.gov.cz/cz/rozcestnik/pro-media/tiskove-zpravy/dalsi-krok-k-rozvoji-umele-inteligence-v-cesku--vlada-schvalila-navrh-na-zajisteni-implementace-ai-aktu--novym-gestorem-je-mpo--287763/>

Technické bariéry

První skupinou překážek bránících širšímu využití AI jsou bariéry technického charakteru.

Nejkritičtějším problémem v této části jsou data. Ta představují základní informace, na kterých je umělá inteligence vystavěna.¹⁴ Jedná se o informace, které je nutné vložit do systému využívající AI.¹⁵

Data lze rozdělit do dvou skupin. První tvoří trénovací data, mezi něž patří právní předpisy, judikatura, odborná literatura, metodické pokyny, správní praxe v podobě předchozích rozhodnutí či výsledky odvolacích řízení. Právě na jejich základě se systém učí základním principům a vzorcům rozhodování.

Druhou skupinou jsou data relevantní pro konkrétní případ, tedy podklady od účastníků řízení, skutková zjištění, informace známé z úřední činnosti správních orgánů, stanoviska dotčených orgánů nebo výstupy z databází. Dle nich AI analyzuje situaci a vytvoří návrh rozhodnutí.

Obě skupiny těchto dat ale v české veřejné správě trpí významnými nedostatky. Hlavním problémem je roztříštěnost dat. Jednotlivé orgány spravují vlastní databáze, které na sebe nejsou navázané a nedokáží spolu jednoduše komunikovat.¹⁶ To vede k tomu, že občan i správní orgány musejí opakovaně dokládat totožné údaje. Pokud data existují, bývají navíc často nekvalitní či neaktuální. Na tuto slabinu upozorňuje i Ministerstvo vnitra, které ve své analýze uvádí, že nedostatky v oblasti dat budou jednou z hlavních překážek implementace AI do veřejné správy.¹⁷ Je tudíž nutné budovat infrastrukturu umožňující jejich získávání, skladování a využívání ve vhodném rozsahu a kvalitě.¹⁸

Dalším nedostatkem je nedostatečná digitalizace. Významná část podkladů stále existuje pouze v papírové podobě, což je patrné zejména v oblasti stavebního práva. Proces digitalizace přitom postupuje pomalu, a ne vždy s kvalitními výsledky. Nedaří se na centrální úrovni s projekty jako digitalizace stavebního řízení, nedotažená E-

¹⁴ PARYCEK, Peter – SCHMID, Verena – NOVAK, Anna-Sophie: Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. In: Journal of the Knowledge Economy, Roč. 15, č. 2 (2024), s. 8390–8415.

¹⁵ OECD: Artificial Intelligence in Society. Paris: OECD Publishing, 2019. s. 2. ISBN 978-92-64-58254-5.

¹⁶ SKALICKÝ, Matěj: Digitalizace není v Česku priorita, mrzí experta. K posouzení DSR prý chybí dostatek dat. [online] [cit. 27.09.2025]. Dostupné na: <https://plus.rozhlas.cz/digitalizace-neni-v-cesku-priorita-mrzi-experta-k-posouzeni-dsr-pry-chybi-g328268>

¹⁷ MINISTERSTVO VNITRA: Analýza a zhodnocení potenciálu využití automatizace a umělé inteligence v agendách veřejné správy. Praha: Ministerstvo vnitra ČR, 2023. 80 s. [online] [cit. 1. 9. 2025]. Dostupné na: <https://www.mvcr.cz/soubor/analiza-a-zhodnoceni-potenciu-vyuziti-automatizace-a-umele-inteligence-v-agendach-verejne-spravy.aspx>

¹⁸ HUBKOVÁ, Pavlína: EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. In: AUC IURIDICA, Roč. 70, č. 2 (2024), s. 101–119.

sbírka či odstoupení od požadavku na povinné datové schránky pro všechny občany. Ale zároveň se nedaří ani na samotných úřadech, a to z důvodu vyčerpání úřadů a nedostatku personálu. I v případech, kdy jsou dokumenty digitalizovány, tak nejsou ve strojově čitelné podobě, které by mohla AI rovnou využít.

V celku se jedná o dlouhodobý proces, na který je nutné vynaložit určité náklady a čas, ale k aktivnímu využívání AI zcela nezbytný.

Nedostatečná je i standardizace dokumentů – jednotlivé správní orgány používají vlastní formáty rozhodnutí i vzory podání či formuláře, což komplikuje zavedení centrálního systému, který by byl optimalizovaný pro zpracování pomocí AI.

Specifickým rysem české veřejné správy je i velký rozsah agend. V současnosti existuje kolem 7 600 poskytovaných služeb¹⁹ s vlastními specifiky. Z toho důvodu není realistické vyvinout jen jeden univerzální nástroj aplikovatelný pro všechny oblasti. S největší pravděpodobností bude nutné vyvíjet více specializovaných nástrojů pro jednotlivé agendy, což proces implementace prodlouží a prodraží.

Významnou překážkou je i nejistota ohledně používání vhodného softwarového řešení. V zásadě existují dvě možnosti, které mají různé výhody i nevýhody. První spočívá v užívání komerčních nástrojů jako ChatGPT, Microsoft Copilot, Google Gemini nebo nespočet dalších. Jejich výhodou je jejich okamžitá dostupnost a poměrně nízká cena. Ve veřejné správě však narážejí na zásadní problémy s ochranou osobních údajů a kybernetickou bezpečností. Zároveň je nelze bezpečně napojit na stávající databáze obsahující osobní údaje o občanech. Navíc tyto nástroje mají často jen základní představu o českém právním systému a nespécializované AI neumí pracovat s judikaturou či odbornou literaturou, a současně se spoléhají převážně na volně dostupné online zdroje, a z důvodu ochrany autorských práv nemají vždy přístup ke komentářovým zněním či recenzované literatuře. Jejich plošné využívání se tedy omezuje spíše na podpůrné úkony jako kontrola pravopisu či jednoduché rešerše.

Druhou možností je vlastní národní software zaměřený přímo na český právní řád a konkrétní oblast. Ten bude mít větší možnost využití, pokud bude mít dostatečně zaručenou ochranu osobních údajů a dostatečné kybernetické zabezpečení. Jedná se ale o nákladný a zdoluhavý proces s možným rizikem selhání, podobně jako digitalizace stavebního řízení.

V neposlední řadě narážíme i na samotné technické limity umělé inteligence. V současnosti existuje pouze tzv. specializovaná AI, která umí řešit pouze jeden úkol a postrádá schopnost komplexního právního myšlení.²⁰ K tomu má AI tendenci

¹⁹ Data jsou dostupná z: DIGITÁLNÍ A INFORMAČNÍ AGENTURA: Služby veřejné správy – gov.cz. In: Portál.gov.cz [online] [cit. 09. 09. 2025]. Dostupné na: <https://portal.gov.cz/sluzby-verejne-spravy/>

²⁰ WIRTZ, Bernd W. – WEYERER, Jan C. – GEYER, Carolin: Artificial Intelligence and the Public Sector—Applications and Challenges. In: International Journal of Public Administration, Roč. 42, č. 7 (2019), s. 600.

generovat tzv. halucinace, tedy nepravdivé či zavádějící výstupy, aby se přiblížila maximálně zadání. Současné modely dokážou sumarizovat a vyhledávat informace, avšak nejsou schopni právního myšlení, tedy pracovat s právními normami, judikaturou a využívat plně lidského myšlení při práci s nimi.

Možné řešení je v systematické podpoře sdružování dat a aktivní propojování databází, aby se omezila jejich roztříštěnost. Nezbytné bude významně podpořit vývoj vlastních softwarů, které budou splňovat požadavky na bezpečnost a funkčnost. K tomu musíme klást důraz na vedení elektronických spisů a přispět správním orgánům finančně i personálně na digitalizaci, sdružování standardizovaných šablon i širší využívání formulářů, které zajistí jednotnost a usnadní zpracování pomocí AI.

Právní hledisko

Zásadní právní překážkou je absence právního zakotvení možnosti využívat umělou inteligence ve správním řízení. Český právní řád v současnosti neobsahuje žádné systematické ustanovení, které by umožňovalo či upravovalo využívání AI ve veřejné správě.

V roce 2025 byl připravován návrh novely správního řádu²¹, která měla v § 15a zakotvit možnost využívat automatizaci ve správním řízení a stanovit základní podmínky jejího využívání. Návrh však nebyl projednán před parlamentními prázdninami a s ohledem na blížící se volby nebyl legislativní proces této novely dokončen.

Určitou pozitivní zprávou je příprava zákona o umělé inteligenci, který má představovat národní implementaci evropského Aktu o AI. Podle dostupných informací by měl tento zákon rozpracovat pravidla stanovená na unijní úrovni v nařízení o AI. V době psaní článku se však návrh nachází teprve ve fázi mezirezortního připomínkového řízení, a jeho výsledná podoba zůstává nejistá.²²

V současnosti tak jedinými předpisy upravující AI jsou nařízení o AI a nařízení GDPR²³. Toto nařízení chrání především práva účastníků řízení při využívání automatizace. Především právo vědět, že a zda jsou jejich data zpracovávána automatizovaně²⁴ a současně právo nebyt předmětem výhradně automatizovaného rozhodování, pokud

²¹ Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“).

²² ODBOR KOMUNIKACE MPO: MPO připravilo návrh zákona o umělé inteligenci. Cílem je vytvořit co nejlepší prostředí pro rozvoj AI v Česku. In: Ministerstvo průmyslu a obchodu [online] [cit. 28.09.2025]. Dostupné na: <https://mpo.gov.cz/cz/rozcestnik/pro-media/tiskove-zpravy/mpo-pripravilo-navrh-zakona-o-umele-inteligenci--cilem-je-vytvorit-co-nejlepsi-prostredi-pro-rozvoj-ai-v-cesku--289653/>

²³ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „nařízení GDPR“).

²⁴ Viz čl. 15 nařízení GDPR.

má právní účinky nebo je významně ovlivňuje.²⁵ A dokud nebude přijata národní právní úprava, tak zůstane tato možnost účastníkům plně zachována.²⁶

Absence jasného legislativního rámce pro oblast veřejné správy vede k situaci, kdy správní orgány nemají jasně vymezené hranice využívání a závazná pravidla, která by jim umožnila využít AI bezpečně a v souladu se zásadami právního státu. Výsledkem je právní nejistota a riziko, že použití těchto nástrojů bude bráno jako nezákonné.

Další významnou překážkou je nestabilita českého legislativního prostředí. Legislativní proces se vyznačuje nedostatečně připravenými podklady pro rozhodování a tzv. přílepky²⁷, které kritizoval i Ústavní soud.²⁸

Na tento problém tedy navazují i časté novelizace předpisů, které tvoří celkovou nestabilitu právního systému. Pro ilustraci se lze podívat na nový stavební zákon²⁹. Ten byl přijat v roce 2021, ale již před přijetím byl dvakrát novelizován a po publikaci byl novelizován osmkrát.

Správní orgány i účastníci tak musí fungovat v dynamicky se měnícím prostředí, které je pro trénink a aplikaci AI problematické. V případě častých legislativních změn bude nutné systémy AI opakovaně přeučovat, což celý proces zpomalí a zvýší riziko chyb. AI nemusí správně vyhodnotit, které ustanovení je v daném okamžiku účinné, může, pracovat s neplatnou právní úpravou nebo naopak přehlížet nově zavedené instituty. V kombinaci s nedostatkem podpůrných materiálů a metodik pro řadu právních institutů tak hrozí, že se AI stane v běžné praxi nepoužitelnou.

Samostatnou kategorii tvoří otázky ochrany osobních údajů. AI bude muset nevyhnutelně pracovat s rozsáhlými databázemi a dokumenty obsahující osobní údaje, jejichž zpracování je přísně regulováno nařízením GDPR. Ale v nynějším právním prostředí bude AI narážet na limity tohoto nařízení.

Obzvláště problematické je zpracovávání tzv. citlivých údajů podle čl. 9 GDPR, jejichž automatizované zpracování je v zásadě znemožněno.³⁰ Toto pravidlo lze obejít tím, že do systémů se budou nahrávat anonymizovaná rozhodnutí bez těchto citlivých dat. Ale stále existuje riziko, že AI si tato data umí získat jiným způsobem a z neosobních dat vytvořit osobní.³¹ Zároveň je nutné zajistit, aby osoby pracující s těmito systémy byly při práci s citlivými údaji dostatečně proškoleny a dodržovaly

²⁵ Viz čl. 22 nařízení GDPR.

²⁶ Viz čl. 22 odst. 2 nařízení GDPR.

²⁷ Věcně a teleologicky nesouvisející pozměňovací návrh. Viz GERLOCH, Aleš – KYSELA, Jan – KÜHN, Zdeněk a kol.: *Teorie a praxe tvorby práva*. Praha: ASPI, 2008. Právní monografie. S. 217. ISBN 978-80-7357-362-1.

²⁸ Viz Nález Ústavního soudu ze dne 12. 2. 2002, sp. zn. Pl. ÚS 21/01 či Nález Ústavního soudu ze dne 15. 2. 2007, sp. zn. Pl. ÚS 77/06.

²⁹ Zákon č. 283/2021 Sb., stavební zákon, ve znění pozdějších předpisů (dále jen „stavební zákon“).

³⁰ Rozsudek Soudního dvora ze dne 27.6.2019 ve věci C-518/18 - C520/18.

³¹ HUBKOVÁ, Pavlína: *Automatizace ve správním rozhodování a soudní přezkum*. In: *Správní právo*, Roč. 2024, č. 6–7 (2024), s. 438.

pravidla. Navíc anonymizace znamená další krok, který bude nutné zajistit před implementací AI.

Zásadním limitem jsou osobní údaje při práci v komerčních nástrojích. Ty nejsou schopné zajistit dostatečnou ochranu těchto údajů, a proto je vhodné je využívat v oblastech, kde se s osobními údaji nepracuje či v anonymizovaných podobách dokumentů.

Poslední překážkou jsou nedokončené digitalizační procesy. Přestože Česká republika sice přijala zákon o právu na digitální služby³², který zaručuje fyzickým i právnickým osobám, že mohou se státem komunikovat digitálně. Ale práva plynoucí z něj nejsou účastníky příliš vynucována, což brzdí další digitalizaci veřejné správy.

Řešením, které je nutné přijmout co nejdříve, je přijetí komplexní právní úpravy, která vymezí podmínky a limity využívání AI a automatizace ve správním řízení, potažmo ve správním rozhodování. Je přitom irelevantní, zda se tak stane v rámci zákona o umělé inteligenci či v rámci jiného právního předpisu. Do budoucna by bylo vhodné i změnit kulturu legislativního procesu, aby více dodržovala principy právního státu. Dále je vhodné začít anonymizovat a připravovat podklady, které budou v souladu s nařízením GDPR a dokončit dosud rozpracované digitalizační projekty. Nezbytné je také důslednější vynucování zákona o právu na digitální služby, aby se z deklarovaného práva občanů stala v praxi skutečně vymahatelná povinnost státu.

Organizační a personální bariéry

Ačkoliv se v odborných debatách častěji zmiňují technické či právní překážky, nelze opomenout, že správní řízení ovládají hlavně úřední osoby, které budou nástroje AI využívat. Proto je nezbytné věnovat pozornost také bariérám organizačním a personálním.

V první řadě, česká veřejná správa se dlouhodobě potýká s nedostatkem kvalifikovaných pracovníků. Chybějí zejména odborníci na technických pozicích³³, kteří by dokázali AI systémy vyvíjet, udržovat a zjišťovat jejich chod. V praxi se tedy bude nutné spoléhat na služby soukromých společností, což může implementaci prodražit.

Výrazný personální deficit se projevuje i v běžných agendách, například stavební úřady se potýkají s obrovskými personálními problémy. A tento problém se bude

³² Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů.

³³ KABINET MÍSTOPŘEDSEDY VLÁDY PRO DIGITALIZACI: Kritický nedostatek ICT pracovníků ve veřejné správě. Praha: Digitální Česko, 2024. [online] [cit. 09. 09. 2025]. Dostupné na: [https://digitalnicesko.gov.cz/media/files/Kriticky%20nedostatek ICT pracovn%C3%ADk%C5%AF ve ve%C5%99ejn%C3%A9 spr%C3%A1v%C4%9B p4K8Plg.pdf](https://digitalnicesko.gov.cz/media/files/Kriticky%20nedostatek%20ICT%20pracovniku%20ve%20verejne%20sprave.pdf)

ještě prohlubovat z důvodu stárnutí úřednického aparátu.³⁴ Najít, a hlavně si udržet pracovníka, který bude odborně zdatný po stránce právní i technické, a zároveň ochotný pracovat za tabulkový plat, je nesmírně obtížné.

Další překážkou je absence metodické podpory. Úřední osoby nemají k dispozici manuály či metodiky, které by jim ukázaly, jak s umělou inteligencí zacházet, jak ji bezpečně využívat v řízení a jak se vyhnout rizikům, která se s jejím používáním pojí. Situace je podobná i v oblasti školení. Stávající vzdělávací akce jsou často příliš obecné a zaměřené spíše na popularizaci umělé inteligence nebo práci s komerčními aplikacemi³⁵, nikoli na skutečnou náplň práce úředních osob, kterou tvoří z většiny kontrola či psaní různých výstupů či jednání s lidmi. Je proto nutné, aby aktéři při implementaci AI do veřejné správy aktivně spolupracovali s lidmi ve veřejné správě, aby tento proces odpovídal jejich představám a požadavkům.

Na počátku může být užitečné, že úřední osoby získají alespoň základní zkušenosti s umělou inteligencí, což může představovat výhodu i pro samotné vývojáře. Je však podstatně vhodnější připravit školení zaměřená přímo pro potřeby úřední praxe s vhodnými nástroji.

Významným faktorem je i otázka důvěry v tuto novou technologii. Některé úřední osoby mohou AI používat nevhodně³⁶, přičemž si nemusí být vědomi všech možných rizik. Tento postoj je posilován tzv. automatizačním zkreslením³⁷, kdy osoby nekriticky přijmou řešení poskytnuté umělou inteligencí, a pokládají ho za lepší než vlastní řešení.³⁸

Naopak značná část úředních osob se k využívání AI staví až přesprávil skepticky, a to kvůli tzv. halucinování, ale i kvůli nejasnostem ohledně ochrany osobních údajů či

³⁴ MINISTERSTVO VNITRA: Analýza stárnutí zaměstnanců veřejné správy [online]. [cit. 27.09.2025]. Dostupné na: <https://mv.gov.cz/soubor/analyza-starnuti-zamestnancu-verejne-spravy-2020.aspx>

³⁵Viz Osnova kurzu. In: Úřad v kurzu [online] [cit. 12. 09. 2025]. Dostupné na: <https://www.uradvkurzu.cz/osnova/> nebo Umělá inteligence (AI) a její využití v praxi úřadů a jejich pracovníků. Využití AI v rámci veřejné správy. In: Vzdělávací centrum Morava [online] [cit. 12. 09. 2025]. Dostupné na: <https://www.vcmorava.cz/seminar/umela-inteligence-ai-a-jeji-vyuziti-v-praxi-uradu-a-jejich-pracovniku-173685>

³⁶ Nahrávají do systémů dokumenty obsahující osobní údaje či řeší konkrétní skutkové okolnosti případu v komerčních nástrojích.

³⁷ GILMAN, Michele: Poverty Lawgorithms. Data & Society, 2020, s. 6. Dostupné na: <https://datasociety.net/library/poverty-lawgorithms/>

³⁸ HUBKOVÁ, Pavlína: EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. In: AUC Iuridica, Roč. 70, č. 2 (2024), s. 101–119. Nejedná se ale o pravidlo, protože naopak někteří lidé naprosto záměrně ignorují výstup AI, protože neodpovídá jejich představě, viz STRAKOŠ, Jan: Právní aspekty automatizace ve správním trestání v kontextu strojového učení. In: Správní právo, Roč. 2024, č. 6–7 (2024), s. 485.

odpovědnosti.³⁹ A na základě toho odmítají jakýkoliv nástroj obsahující AI, i přesto že využívání AI by jejich práci zrychlilo či zefektivnilo. Ke zvýšení důvěry nepřispívá ani negativní zkušenost s digitalizací stavebního řízení ani s dalšími digitalizačními projekty.

S uvedeným úzce souvisí otázka odpovědnosti za rozhodnutí učiněná s využitím AI. Mnoho z nedostatků lze vyřešit skrze klasické opravné prostředky, kde bude nutné zajistit přítomnost člověka. V českém právním řádu odpovědnost za škodu způsobenou výkonem veřejné moci primárně leží na státu nebo územním samosprávném celku, který odpovídá za škodu způsobenou nezákonným rozhodnutím či nesprávným úředním postupem. Možný regres vůči konkrétní úřední osobě přichází v úvahu pouze tehdy, pokud se prokáže zaviněné porušení povinností. V případě chyb v systému AI, které nelze přičíst konkrétní osobě, se uvažuje o sdílené odpovědnosti vývojářů systémů AI, avšak toto řešení zatím nemá oporu v právní úpravě.⁴⁰

Možnými řešeními těchto problémů je zejména zaměření se na vytvoření dostatečných metodických pokynů a personalizovaných školení pro úřední osoby, které budou postupně zvyšovat důvěru těchto osob v umělou inteligenci, ale zároveň subjekty seznámí s možnými riziky.

Zároveň je nutné zvyšovat kvalifikaci pracovníků a podpořit zaměstnávání odborníků, hlavně v oblasti informačních technologií. Důležité je i najisto postavit otázku odpovědnosti za rozhodnutí učiněná s využitím AI.

Závěr

Překážek bránících širšímu využívání umělé inteligence jsem v příspěvku představila celou řadu. Nejvýraznější problémy lze spatřovat v oblasti dat a digitalizace, absence právního zakotvení možnosti využívání AI ve veřejné správě a nedostatku vzdělávací a metodické podpory úředních osob. Tyto bariéry jsou přitom zásadně řešitelné v krátkodobém horizontu, a v České republice již existují snahy o jejich překonání, ať se jedná o práci na nových právních úpravách, podpory sběru dat i přípravy vzdělávání. Lze proto očekávat, že tyto překážky budou během několika let eliminovány.

Dlouhodobějším problémem je pomalý proces digitalizace, nestabilita a nesrozumitelnost právního řádu a otázky důvěry úředních osob v systémy AI. Tyto

³⁹ SOUSA, Wesley Gomes de et al.: How and Where is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda. In: Government Information Quarterly, Roč. 36, č. 4 (2019), s. 2.

⁴⁰ WIRTZ, Bernd W. – WEYERER, Jan C. – GEYER, Carolin: Artificial Intelligence and the Public Sector—Applications and Challenges. In: International Journal of Public Administration, Roč. 42, č. 7 (2019), s. 606.

překážky mají hlubší systémový charakter a jejich odstranění vyžaduje větší změnu přístupu a koordinaci napříč jednotlivými aktéry.

Je proto znovu nutné zdůraznit, že řešení překážek je nutné provádět provázaně. Úspěšná implementace umělé inteligence závisí na promyšleném postupu, který propojí právní, technické i organizační aspekty. Ale pokud se podaří tyto překážky překonat, může se z umělé inteligence vytvořit nástroj, který posune veřejnou správu vpřed do digitálního věku.

Zoznam použitej literatury

1. DIGITÁLNÍ A INFORMAČNÍ AGENTURA: Katalog využití umělé inteligence ve veřejném sektoru. In: Digitální a informační agentura [online] [cit. 27.09.2025]. Dostupné na: <https://egovai.dia.gov.cz/>
2. DIGITÁLNÍ A INFORMAČNÍ AGENTURA: Služby veřejné správy – gov.cz. In: Portál.gov.cz [online] [cit. 09. 09. 2025]. Dostupné na: <https://portal.gov.cz/sluzby-verejne-spravy/>
3. EVROPSKÁ VESMÍRNÁ AGENTURA: DROMAS | ESA Space Solutions. In: European Space Agency [online] [cit. 27.09.2025]. Dostupné na: <https://business.esa.int/projects/dromas>
4. FIALOVÁ, Eva – MATEJKA, Ján – GÜTTLER, Vojen: Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod. Praha: Ústav státu a práva AV ČR, v. v. i., 2020. 78 s. ISBN 978-80-87439-42-5.
5. GERLOCH, Aleš – KYSELA, Jan – KÜHN, Zdeněk et al.: Teorie a praxe tvorby práva. Praha: ASPI, 2008. Právní monografie. ISBN 978-80-7357-362-1.
6. GILMAN, Michele: Poverty Lawgorithms [online]. [cit. 06.03.2025]. Dostupné na: <https://datasociety.net/library/poverty-lawgorithms/>
7. HUBKOVÁ, Pavlína: Automatizace ve správním rozhodování a soudní přezkum. In: Správní právo, Roč. 2024, č. 6–7 (2024), s. 435–451.
8. HUBKOVÁ, Pavlína: EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. In: AUC Iuridica, Roč. 70, č. 2 (2024), s. 101–119.
9. KABINET MÍSTOPŘEDSEDY VLÁDY PRO DIGITALIZACI: Kritický nedostatek ICT pracovníků ve veřejné správě. Praha: Digitální Česko, 2024. [online] [cit. 09. 09. 2025]. Dostupné na: https://digitalnicesko.gov.cz/media/files/Kritick%C3%BD_nedostatek_ICT_pracovn%C3%ADk%C5%AF_ve_ve%C5%99ejn%C3%A9_spr%C3%A1v%C4%9B_p4K8PIg.pdf
10. LEGG, Shane – HUTTER, Marcus: A Collection of Definitions of Intelligence. In: Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms, Roč. 157, (2007).

11. MĚSTSKÁ ČÁST PRAHA 8: Úřad MČ Praha 8: Informace z úřadu – V Praze 8 řeší přestupky za špatné parkování softwarový robot. In: Městský úřad Praha 8 [online] [cit. 27.09.2025]. Dostupné na: <https://m.praha8.cz/v-praze-8-resi-prestupky-za-spatne-parkovani-softwarovy-robot-1.html>
12. MINISTERSTVO VNITRA: Analýza a zhodnocení potenciálu využití automatizace a umělé inteligence v agendách veřejné správy. Praha: Ministerstvo vnitra ČR, 2023. 80 s. [online] [cit. 1. 9. 2025]. Dostupné na: <https://www.mvcr.cz/soubor/analyza-a-zhodnoceni-potencialu-vyuziti-automatizace-a-umele-inteligence-v-agendach-verejne-spravy.aspx>
13. MINISTERSTVO VNITRA: Analýza stárnutí zaměstnanců veřejné správy [online]. [cit. 27.09.2025]. Dostupné na: <https://mv.gov.cz/soubor/analyza-starnuti-zamestnancu-verejne-spravy-2020.aspx>
14. NEJEDLÝ, Matěj: AI v české státní správě? Když zaspíme, ekonomika neporoste, varují experti. In: Seznam Zprávy [online] [cit. 27.09.2025]. Dostupné na: <https://www.seznamzpravy.cz/clanek/domaci-ai-v-ceske-statni-sprave-kdyz-zaspime-ekonomika-neporoste-varuji-experti-263061>
15. ODBOR KOMUNIKACE MPO: Další krok k rozvoji umělé inteligence v Česku. Vláda schválila návrh na zajištění implementace AI Aktu, novým gestorem je MPO. In: Ministerstvo průmyslu a obchodu [online] [cit. 27.09.2025]. Dostupné na: <https://mpo.gov.cz/cz/rozcestnik/pro-media/tiskove-zpravy/dalsi-krok-k-rozvoji-umele-inteligence-v-cesku--vlada-schvalila-navrh-na-zajisteni-implementace-ai-aktu--novym-gestorem-je-mpo--287763/>
16. ODBOR KOMUNIKACE MPO: MPO připravilo návrh zákona o umělé inteligenci. Cílem je vytvořit co nejlepší prostředí pro rozvoj AI v Česku. In: Ministerstvo průmyslu a obchodu [online] [cit. 28.09.2025]. Dostupné na: <https://mpo.gov.cz/cz/rozcestnik/pro-media/tiskove-zpravy/mpo-pripravilo-navrh-zakona-o-umele-inteligenci--cilem-je-vytvorit-co-nejlepsi-prostredi-pro-rozvoj-ai-v-cesku--289653/>
17. OECD: Artificial Intelligence in Society [online]. Paris: OECD Publishing, 2019. 152 s. ISBN 978-92-64-58254-5.
18. PARYCEK, Peter – SCHMID, Verena – NOVAK, Anna-Sophie: Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. In: Journal of the Knowledge Economy, Roč. 15, č. 2 (2024), s. 8390–8415.
19. POLČÁK, Radim: Umělá inteligence ve správní praxi. In: Správní právo, Roč. 2024, č. 6–7 (2024), s. 452–462.
20. SKALICKÝ, Matěj: Digitalizace není v Česku prioritou, mrzí experta. K posouzení DSŘ prý chybí dostatek dat. [online] [cit. 27.09.2025]. Dostupné na: <https://plus.rozhlas.cz/digitalizace-neni-v-cesku-priorita-mrzi-experta-k-posouzeni-dsr-pry-chybi-9328268>

21. SOUSA, Wesley Gomes de et al.: How and Where is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda. In: Government Information Quarterly, Roč. 36, č. 4 (2019), s. 1-14.
22. STAŠA, Josef: Umělá inteligence z pohledu (naší) veřejné správy. In: Správní právo, Roč. 2024, č. 6–7 (2024), s. 468–474.
23. STRAKOŠ, Jan: Právní aspekty automatizace ve správním trestání v kontextu strojového učení. In: Správní právo, Roč. 2024, č. 6–7 (2024), s. 475–490.
24. SURDEN, Harry: Machine Learning and Law: An Overview. In: Research Handbook on Big Data Law. Stanford: Edward Elgar Publishing, 2021, s. 171–184. ISBN 978-1-78897-282-6.
25. VLÁDA ČR: Národní strategie umělé inteligence České republiky 2030. [online] Praha. [cit. 30. 10. 2024]. Dostupné na: <https://www.mpo.gov.cz/assets/cz/podnikani/2024/9/Narodni-strategie-umele-intelligence-CR-2030.pdf>
26. WIRTZ, Bernd W. – WEYERER, Jan C. – GEYER, Carolin: Artificial Intelligence and the Public Sector—Applications and Challenges. In: International Journal of Public Administration, Roč. 42, č. 7 (2019), s. 596–615.

Kontaktné údaje

Mgr. Kateřina Ištuková

509048@mail.muni.cz

Katedra správní vědy a správního práva Právnické fakulty Masarykovy univerzity

OZBROJENÝ ĽUD...NIE, ŽANDÁRSTVO

ARMED PEOPLE... NOT GENDARMERIE

Tomáš Rulíšek¹

Abstrakt: Tematické zameranie príspevku je motivované zmenami právnej úpravy v oblasti policajnej správy, ktoré sa aktuálne realizujú v dôsledku nadobudnutia účinnosti zákona č.150/2025 Z. z. o niektorých opatreniach na zvýšenie odolnosti v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene a doplnení niektorých zákonov. Prevažná časť rozboru skúmanej problematiky sa venuje organizačnému poňatiu novozavedeného subjektu policajnej správy, ktorým je Žandársky zbor. S využitím historicko-právnej a komparatívnej metódy sa poukazuje na podobnosti ako aj rozdielnosti novej zákonnej úpravy žandárstva s historickým organizačným modelom tejto súčasti policajnej správy v slovenských podmienkach. Rozhodujúca časť analýzy dotknutej právnej úpravy sa týka organizačných, riadiacich a kontrolných mechanizmov zavedených pre novozriadený Žandársky zbor, a to zároveň v spojitosti s funkčnými väzbami na iné subjekty policajnej správy, najmä Policajný zbor a Vojenskú políciu. Súčasťou analýzy je tiež snaha o vysvetlenie vplyvu zákonodarcom zvoleného modelu organizácie a riadenia Žandárskeho zboru na podobu normatívneho vymedzenia jeho vecnej, personálnej a územnej pôsobnosti, a v konečnom dôsledku na zmenu koncepčného prístupu bezpečnostnej politiky charakterizovanú militarizáciou policajnej správy a „spolicajnením“ správy obrany. Kritický náhľad na viaceré ustanovenia novej zákonnej úpravy si kladie za cieľ stimulovať odbornú diskusiu týkajúcu sa efektivity verejno-poriadkového a verejno-bezpečnostného pôsobenia štátu v súčasnom vnútrobezpečnostnom prostredí štátu.

Kľúčové slová: policajná správa, Policajný zbor, Vojenská polícia, Žandársky zbor

Abstract: The topic of this entry is motivated by the legal changes in the field of Police administration that are currently taking place as a result of Act no. 150/2025 Coll. on measures to increase the abilities of the state to defend and secure itself, on civil defense education, on modifications and amendments to certain laws. The majority of the examined issues focus on the organizational

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra správneho práva a environmentálneho práva.

concept of the newly established police administration entity, the Gendarmerie Corps. Using historical-legal and comparative methods, it highlights the details and differences between the new legal regulation of the gendarmerie and the historical organizational model of this part of the police administration in the context of Slovakia. A crucial part of the analysis of the relevant legislation concerns the organizational, management, and control mechanisms for the newly established Gendarmerie Corps, in conjunction with functional links to other police administration entities, in particular the Police Corps and the Military Police. The analysis also attempts to explain the impact of the model of the organization and management of the Gendarmerie chosen by the legislator on the normative definition of its material, personnel, and territorial jurisdiction, and ultimately on the change in the conceptual approach to security policies characterized by the militarization of the police administration and "policing" of defense administration. A critical review of several provisions of the new legislation aims to stimulate professional discussion on the effectiveness of the state's public order and public security activities in the current internal security environment of the state.

Key words: Police Administration, Police Force, Military Police, Gendarmerie Corps

Úvod

Pri teoretickom skúmaní rovnako ako pri vyhodnocovaní stavu aplikačnej praxe sa naša pozornosť často zameriava na funkčné poňatie plnenia štátno-správnych úloh. Je to prirodzené, veď efektivitu činnosti vykonávateľov verejnej správy vo všeobecnosti zvykneme merať podľa kvalitatívnych a kvantitatívnych ukazovateľov fungovania orgánov verejnej správy. Okrem prípadov verejnej kritiky existencie niektorých ústredných orgánov štátnej správy, ktorá je často skôr výsledkom politického kalkulu a nie vždy spoločenskou potrebou, však v tomto procese skúmania už menej rezonuje zohľadnenie organizačnej stránky výkonu správnych činností. Pritom statické poňatie verejnej správy je rovnako ako to funkčné základom pre dosiahnutie legitímneho očakávania verejnosti, že sa verejná správa bude vykonávať efektívne.

Úvaha k spoločenskej potrebe zriadiť Žandársky zbor

Dynamika legislatívnych prác v oblasti administratívno-politickej správy je notorietou, ktorá odráža nielen spoločenskú objednávku vyvolanú problémami či požiadavkami praxe, ale tiež neutíchajúcim apetítom politikov meniť administratívno-právny rámec štátnych funkcií v tejto správe. Jednou zo zložiek

administratívno-politickej správy, ktorá je tým poznačená je policajná správa a správa obrany. Silný politický prvok prítomný v tejto časti verejnej správy spojený so spoločenskou citlivosťou jej vnímania obyvateľstvom je zdrojom politickej atraktivity aj kontroverzií a preto tu má legislatíva občas sklon k experimentovaniu, čo nebýva pre stabilitu právnej regulácie spravidla dobrá správa. Na druhej strane obe správy v praxi zaznamenávajú veľmi dynamicky sa meniacu realitu, keď je bezpečnostné prostredie štátu vystavené rýchlo sa meniacim materiálnym podmienkam odrážajúcim nové a meniace sa bezpečnostné hrozby a výzvy. Od štátu sa legitímne očakáva schopnosť ochrániť bezpečnosť štátu a spoločnosti na požadovanej úrovni a z tohto dôvodu musí byť štát dostatočne rezistentný k ohrozeniam, ktorým čelí. Jedným z pokusov štátu dosiahnuť potrebnú mieru odolnosti je aj schválenie zákona o niektorých opatreniach na zvýšenie odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene doplnení niektorých zákonov.²

Dosiahnutie politického konsenzu potrebného na prijatie tohto zákona v zákonodarnom zbore sa nerodilo bez problémov, čo preukazujú najmä pozmeňovacie návrhy poslanca Tomáša Valáška³ a Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť⁴, ale tiež pripomienky, ktoré už počas legislatívneho procesu v štádiu pred predložením návrhu zákona uplatnil napr. verejný ochranca práv.⁵

Pred prijatím zákona snád' najviac rezonovala výmena názorov na to opatrenie zavádzané novou zákonnou úpravou, ktorého primárnym cieľom pri zvyšovaní odolnosti štátu v oblasti obrany a bezpečnosti je činnosť tzv. Žandárskeho zboru. Tá má za cieľ, ako deklaruje predkladateľ v dôvodovej správe, podporovať Policajný zbor najmä pri zabezpečovaní verejného poriadku. To napokon v schválenej a publikovanej verzii našlo svoj odraz aj v spojení novej zákonnej úpravy s vymedzením vecnej pôsobnosti Policajného zboru podľa § 2 zákona NR SR č. 171/1993 z. z. Hoci dôvodová správa a dokonca ani vymedzenie predmetu zákona v základných

² Zákon č. 150/2025 Z. z. o niektorých opatreniach na zvýšenie odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene doplnení niektorých zákonov.

³ Pozmeňujúci a doplňujúci návrh poslanca Národnej rady Slovenskej republiky Tomáša Valáška k vládnemu návrhu zákona o niektorých opatreniach na zvýšenie odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene doplnení niektorých zákonov (tlač 716) [online]. [cit. 2025-09-11]. Dostupné z:

<https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=566075>

⁴ Spoločná správa (716a) [online]. [cit. 2025-09-11]. Dostupné z:

<https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=566006>

⁵ VEREJNÝ OCHRANCA PRÁV: V ZÁKONE O ŽANDÁRSTVE NAVRHUJEM VYŠŠIE GARANCIE ĽUDSKÝCH PRÁV [online]. Bratislava, 28.01. 2025, [cit. 2025-9-11].

Dostupné z:

<https://vop.gov.sk/wp-content/uploads/2025/01/Tlacova-sprava-VOP-28.-01.-2025.pdf>

ustanoveniach na to nereflektujú ⁶, napokon sa do zákonnej úpravy dostali aj ustanovenia týkajúce sa podpory nielen Policajného zboru ale aj Vojenskej polície, čo ako sa zdá, bolo motivované aj logistickými aspektami spojenými s vytvorením Žandárskeho zboru. Podpora plnenia úloh Policajného zboru je explicitne vyjadrená v ust. § 1 ods. 2 písm. b) zákona v spojení s § 22 ods. 1 zákona.

A tak sa v objektívnom práve objavuje nová súčasť, ktorá si v ďalšej aplikačnej praxi musí nájsť miesto v sústave subjektov policajnej správy v Slovenskej republike. Aj bez ohľadu na verejne či mediálne komunikované výhrady niektorých poslancov Národnej rady, spájajúcich novú zákonnú úpravu žandárstva s údajne negatívnym obrazom tohto historického orgánu štátnej politickej správy⁷ povereného výkonom bezpečnostnej služby⁸ je potrebné považovať širšiu odbornú debatu o skutočnej potrebe žandárov a následne vhodnej podobe tohto komplementárneho vykonávateľa verejno-poriadkových funkcií policajnej správy v súčasnosti za prinajmenšom prínosnú.

Keďže bezpečnosť je premenlivá spoločenská hodnota, stalo sa akousi notoriou, že Policajný zbor ako najvýznamnejší bezpečnostný ozbrojený zbor čelí s meniacim sa vnútrobezpečnostným prostredím stále narastajúcim výzvam organizačného, logistického a z hľadiska početných stavov svojho personálneho substrátu aj značnej deficiencii. Najnovšie štatistiky uvádzajú, že len v Bratislavskom kraji chýba takmer 600 policajtov. ⁹

Policajná správa je v slovenských podmienkach jednou z kľúčových zložiek administratívno-politickej správy.¹⁰ Je to oblasť, v ktorej sa výrazne prejavuje *inter alia* realizácia jednej z najdôležitejších funkcií exekutívnej zložky štátnej moci a to zaistovanie verejnej bezpečnosti a verejného poriadku. Práve v tejto časti sa s vysokou intenzitou aj rozsahom uplatňujú mocenské zásahy do individuálnych práv a slobôd jednotlivcov, vrátane základných práv a slobôd. Použitie legitímneho násillia na dosiahnutie účelu policajných činností smerom do vnútra štátu a spoločnosti je tradičnou súčasťou vnímania policajného pôsobenia a to už od inštitucionálnej separácie polície od iných ozbrojených zložiek štátnej moci, najmä ozbrojených síl.

⁶ § 1 ods. 2 písm. b) zákona č. 150/2025 Z. z.

⁷ BOHATA, I. Protidivná úloha četnictva v letech 1918-1938. 1. vydanie: Praha, Východočeské tiskárny, 1978. s. 8.

⁸ Pozri § 2 zákona č. 299/1920 Sb. o četnictvu.

⁹ Rezort vnútra predĺžil novým policajtom povinnú službu v Bratislave. Chce tak riešiť ich nedostatok, odborári to kritizujú [online]. 18.03. 2025, [cit. 2025-9-11].

Dostupné z:

<https://spravy.stvr.sk/2025/03/novi-policajti-budu-moct-sluzit-dva-roky-v-bratislave-stat-tak-chce-riesit-ich-nedostatok-odborari-zmenu-kritizuju/>

¹⁰ VRABKO, M. a kol. Správne právo hmotné. Osobitná časť. 3. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2017. s. 126.

Vykonávatelia verejnej správy na úseku verejnej bezpečnosti a verejného poriadku predstavujú vertebrálny pilier organizačného poňatia systému štátnomocenského riadenia spoločnosti ako aj presadzovania práva, a to práve v tých oblastiach, ktoré sa často vyznačujú preferenčným režimom verejného záujmu v konfrontácii s individuálnymi záujmami jednotlivca v spoločenských vzťahoch. Stabilita bezpečnostného aparátu štátu je na jednej strane závislá od koncepčných riešení pružne reagujúcich na aktuálne bezpečnostné prostredie doma aj v zahraničí. Na strane druhej by však podoba tohto aparátu mala mať solídny a historicky overený základ. Žiaľ práve zmeny spoločensko-politických a ústavných pomerov opakovane spôsobili v slovenských podmienkach diskontinuitu vo vývoji bezpečnostného aparátu štátu, ktorá stabilite neprospieva. Pri voľbe nesprávneho riešenia to potom platí aj o zavádzaní resp. znovu-zavádzaní žandárstva do sústavy subjektov policajnej správy.

Ak bola vyššie položená hypotéza týkajúca s potrebnosti takéhoto doplnenia sústavy subjektov policajnej správy, potom sa naskytuje podotázka, či ide o zavedenie nového subjektu policajnej správy formou znovuzrodenia žandárstva ako bezpečnostného orgánu, ktorý na Slovensku existoval pred centralizáciou bezpečnostného aparátu pred rokom 1947¹¹ resp. pred účinnosťou nariadenia predsedníctva Slovenskej národnej rady č. 6/1945 Zb. n. SNR z 23. februára 1945, ktorým boli rozpustené žandárske organizácie v súvislosti s vytvorením organizácie bezpečnostnej služby zriadenej nariadením predsedníctva SNR č. 71/1945 Zb. n. Teda či, sa zákonodarca v súčasnosti inšpiruje historickou právnou úpravou, alebo ide o vytvorenie „novotvaru“, ktorému sa dáva len starý názov. S cieľom porozumieť podobnostiam alebo naopak rozdielom medzi súčasným žandárskym zborom a historickým žandárstvom je namieste venovať aspoň čiastočne pozornosť správnej vedy deskripcii právnej úpravy československého četníctva najmä v období tzv. Prvej republiky.

Pri oboch spomenutých možnostiach je ale určite namieste otázka, či má policajná správa z hľadiska organizačného poňatia „trhlinu“, ktorej scelenie je možné len doplnením nového subjektu bezpečnostného aparátu štátu a s právnym vymedzením úloh verejno-poriadkového charakteru.

Organizácia, riadenie a kontrola Žandárskeho zboru

Vychádzajúc z dôvodovej správy ako aj z pozorovania priebehu verejnej diskusie v rámci legislatívneho procesu je nepochybné, že primárnym cieľom novej zákonnej úpravy je vytvoriť právny režim regulácie takých opatrení, ktoré by priniesli zvýšenie

¹¹ Abrogácia zákona č. 299/1920 Sb. o četníctvu v znení zákona č. 28/1928 Sb. a niektorých právnych predpisov, ktoré prijali zákonodarne orgány Slovenskej republiky medzi rokmi 1939 až 1945, osobitne zákon č. 48/1944 Sl. z. o žandárstve.

odolnosti štátu v oblasti obrany a bezpečnosti. Návrh zákona vyšiel z dielne ministerstva obrany Slovenskej republiky a tak je prirodzené, že primárny cieľ novej právnej úpravy sa týka správy obrany. Kvalitatívne najdôležitejšou zmenou oproti doterajšiemu stavu odolnosti štátu voči novým bezpečnostným ohrozeniam v oblasti obrany je vytvorenie tzv. Národných obranných síl, ktoré nahrádzajú doterajší systém ozbrojených síl. Z administratívnoprávneho hľadiska tak nová právna úprava mení reguláciu nielen brannej povinnosti ako projekcie čl. 25 Ústavy Slovenskej republiky, ale vytvára tiež nový právny základ pre organizáciu personálneho substrátu obranných kapacít štátu podľa druhu krízovej situácie, či už vyvolanej vojenským alebo nevojenským ohrozením bezpečnosti štátu.

Schválená podoba zákona však zavádza nové opatrenia na zvýšenie odolnosti štátu aj v oblastiach, ktoré nie sú vojenskou zložkou bezpečnosti štátu ako právom chránenej hodnoty, ale týkajú sa skôr zabezpečovania verejného poriadku, tradične predstavujúceho objekt ochrany policajnej správy. Z organizačného hľadiska má byť takýmto opatrením činnosť Žandárskeho zboru a to v rozsahu ustanovenom týmto zákonom.¹²

Presahy inštitucionálnych prvkov vojenskej súčasti bezpečnostnej správy do policajnej správy relativizujú systém vyznačujúci sa separáciou obranných a policajných činností, ktorý bol v našich podmienkach zavádzaný po roku 1989 v dôsledku zmien spoločensko-politických pomerov. Tie odmietali militarizovanú podobu polície v kontraste s tou, s ktorou predtým počítala posledná zákonná úprava Zboru národnej bezpečnosti.¹³

V tomto zmysle nemožno nevidieť určitý návrat k filozofii organizácie bezpečnostnej správy, ktorý v podmienkach československého štátu existoval dokonca pred vytvorením Zboru národnej bezpečnosti a ktorú charakterizoval dualizmus rezortnej subordinácie. Žandárstvo (četníctvo)¹⁴ bolo vo vojenských veciach a disciplinárnych veciach podriadené vrchnému vojenskému veliteľovi, v služobných otázkach ministrovi vnútra.¹⁵ Nová právna úprava podriaďuje žandára pod organizačnú, riadiacu a kontrolnú činnosť útvaru Policajného zboru podľa miesta zaradenia (resp. Vojenskej polície, ak sa spolupodieľa na plnení jej úloh), avšak odborné, organizačné

¹² § 1 ods. 2 písm. b) zákona č. 150/2025 Z. z.

¹³ Medzi základne úlohy Zboru národnej bezpečnosti podľa § 4 zákona č. 40/1974 Zb. o Zbore národnej bezpečnosti patrilo aj spolupôsobenie pri obrane československej socialistickej republiky, pričom zbor bol organizovaný podľa vojenských zásad (§8 zákona č. 40/1974 Zb.).

¹⁴ V slovenských podmienkach bol názov četníctvo zmenený na žandárstvo vyhláškou prezídia MV č. 246/1939 zo dňa 6. októbra 1939.

¹⁵ Zemandlová, L. Polícia a četníctvo na našom území v rokoch 1848- 1918 (historicko-právne aspekty). [online]. [cit. 2025-09-11]. Dostupné z:

<https://www.akademiapz.sk/sites/default/files/OVVP/009%20%20ZEMANDLOVA%20%20Bezpecnostne%20zlozky%20na%20nasom%20uzemi%20v%20rokoch%201848.pdf>

a technické zabezpečenie Žandárskeho zboru zveruje Vojenskej polícii.¹⁶ Aj v nadväznosti na nižšie rozoberané otázky prelínania sa policajnej správy so správou obrany možno podotknúť, že tu je v porovnaní s historickou zákonnou úpravou zásadný rozdiel. Československé četníctvo, hoci poznačené už spomenutou dualitou subordinácie podliehalo ministerstvu vnútra, ako zakotvovala právna úprava „v poslednej inštancii“ a to tak vo veciach plnenia úloh (vtedy vecne správne označovaných ako bezpečnostná služba-pozn. autora) ako aj v podporných záležitostiach (výcvik, disciplína, kontrola služby, materiálne zabezpečenie). Dohodu ministerstva vnútra a ministerstva národnej obrany zákon vyžadoval len v otázke výzbroje četníctva.¹⁷ Napriek tomu aj v podmienkach historického žandárstva zaznamenávame spory medzi československým Ministerstvom národnej obrany a Ministerstvom vnútra, ktoré by sme dnes nazvali kompetenčnými spormi. Tieto spory vychádzali zo zdedených problémov bezpečnostného aparátu Rakúsko-Uhorska, ktorý bol na základe tzv. recepčnej normy¹⁸ prevzatý aj v československej sústave bezpečnostných orgánov. Žandárstvo bolo podľa recipovanej právnej úpravy vojenským jednotným strážnym zborom zriadeným za účelom zachovávanía verejného poriadku a bezpečnosti¹⁹ a táto „hybridná“ charakteristika bola zdrojom viacerých sporov na úrovni vtedajšej ústrednej politickej správy novovzniknutého československého štátu. V slovenských podmienkach bola navyše situácia okolo žandárstva kompetenčne ešte zmätočnejšia, pretože posledná „predrepubliková“ zákonná úprava definovala žandárstvo ako vojensky organizovaný, ministerstvu vnútra a obrany podriadený zbor.²⁰ Podriadenie žandárstva ministerstvu vnútra, ktoré malo v pôsobnosti bezpečnostné záležitosti štátu podľa novovytvorenej sústavy najvyšších správnych úradov²¹ presadil prvý minister vnútra Antonín Švehla²² a prvá zákonná úprava v československých podmienkach to definitívne potvrdila.²³ Napriek tomu, prakticky v celej ére existencie historického československého žandárstva bolo na tento zbor obyvateľstvom nahliadané ako na vojenský zbor a súčasť tzv. brannej moci, čo bolo umocnené pridelením štábného dôstojníka československého vojska k žandárstvu za účelom podpory žandárov plniť úlohy spojené s vonkajším (vojenským) ohrozením štátu.²⁴ Zároveň sa však otázka

¹⁶ § 22 ods. 5 zákona č. 150/2025 Z. z.

¹⁷ § 3 zákona č. 299/1920 Zb.

¹⁸ Zákon č. 11/1918 Zb. z. a nar. o zriadení samostatného štátu Československého.

¹⁹ § 1 zákona č. 1/1895 r. z. o četníctve.

²⁰ Zák. čl. 3/1881 r. z.

²¹ § 1 zákona č. 2/1918 Zb. z. a n., ktorým sa zriaďujú najvyššie správne úrady v štáte československom.

²² JANÁK, J., HLEDÍKOVÁ, Z., Dobeš J. Dějiny správy v českých zemích od počátku štátu po současnost. Praha: Nakladatelství Lidové noviny, 2005. s. 413.

²³ § 2 zákona č. 299/1920 Zb.

²⁴ § 4 zákona č. 299/1920 Zb.

organizačnej podriadenosti ministerstvu vnútra právne vyriešila a žandárstvo bolo zákonne ukotvené ako orgán politickej štátnej správy. Na čele československého četníctva bol generálny veliteľ četníctva s hodnosťou generála, ktorý disponoval na výkon funkcie poverením prezidenta republiky a pochádzal z dôstojníckeho zboru četníctva.²⁵

Historický exkurz tu podávam preto, lebo poznanie historických reálií by malo byť zdrojom poučenia pri koncipovaní súčasnej podoby právnej úpravy aj organizačnej stránky tejto súčasti administratívno-politickej správy.

Napriek tomu, že zákon výslovne pomenúva Žandársky zbor, nijakým spôsobom ho nedefinuje. Tým, že zákonodarca zvolil model, podľa ktorého žandár plní úlohy mimo služobného času alebo v čase preventívnej rehabilitácie vykonávanej formou aktívneho odpočinku alebo pravidelného cvičenia vojaka operačných záloh, vznikol síce právny základ pre fungovanie tohto zboru, ale zároveň sa javí ako akási „fikcia“ a nie zákonom zriadená entita, ktorá má byť novou zložkou polície.

Je tu jednoznačný rozdiel od iných zložiek polície, keď zákon NR SR č. 171/1993 Z. z. o Policajnom zbore tento definuje ako ozbrojený bezpečnostný zbor a odhliadnuc od pretrvávajúcej polemiky o jeho ne/zaradení do sústavy orgánov štátnej správy, je Policajný zbor zákonne definovaný a ako taký je zároveň podriadený ministrovi vnútra Slovenskej republiky. To je spôsob, akým zákonodarca vyriešil riadenie Policajného zboru. Táto právna úprava je spojená s organizáciou ústrednej štátnej správy a zákonným zakotvením postavenia Ministerstva vnútra Slovenskej republiky ako ústredného orgánu štátnej správy pre Policajný zbor podľa § 11 písm. c) zákona č. 575/2001 Z. z. Podobne ako Policajný zbor, aj Vojenská polícia ako ďalšia zo štátnych zložiek polície má podľa osobitnej právnej úpravy definičné vymedzenie ako policajnej služby, pričom zákon organizáciu Vojenskej polície upravuje formou priamej podriadenosti jej riaditeľovi ministrovi obrany Slovenskej republiky.²⁶ V prípade Žandárskeho zboru však obdobná definícia absentuje úplne, čo možno považovať za nedostatok novej zákonnej úpravy, a len teoretickým vymedzením odvodeným od vecnej povahy zákonom zverených úloh a povinností žandára sa dá definovať ako štátna zložka polície. Je potrebné poznamenať, že Žandársky zbor bude pôsobiť navonok voči jednotlivcom ako v policajnej správe spravovaným subjektom a to napr. formou zákroku spojeného s bezprostredným zásahom do základných práv a slobôd.²⁷ Žandárom sa zákonom priznávajú viaceré, pre policajnú správu typické oprávnenia podľa § 26 až 35, vrátane oprávnenia na použitie donucovacích prostriedkov. Okrem zákrokov došlo aj k novelizovanej úprave prejednávania priestupkov v blokovom konaní, kde sa uvedené zveruje žandárom pre

²⁵ § 2 štvrtá veta zákona č. 299/1920 Zb.

²⁶ § 4 ods. 2 druhá veta zákona č. 124/1992 Zb. o Vojenskej polícii.

²⁷ § 25 ods. 3 a 4 zákona č. 150/2025 Z. z.

viaceré priestupky.²⁸ Za zmienku preukazujúcu priznanie oprávnení policajnej povahy je napríklad doplnenie povinnosti štátnych príslušníkov tretej krajiny v rámci regulácie cudzineckého režimu preukázať totožnosť a oprávnenosť pobytu na území Slovenskej republiky žandárovi, pri plnení úloh Žandárskeho zboru.

Výkon policajnosprávnej činnosti si tiež vyžaduje zákonom predpokladanú prezentáciu smerom navonok, či už znakmi rovnošaty vyjadrujúce príslušnosť k Žandárskemu zboru, preukazom žandára a ústnym vyhlásením podľa § 24 zákona. Zákon podobne ako v prípade služobných zákrokov príslušníkov Policajného zboru predpokladá tiež použitie slov „v mene zákona“. Zákon predpokladá požívanie označenia „ŽANDÁRI“ aj na vozidlách používaných Žandárskym zborom a v spojení s tým došlo k priamej novelizácii zákona č. 8/2008 Z. z. o cestnej premávke s cieľom doplniť zákaz vodičom použiť na jazdu vozidlo s farebným vyhotovením a označením zameniteľným s vozidlom Žandárskeho zboru, teda zhodne s režimom pre iné zložky polície a záchranné zložky.²⁹ Účelu realizácie zákonom priznaných oprávnení ako aj s tým súvisiacej zvýšenej právnej ochrany žandára pri plnení zákonných úloh zodpovedá priznanie postavenia verejného činiteľa žandárovi podľa § 22 ods. 8 zákona.

Zákonná dikcia navyše na viacerých miestach rozoznáva pojmy ako úlohy Žandárskeho zboru alebo činnosť Žandárskeho zboru, avšak ako sme už uviedli, ako subjekt bezpečnostnej správy tento zbor nijako nedefinuje.

Absencia zákonnej definície Žandárskeho zboru má za následok nejasnosti právnej regulácie súvisiacich organizačných a riadiacich aspektov činnosti Žandárskeho zboru. Tým, že zákon Žandársky zbor nedefinuje ako entitu, zákonná úprava sa pri riadení a organizácii obmedzuje len na žandára samotného, nie však na zbor ako taký. Na tomto mieste sa žiada spomenúť rozdiel od historickej právnej zákonnej úpravy, kde najvyšším riadiacim orgánom bol generálny inšpektor četníctva, súčasná zákonná úprava vzhľadom na zvolený model kreovania žandárskeho zboru však nijako neupravuje takýto alebo obdobný orgán samostatného riadenia tohto zboru. Pre otázku právnej regulácie riadenia sa teda ostáva aplikácia jednak § 22 ods. 7 zákona, podľa ktorého žandár podlieha počas plnenia úloh podľa odseku 1 organizačnej, riadiacej a kontrolnej činnosti útvaru Policajného zboru a to podľa miesta svojho zaradenia. Ak sa žandár spolupodieľa na úlohách Vojenskej polície, potom podlieha jej odboru alebo oddeleniu. Tu sa však tiež ukazuje ďalší moment, ktorý vyvoláva otázku a týka sa prepojenia plnenia úloh Žandárskeho zboru a riadenia. „Spolupôsobenie“ pri plnení úloh Policajného zboru alebo Vojenskej polície si vyžaduje jasnejšie vymedzenie vzťahu oboch vykonávateľov policajnej správy a to

²⁸ § 86 písm. i) zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch.

²⁹ § 4 ods. 2 písm. o) zákona č. 8/2009 Z. z. o cestnej premávke v znení čl. XXVI bod 2. zákona č. 150/2002 Z. z.

tak na vyššej, strategickej, ako aj operačnej úrovni, napríklad pri vykonávaní služobných zákrokov.

Na účel určitej exemplifikácie, ale tiež porovnania možno spomenúť právnu úpravu organizácie, riadenia a kontroly v prípade vojakov v činnnej službe vyčlenených na plnenie úloh Policajného zboru. Na základe ustanovenia § 1 vyhlášky MV SR č. 283/1993 Z. z., ktorou sa upravujú podrobnosti výkonu služby vojakov pri plnení úloh Policajného zboru sa vojaci vyčlenení na plnenie úloh Policajného zboru podľa § 70 ods. 1 zákona č. 171/1993 Z. z. o Policajnom zbore dostávajú z hľadiska riadenia do podriadenosti Policajného zboru. Verejnoporiadkové funkcie však takto vyčlenení vojaci môžu vykonávať len v hliadke, v ktorej veliteľom je príslušník Policajného zboru a samostatne je im dovolené vykonávať službu len pri zabezpečovaní ochrany štátnych hraníc a strážení objektov.³⁰

Aj takto sa podľa právnej úpravy poriadku v doterajšej praxi sanovali nedostatočné vlastné kapacitné možnosti Policajného zboru pri plnení verejnoporiadkových činností. Zákonná úprava totiž vtedy predpokladá splnenie materiálnej podmienky v oblasti vnútornej bezpečnosti štátu, a síce že k vyčleneniu dochádza vtedy, keď sily a prostriedky Policajného zboru nepostačujú na dosiahnutie zákonom vymedzeného účelu ochrany verejného poriadku, kontroly hraníc, boja proti terorizmu a organizovanému zločinu. Odhliadnuc od faktu, že to spôsobovalo a spôsobuje ozbrojeným silám Slovenskej republiky často ťažkosti najmä s plnením svojich základných úloh, najmä naplňovaním početných stavov do výcviku a s plnením ďalších záväzkov, právna úprava aspoň výslovne a zrozumiteľne upravuje riadiace vzťahy k Policajnému zboru a to aj na taktickej úrovni výkonu verejnoporiadkových úloh.

V zákonnej úprave žandárstva však nielenže neexistuje obdobná právna úprava, ale nedošlo ani k zakotveniu splnomocňovacieho ustanovenia, ktoré by tieto organizačné a riadiace vzťahy upravili na podzákonnej úrovni všeobecne záväzným právnym predpisom. Napriek tomu a v kontraste s vyššie spomenutým modelom riadenia vojakov vyčlenených na plnenie úloh Policajného zboru, zákonná úprava žandárstva explicitne v § 22 ods. 6 tretia veta ustanovuje, že žandár môže plniť úlohy aj samostatne. Hoci podľa nasledujúceho odseku 7 cit. zákona podlieha pri plnení úloh riadiacej činnosti útvaru Policajného zboru resp. odboru alebo oddelenia Vojenskej polície, je táto úprava riadenia tak aplikačne nejasná a v porovnaní s úpravou podriadenosti vojakov vyčlenených na plnenie úloh Policajného zboru zásadne nedostatočná. Navyše odborné, organizačné a technické zabezpečenie Žandárskeho zboru patrí Vojenskej polícii. Táto zároveň vedie zoznam žandárov a to aj pre potreby Policajného zboru, ktorému ho poskytuje podľa § 23 ods. 1 na účely podľa § 22 ods. 7

³⁰ § 3 vyhlášky Ministerstva vnútra Slovenskej republiky č. 283/1993 Z. z., ktorou sa upravujú podrobnosti výkonu služby vojakov pri plnení úloh Policajného zboru.

zákona. To znamená že neverejný zoznam žandárov vedie Vojenská polícia aj vtedy, ak sa žandár spolupodieľa na plnení úloh Policajného zboru. Niet tak pochyb, že sa v oblasti riadenia Žandárskeho zboru prejavuje militarizačný prvok a prevalencia riadiacich a organizačných kompetencií Vojenskej polície je oproti Policajnému zboru prítomná na viacerých miestach právnej úpravy. Toto hodnotenie možno ďalej podporiť aj poznámkami k ďalším ustanoveniam nielen samotného zákona č. 150/2025 Z. z., ale aj k súvisiacej a blanketovou normou prepojenej zákonnej úprave. Pri absencii definičného vymedzenia Žandárskeho zboru a zároveň absencii právnej úpravy podriadenosti zboru samotného (nie žandára ako jeho príslušníka) konkrétnemu orgánu ústrednej štátnej správy je potrebné ďalej spomenúť ustanovenie § 3 ods. 1 písm. q) zákona č. 124/1992 Zb. o Vojenskej polícii v znení novelizovanom zákonom č. 150/2025 Z. z. Toto ustanovenie zakotvuje novú úlohu Vojenskej polície vo vzťahu k Žandárskemu zboru. Vojenská polícia riadi, koordinuje, metodicky usmerňuje, kontroluje, materiálne a technicky zabezpečuje činnosť Žandárskeho zboru. Toto ustanovenie osobitnej právnej úpravy nadväzuje na § 22 ods. 5 zákona č. 150/2025 Z. z., podľa ktorého úlohy spojené s odborným, organizačným a technickým zabezpečením plní Vojenská polícia. Posúdením vzájomnej výkladovej spojitosti oboch ustanovení je zrejmé, že obe právne úpravy konzistentné nie sú. Zákonná úprava novelizujúca zákon o Vojenskej polícii totiž zveruje riadenie Žandárskeho zboru Vojenskej polícii (odhliadnuc od koordinovania a metodického usmerňovania), čo sa však z pohľadu ustanovenia § 22 ods. 7 zákona č. 150/2025 Z. z. upravujúceho riadiacu, kontrolnú a organizačnú nadriadenosť Policajného zboru voči žandárovi, ktorý sa spolupodieľa na činnosti Policajného zboru javí ako rozpor dvoch právnych úprav. Treba podotknúť, že novozavedená úloha Vojenskej polície spolupracovať s Policajným zborom pri zabezpečovaní činnosti Žandárskeho zboru³¹ sa však týka plnenia úloh Žandárskeho zboru, nie jeho riadenia. Za zmienku na tomto mieste stojí aj to, že žandár je podľa § 25 ods. 1 písm. b) zákona povinný dodržiavať služobné a iné interné predpisy, upravujúce činnosť Žandárskeho zboru. Zákon tak predpokladá v budúcnosti existenciu takýchto predpisov. Je otázne, či tieto predpisy bude vydávať Vojenská polícia a to aj pre prípad, že žandár sa bude spolupodieľať na plnení úloh Policajného zboru, keďže zákon bližšiu úpravu normotvornej právomoci neobsahuje. Keďže je však interná normotvorba výrazom riadiacej činnosti orgánov verejnej moci a vychádzajúc z už spomenutého ustanovenia o riadení Žandárskeho zboru Vojenskou políciou, možno sa domnievať, že interná normotvorba Žandárskeho zboru bude patriť práve jej. Tento záver podporuje aj fakt, že obdobná riadiaca úloha ako je uložená Vojenskej polícii novelizáciou zákona č. 124/1992 Zb. sa do zákona NR SR č. 171/1993 Z. z. pre

³¹ § 3 ods. 1 písm. f) zákona č. 124/1992 Z. z. o Vojenskej polícii v znení čl. V bod 6. zákona č. 150/2025 Z. z.

Policajný zbor a poťažmo Ministerstvo vnútra Slovenskej republiky nedostala. Či a prípadne akú úlohu bude v tejto normotvorbe zohrávať samotné ministerstvo obrany Slovenskej republiky taktiež nie z právnej úpravy zrejme.

V rámci poznámok k organizačným a riadiacim aspektom existencie a činnosti Žandárskeho zboru aj verejnej rozpravy ktorá predchádzala schváleniu novej zákonnej úpravy možno badať vcelku pochopiteľnú a racionálnu snahu zákonodarcu zohľadniť finančnú „podvýživenosť“ polície a preniesť zabezpečenie fungovania Žandárskeho zboru na vojenské súčasti bezpečnostného aparátu. Mám však zato, že filozofia zákona má skôr ako z rozpočtovej reality vychádzať z charakteru štátnosprávnych funkcií, ktoré ten ktorý vykonávateľ plní.

Organizačné a subordinačné aspekty policajnej správy nie sú a nemajú byť účelovým výsledkom momentálnej naliehavej potreby sanovať kapacitné limity doterajšej sústavy zložiek polície. Model organizácie polície, rovnako ako model organizácie ozbrojených síl totiž vychádza z bezpečnostnou stratégiou štátu doktrínálne zavedeného rozlišovania vnútorných a vonkajších bezpečnostných funkcií štátu. Treba doplniť, že tento model musí súčasne reflektovať na vzájomnú interakciu vonkajších a vnútorných bezpečnostných hrozieb. Tomu by v objektívnom práve malo vhodne zodpovedať jednak rozlíšenie funkcií policajnej správy a správy obrany. Toto rozlišovanie by malo byť spojené so súbežným zavedením právneho režimu vzájomných riadiacich a organizačných väzieb tak, aby sa nenahrádzali, ale boli postavené na kooperatívnom princípe a zároveň jasnej separácii ich konkrétnych vykonávateľov.

Pre účely stručného záveru k tejto časti príspevku a s vyššie naznačenou referenciou na kompetenčné problémy spojené s riadením a organizáciou žandárstva v minulosti sa domnievam, že spôsob právnej regulácie organizácie a riadenia nového Žandárskeho zboru, žiaľ tiež vytvára aj živnú pôdu pre aplikačné problémy a opakovanie „starých“ chýb z čias historického československého četníctva. A to napriek nespochybniteľnej racionalite snahy štátu o posilnenie výkonu verejnoporiadkových funkcií v policajnej správe.

K niektorým otázkam funkčného poňatia žandárskeho zboru.

Keďže bezprostredne s organizáciou akejkoľvek zložky polície súvisí aj vymedzenie nielen vecnej, ale tiež územnej a poťažmo personálnej pôsobnosti, stojí za zmienku aj spôsob, ktorý zákonodarca zvolil pre Žandársky zbor. Personálna pôsobnosť nie je v zákone explicitne upravená, ale domnievam sa, že logickým riešením je previazať ju s pôsobnosťou buď Policajného zboru alebo Vojenskej polície, a to podľa toho, či sa bude žandár spolupodieľať na plnení úloh jednej alebo druhej z týchto zložiek polície. Keďže Policajný zbor a Vojenská polícia nemajú jej rozsah zhodný, bude sa v prípade činnosti žandára zrejme musieť riadiť podľa rozsahu ustanoveného

osobitnými zákonmi o Policajnom zbore a zákonom o Vojenskej polícii. Vecná pôsobnosť je explicitne upravená zákonnou úpravou v tom zmysle, že rešpektuje rozdelenie pre podporu plnenia úloh Policajného zboru alebo Vojenskej polície. Niektoré otázky napriek tomu vznikajú. V tomto príspevku aj vzhľadom na krátkosť času od nadobudnutia účinnosti zákona, nejde síce o podrobnejší rozbor samotného fungovania Žandárskeho zboru z hľadiska výkonu vecnej pôsobnosti, ale zákonom zavedené riešenie jeho organizácie a subordinácie má prirodzene vplyv aj na funkčné poňatie výkonu policajných bezpečnostných činností. Zákonná úprava pre vymedzenie povahy úloh, ktoré má Žandársky zbor plniť zaviedla pojem „sa spolupodieľa“ pri plnení policajných bezpečnostných činností v ustanovenom rozsahu.³² Aký je však tento rozsah? *Prima facie* je zodpovedanie tejto otázky pomerne jednoduchým výkladom odvoditeľné z § 22 ods. 1 resp. odseku 2 zákona. Citované ustanovenia uvádzajú enumeráciu úloh Žandárskeho zboru a pri bližšom skúmaní vecnej podstaty týchto úloh je zrejmé, že všetky majú verejno-poriadkovú povahu. Menej zrejmé je aký dôvod mal zákonodarca na demonštratívny spôsob vyjadrenia dikcie základného ustanovenia v § 1 ods. 2 písm. b) zákona, kde sa ustanovuje, že úlohy Žandárskeho zboru majú byť plnené „s cieľom podporovať Policajný zbor najmä pri zabezpečovaní verejného poriadku“. Žiada sa pripomenúť, že vymedzenie rozsahu vecnej pôsobnosti Žandárskeho zboru by malo rovnako ako u iných vykonávateľov štátnosprávnych funkcií rešpektovať ústavnoprávne zakotvenú požiadavku čl. 2 ods. 2 Ústavy SR, a to konkrétne pokiaľ ide o zákaz konania štátnej moci *ultra vires*. Mám zato, že použité príkladnosti pri vyjadrení rozsahu vecnej pôsobnosti Žandárskeho zboru v základných ustanoveniach je z tohto dôvodu nevhodné a výklad bude možné v aplikačnej praxi realizovať len v spojení s ustanoveniami § 22 a nasl. zákona. A navyše rozsah vecnej pôsobnosti Žandárskeho zboru pri spolupôsobení pri plnení úloh Vojenskej polície bude možné odvodiť výlučne z týchto ustanovení, keďže podpora Vojenskej polície Žandárskym zborom sa do základných ustanovení vymedzujúcich predmet zákona neuviedla vôbec.

K tejto časti možno doplniť niekoľko záverečných poznámok. Ako už bolo všeobecnejšie naznačené vyššie, verejno-bezpečnostné a verejno-poriadkové úlohy, ktoré sú vlastné a charakterizujú podstatnú časť funkcií policajnej správy budú po novom v podaní Žandárskeho zboru predstavovať určité presahy inštitucionálnych prvkov vojenskej súčasti bezpečnostnej správy do policajnej správy. Tomu jednoznačne prispieva jednak spomenutá úloha Vojenskej polície prevziať akúsi starostlivosť o Žandársky zbor a jednak vymedzenie jeho personálneho substrátu, keďže žandárom môže byť len profesionálny vojak, príslušník Policajného zboru, ak je vojakom pohotovostných záloh alebo bývalý príslušník Policajného zboru, ak je

³² § 22 ods. 1 a 2 zákona č. 150/2025 Z. z.

vojakom operačných záloh.³³ Uvedené zákonné riešenie nepochybne prispieva k naplneniu účelu zákona tak, ako sa tento koniec koncov odzrkadľuje aj v názve zákona. Nepochybne rozšírenie bezpečnostného aparátu o nový subjekt zvyšuje odolnosť Slovenskej republiky v oblasti nielen obrany, ale aj bezpečnosti, na strane druhej vytvára právny základ pre stieranie deliácií čiar medzi správou obrany a policajnou správou. Aj z hľadiska funkčného a nielen zákonodarcom zvoleného organizačného a riadiaceho modelu Žandárskeho zboru ide v oblastiach patriacich prinajmenšom do pôsobnosti služby poriadkovej polície o zmenu v ponímaní zaužívaného a už vyššie spomenutého konceptu separácie vnútornej a vonkajšej bezpečnosti. Táto zmena prináša určitú mieru militarizácie policajnej správy a možno povedať aj „spolicajnenie“ správy obrany. Pritom práve opačný koncepčný prístup bezpečnostnej politiky sa v nedávnej minulosti opieral o hlasy volajúce po oddelení subjektov policajnej správy od správy obrany, čo viedlo *inter alia* k zániku vojsk ministerstva vnútra.

V nadväznosti na predchádzajúci rozbor je tiež zaujímavé, ako sa zákonodarca vysporiadal s otázkou územnej pôsobnosti. Ustanovenie § 22 ods. 4 druhá veta zákona ustanovuje, že žandár plní úlohy najmä v prímestských oblastiach alebo vidieckych oblastiach. Bližšie vymedzenie v zákone upravené nie je a to ani formou odkazu. K tomu sa žiadajú tri poznámky. Prvou je zjavná snaha priblížiť pôsobenie Žandárskeho zboru z hľadiska územnej pôsobnosti a na rozdiel od jeho definovania ako entity ako aj systému jeho riadenia a organizácie takému modelu, ktorý fungoval v podmienkach historického československého četníctva.³⁴ Druhou je, že táto pôsobnosť sa stáva v dôsledku demonštratívneho spôsobu vyjadrenia zákonnej dikcie relativizovanou a otáznou je, či nie je preto zbytočná. Obsah použitých pojmov „prímestský“ a „vidiecky“ je navyše právne neurčitý a najmä vo svojej podstate mätúci. Otázkou totiž je, či je na uvedenú formuláciu aplikovateľný právny režim úpravy územia obce (mesta), tak ho upravuje napr. § 2 zákona č. SNR č. 369/1990 Zb. o obecnom zriadení, prípadne definičný rámec pojmov v oblasti územného plánovania podľa § 5 zákona č. 200/2022 Z. z. o územnom plánovaní, ktorý vymedzuje pojmy ako napríklad osobitné územie, región, mikroregión, zastavané územie, verejný priestor a sídelné prostredie. Čo znamená vidiecka oblasť v právnom význame, keďže v kodifikovanej podobe štátneho jazyka znamená obývaný priestor mimo mestského osídlenia a charakterizovaný nižšou hustotou osídlenia.³⁵ Podobne význam pojmu „prímestský“ znamená „v blízkosti mesta“. Nejde však o právne upravené kategórie a preto sú na účely vymedzenia územnej pôsobnosti nevhodné.

³³ § 22 ods. 3 zákona č. 150/2025 Z. z.

³⁴ MACEK, P., UHLÍŘ, L. Dejiny polície a četníctva II. Československá republika (1918-1939). Praha: POLICE HISTORY, 1999. s. 55.

³⁵ KAČALA, M., PISARČÍKOVÁ, M., POVAŽAJ, M. Krátky slovník slovenského jazyka, 3. doplnené a prepracované vyd. Bratislava: Veda, 1997. s. 798.

Záver

Oddelenie úsekov verejnej správy a ich organizácia na celoštátnej úrovni spôsobom rešpektujúcim nielen vecnú racionalitu, ale aj potrebu rezortnej dekoncentrácie moci považujem za dôležitú záruku realizácie ústavnej požiadavky po rovnováhe moci. Z perspektívy teoretického skúmania organizačného poňatia štátnej správy vyslovujem názor, že pri vytváraní právnej úpravy vymedzenia vecnej pôsobnosti jednotlivých vykonávateľov štátno- správnych funkcií je potrebné zohľadniť nielen vecný charakter týchto funkcií, ale tiež dbať na rovnováhu jednotlivých úsekov štátnej správy.

Racionálne začlenenie úloh v konkrétnej oblasti štátnej správy je síce možné vnímať ako základ pre jej správne a efektívne vykonávanie, zo statického hľadiska organizácie verejnej správy to však nestačí. Je tiež potrebná vyváženosť rozdelenia vecnej agendy, ktorá v rámci výkonnej zložky štátnej moci patrí konkrétnemu vykonávateľovi. Tak ako sa princíp decentralizácie moci v ústavnoprávnom a štátovednom zmysle premietol do trichotonómie moci vo všeobecnosti, tak v rámci výkonnej zložky štátnej moci, ktorá sa realizuje plnením štátno-správnych úloh stojí za úvahu oddeľovať tieto úlohy aj v záujme zabrániť prílišnej koncentrácii mocenských funkcií. Tento názor vyslovujem najmä s prihliadnutím na už zmienenú skutočnosť, že ozbrojený mocenský aparát štátu patrí k najsilnejšej inštrumentálnej výbave štátnej moci.

Vyššie bola položená otázka k spoločenskej objednávke po novej zložke polície v podobe žandárskeho zboru, pričom analýzou novej právnej úpravy aj so zohľadnením reality vnútrobezpečnostného prostredia Slovenskej republiky, keď sú kapacity Policajného ako najvýznamnejšej zložky polície obmedzené je vytvorenie Žandárskeho zboru podľa môjho názoru prínosom. Položená podotázka, ktorá je nosnou témou príspevku a týka sa podoby Žandárskeho zboru, podmieneného spôsobom, akým zákonodarca upravil najmä riadenie Žandárskeho zboru a vytvoril „entitu bez entity“ nepovažujem za správnu. Usudzujem tak z viacerých dôvodov. Vymedzenie organizačných a riadiacich mechanizmov novovzniknutého žandárskeho zboru nerešpektuje dôsledne historickú podobu organizácie žandárstva v minulosti, čo by samo osebe nebolo problémom, keby sa zákonodarca vyhol príčinám problémov, ktoré historický model československého četníctva sprevádzali. Po druhé nemožno nevnímať značnú militarizáciu tejto novej zložky polície najmä napojením na Vojenskú políciu v oblasti riadenia, koordinácie, výcviku a materiálneho zabezpečenia. Pritom plne rozumiem snahe využiť priaznivejšie rozpočtové pokrytie z kapitoly obranného rezortu v porovnaní s rezortom vnútra. Venovať hlbšiu pozornosť funkčnému poňatiu žandárstva u nás bude prirodzene možné až na základe vyhodnotenia výkonu funkcií, ktoré nová zákonná úprava Žandárskemu zboru zverila. Teda až na základe aplikačnej skúsenosti v budúcnosti

bude samozrejme možné objektívne vyhodnotiť, či Žandársky zbor skutočne prispel k účinnejšej odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, ako to deklarovali predkladatelia zákona. Napriek predčasnosti zaoberať v tomto období samotnou funkčnou stránkou, schválená zákonná úprava vykazuje niektoré prinajmenšom formulačné nezrovnalosti pri vymedzení pôsobnosti Žandárskeho zboru, ktoré si zaslúžia pozornosť nielen z pohľadu správne vedy, ale aj z hľadiska budúcej legislatívnej reparácie.

Napriek v článku naznačenej kritike novej zákonnej úpravy vyjadrujem presvedčenie, že si Žandársky zbor nájde v súčasnom bezpečnostnom aparáte Slovenskej republiky miesto, ktoré si získa dôveru občanov efektívnym a zákonným prispievaním k výkonu funkcií policajnej správy. Netreba totiž zabúdať, že efektivita verejnoporiadkového a verejnobebezpečnostného pôsobenia štátu v živote spoločnosti je zvlášť závislá od dôvery, ktorú občania prechovávajú k bezpečnostným orgánom a preto je žiadúce podrobiť novovzniknutý Žandársky zbor zodpovednej analýze nielen zo strany riadiacich orgánov štátnej správy, ale tiež v právno-teoretickom zmysle.

Zoznam použitej literatúry

Knižné publikácie

1. BOHATA, I. Protilidová úloha četnictva v letech 1918-1938. 1. vydanie: Praha, Východočeské tiskárny, 1978. 96 s.
2. JANÁK, J., HLEDÍKOVÁ, Z., Dobeš J. Dějiny správy v českých zemích od počátku štátu po současnost. Praha: Nakladatelství Lidové noviny, 2005. 568s. ISBN 80-7106-709-1.
3. KAČALA, M., PISARČÍKOVÁ, M., POVAŽAJ, M. Krátky slovník slovenského jazyka 3. doplnené a prepracované vyd. Bratislava: Veda 1997. 943 s. ISBN 80-224-0464-0.
4. MACEK, P., UHLÍŘ, L. Dejiny policie a četnictva II. Československá republika (1918-1939). Praha: POLICE HISTORY, 1999. 230 s. ISBN 80-902670-0-9.
5. VRABKO, M. a kol. Správne právo hmotné. Osobitná časť. 3. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2017. 512 s. ISBN 9788081687471.

Právne predpisy

1. Zákon č. 150/2025 Z. z. o niektorých opatreniach na zvýšenie odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene doplnení niektorých zákonov.
2. Zákon č. 124/1992 Zb. o Vojenskej polícii.
3. Zákon č. 299/1920 Sb. o četníctvu.

4. Zákon Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch.
5. Zákon č. 8/2008 Z. z. o cestnej premávke.
6. Zákona č. 40/1974 Zb. o Zbore národnej bezpečnosti.
7. Vyhláška Ministerstva vnútra Slovenskej republiky č. 283/1993 Z. z., ktorou sa upravujú podrobnosti výkonu služby vojakov pri plnení úloh Policajného zboru.

Internetové zdroje

1. Pozmeňujúci a doplňujúci návrh poslanca Národnej rady Slovenskej republiky Tomáša Valáška k vládnemu návrhu zákona o niektorých opatreniach na zvýšenie odolnosti Slovenskej republiky v oblasti obrany a bezpečnosti, o brannej povinnosti a o zmene doplnení niektorých zákonov (tlač 716) [online]. [cit. 2025-09-11]. Dostupné z: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=566075>
2. Spoločná správa (716a) [online]. [cit. 2025-09-11]. Dostupné z: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=566006>
3. VEREJNÝ OCHRANCA PRÁV: V ZÁKONE O ŽANDÁRSTVE NAVRHUJEM VYŠŠIE GARANCIE ĽUDSKÝCH PRÁV [online]. Bratislava, 28.01. 2025, [cit. 2025-9-11]. Dostupné z: <https://vop.gov.sk/wp-content/uploads/2025/01/Tlacova-sprava-VOP-28.-01.-2025.pdf>
4. Rezort vnútra predĺžil novým policajtom povinnú službu v Bratislave. Chce tak riešiť ich nedostatok, odborári to kritizujú [online]. 18.03. 2025, [cit. 2025-9-11]. Dostupné z: <https://spravy.stvr.sk/2025/03/novi-policajti-budu-moct-sluzit-dva-roky-v-bratislave-stat-tak-chce-riesit-ich-nedostatok-odborari-zmenu-kritizuju/>
5. Zemandlová, L. Polícia a četníctvo na našom území v rokoch 1848- 1918 (historicko-právne aspekty). [online]. [cit. 2025-09-11]. Dostupné z: <https://www.akademiapz.sk/sites/default/files/OVVP/009%20%20ZEMANDLOVA%20%20Bezpecnostne%20zlozky%20na%20nasom%20ouzemi%20v%20rokoch%201848.pdf>

Kontaktné údaje

JUDr. Tomáš Rulíšek, PhD., MBA
tomas.rulisek@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra správneho práva a environmentálneho práva

**Sekcia práva informačných technológií a práva
duševného vlastníctva**

Regulácia, kybernetická bezpečnosť a digitalizácia
práva

THE RISKS FOR CHILDREN IN THE ONLINE ENVIRONMENT AND THE ROLE OF EUROPEAN LEGISLATION IN THEIR PROTECTION

Lucia Rybanová¹

Abstract: Social media and the online environment have become an integral part of children's lives, offering many opportunities for learning and discovering new information. However, this also comes with various risks that affect their mental well-being and privacy. Some of the most common problems include cyberbullying, access to harmful and inappropriate content, misuse of personal data (also by their parents), and exposure of children to targeted marketing and profiling. The aim of this article is to identify the risks associated with children's use of social media platforms and to analyse how the European Union's digital legislation responds to these risks. The article will focus on the General Data Protection Regulation (GDPR), which introduces specific rules for the processing of children's data, as well as the Digital Services Act (DSA), which seeks to contribute to the creation of a safe and transparent online environment that protects individuals (including children) from harmful content or profiling. The author will also address the Audiovisual Media Services Directive (AVMSD), which applies to all services with audiovisual content and protects children from inappropriate advertising or harmful content. The author's goal is to assess the extent to which these legal acts reflect the identified problems and to highlight the remaining gaps and challenges for the future.

Keywords: protection of minors, social media, GDPR, Digital Services Act

Introduction

The online environment has become an integral part of our daily lives, taking into account the digital era in which we live today. Children are not excluded from internet access, as they spend time in the online space daily. This has been shown by data analyses collected over the past years from 78 countries that participated in the Organisation for Economic Co-operation and Development (OECD) Programme for International Student Assessment (PISA). These data show that in the past 20 years, the ability of 15-year-olds to connect to the internet at home has increased rapidly,

¹ Comenius University Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property Law.

revealing that only 3 % of surveyed children did not have internet access at home in 2022.²

Based on the survey, the majority of children in these countries have convenient home internet access, which facilitates their use of social media platforms. On the one hand, this creates a great opportunity for them to develop their digital skills and learn how to live in the online world, which has become an almost inevitable part of our lives. On the other hand, it is crucial to take into account the risks that may arise from their access to social media platforms, and to search for ways to mitigate them. The aim of this article is to point out the greatest risks for children on social media platforms, and to analyse how the digital legislation of the European Union responds to these risks, with special regard to the General Data Protection Regulation³ (GDPR), the Digital Services Act⁴ (DSA), and the Audiovisual Media Services Directive⁵ (AVMSD). First, we analyse selected summary reports to identify the biggest risks in the world of social media platforms for children. We then identify three relevant legal acts regulating social media and, through deduction, attempt to highlight gaps in the legal framework and how they could be filled. The conclusions will be summarised in the last paragraph.

Risks for children on social media platforms

Firstly, it is necessary to point out that we will focus on the biggest risks that children may face, particularly on social media platforms, and for this part we used data from two papers. One of them is *Children in the digital environment: revised typology of risks*,⁶ which is a paper from 2021, issued by the Organisation for Economic Co-operation and Development, providing an overview of risks for children in the online

² UNICEF Innocenti: Global Office of Research and Foresight, *Childhood in a Digital World: Screen time, skills and mental health*. UNICEF Innocenti, Florence, (2025), p. 5-7. Available at: <https://www.unicef.org/innocenti/reports/childhood-digital-world>. [accessed: September 2025].

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

⁵ Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).

⁶ OECD: *Children in the Digital Environment: Revised Typology of Risks*. OECD Digital Economy Papers, no. 302, (2021). Available at: <https://doi.org/10.1787/9b8f222e-en>. [accessed: September 2025].

environment. The second paper is *Childhood in a digital world*,⁷ issued by UNICEF in 2025, which focuses on connectivity, digital skills, and the mental health of children. The papers were selected for their recent publication dates and authoritative focus on risks faced by children in the digital environment. Both sources provide a comprehensive analysis of online threats, including risks arising from the use of social media platforms. Their recency ensures that the findings reflect the current situation, while their scope makes them highly relevant for examining social media platforms. Based on these papers, we concentrated on risks specifically associated with social media platforms and prioritized those that were most frequently emphasized across both sources. This approach aims to ensure that the selected risks represent the most pressing and widely recognized threats to children's safety and well-being online. We identified the following major risks for children on social media platforms: cyberbullying; online sexual abuse; access to harmful and inappropriate content; misuse of personal data; sharenting; and exposition to targeted marketing and profiling. Before we focus on European Union's digital legislation and its reaction to these issues, we will briefly describe each of these risks and their potentially negative consequences on children.

Cyberbullying does not have a widely accepted definition. For the purpose of this article, we will use the following definition suggested by Smith et al: "*an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself*".⁸ A 2024 paper on cyberbullying indicates that the mental well-being of victims of cyberbullying, as well as the mental well-being of bullies, is severely affected. Consequently, this has led to several problems, such as suicidal thoughts and depression.⁹

Online sexual abuse of children has also become an important part of the discussion about the risks to children. It has been shown that minors who are victims of online sexual abuse (and cyberbullying) are significantly more likely to self-harm, suffered higher levels of anxiety, and show increased suicidal thoughts or behaviours.¹⁰

⁷ UNICEF Innocenti: Global Office of Research and Foresight, *Childhood in a Digital World: Screen time, skills and mental health*. UNICEF Innocenti, Florence, (2025). Available at: <https://www.unicef.org/innocenti/reports/childhood-digital-world>. [accessed: September 2025].

⁸ SMITH, Peter K., et al.: Cyberbullying: Its nature and impact in secondary school pupils. In: *Journal of child psychology and psychiatry*, vol. 49, issue 4 (2008), p. 376. Available at: <https://doi.org/10.1111/j.1469-7610.2007.01846.x>.

⁹ BANSAL, Suhans, et al.: Cyberbullying and mental health: past, present and future. In: *Frontiers in Psychology*, vol. 14 (2024), p. 14. Available at: <https://doi.org/10.3389/fpsyg.2023.1279234>.

¹⁰ UNICEF Innocenti: Global Office of Research and Foresight, *Childhood in a Digital World: Screen time, skills and mental health*. UNICEF Innocenti, Florence, (2025), p. 5-7. Available at: <https://www.unicef.org/innocenti/reports/childhood-digital-world>. [accessed: September 2025].

Another risk arising from the use of social media platforms by children is access to harmful and inappropriate content. This content may appear in various forms, including videos, pictures, words, or symbols. A study conducted by the European Union revealed that the most frequently reported harmful content by children includes hate messages, as well as violent images. Such illegal content is likely to expose minors to concepts that they are not capable of processing.¹¹

Children's personal data may also be at risk on social media platforms, primarily due to the misuse of personal data or sharenting. Minors do not always possess sufficient comprehension or literacy skills to understand not only the concept of processing their personal data but also its use for commercial purposes,¹² which is also connected to the risk of targeted marketing and advertising aimed at children, exposing them to consumer risks, such as inappropriate advertisements, commercial messages aimed at adults, or advertisements that exploit their credulity and inexperience.¹³

Lastly, the risks concerning their personal data are also related to sharenting. This refers to situations where parents share their children's personal data online, which is a very popular practice. However, this can result in the infringement of the child's privacy and undermine the protective role of the parent.¹⁴

Protection of children by European legislation and potential gaps in this protection

As we have introduced the greatest risks for children on social media platforms, we will now examine how European legislation responds to them, with a special focus on the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and the Audiovisual Media Services Directive (AVMSD).

The Digital Services Act is a regulation that lays down obligations for various online services used by individuals in the European Union, regardless of where the service is based.¹⁵ The biggest stakeholders within the social media platforms, such as Facebook, Instagram, Snapchat, or TikTok, which are largely used by children, were

¹¹ OECD: Children in the Digital Environment: Revised Typology of Risks. OECD Digital Economy Papers, no. 302, (2021), p. 8. Available at: <https://doi.org/10.1787/9b8f222e-en>. [accessed: September 2025].

¹² LIVINGSTONE, Sonia – STOILOVA, Mariya – NANDAGIRI, Rishita: Children's data and privacy online: growing up in a digital age: an evidence review. London: London School of Economics and Political Science (2019), p. 34. Available at: <http://eprints.lse.ac.uk/id/eprint/101283>.

¹³ OECD: Children in the Digital Environment: Revised Typology of Risks. OECD Digital Economy Papers, no. 302, (2021), p. 11. Available at: <https://doi.org/10.1787/9b8f222e-en>. [accessed: September 2025].

¹⁴ *Ibidem*, p. 14.

¹⁵ Article 2, par. 1 of the DSA.

designated under the DSA as very large online platforms (VLOP).¹⁶ Since VLOPs are the largest types of platforms regulated under the DSA, the abovementioned social media platforms must comply with the strictest rules. The question is whether these rules and obligations adequately mitigate the risks that children face on social media platforms.

The protection of children is already addressed in several recitals of the DSA. They emphasise, for example, the importance of considering the capacity of children to understand the design and functioning of the service,¹⁷ the obligation to take mitigation measures to protect minors from harmful or inappropriate content,¹⁸ or the prohibition of dark patterns.¹⁹ The measures to protect children can be found mainly in Articles 14, 16, 22, 28, 34, and 35 of the DSA.

Firstly, Article 14 of the DSA states in par. 3 that if the service is primarily directed at children, or predominantly used by them, the service provider has an obligation to ensure that conditions or restrictions on the use of their service are clearly understood by minors.²⁰ This rule aims to ensure that minors understand the terms and conditions they are agreeing to, with special regard to terms and conditions pertaining to the processing of personal data or service limitations.²¹ This provision's requirement that the service must be aimed at or predominantly used by children may be viewed as problematic, since it means that the platform needs to be aware that its particular users are minors. This fact is not problematic *per se* but may be related to the lack of age verification measures, which will be discussed further in this article.

Article 16 deals with notice and action mechanisms. The system for submitting complaints shall be designed to be easy and accessible, making it easier to report and remove illegal content.²² This mechanism, together with the help of trusted flaggers,²³ is an important tool for protecting children from harmful or inappropriate content that can be shared on social media platforms. However, a paper evaluating these reporting mechanisms reveals that they are not always designed in a user-friendly way, due to legal complexity related to the mechanism of filing a report

¹⁶ Online platforms are designated as VLOPs by a decision of European Commission, according to article 33 par. 4 of the DSA. The overview of the designated VLOPs is available here: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>. [accessed: September 2025].

¹⁷ Recital 81 of the DSA.

¹⁸ Recital 89 of the DSA.

¹⁹ Recital 67 of the DSA.

²⁰ Article 14, par. 3 of the DSA.

²¹ NOVOVIĆ, Miloš: The EU Digital Services Act (DSA): A Commentary. Netherlands: Kluwer Law International B. V., 2024, p. 121. ISBN: 978-94-035-1077-4.

²² Article 16 par. 1 of the DSA.

²³ Article 22 of the DSA.

under the DSA.²⁴ The negative effect of the above-mentioned issue manifests itself in two ways, both of which lead to the same result. The first is that it can result in a declining number of users who decide to report illegal content on social media platforms, meaning the content is not reported and remains available to everyone, including children. The second is that if the system is difficult to use, a child cannot report illegal content, so it remains visible to them.

Under Article 28 of the DSA, social media platforms that are accessible to minors are required to have “*appropriate and proportionate measures*” in place to protect children with respect to their privacy, safety, and security.²⁵ Paragraph 3 of this article sets out that the European Commission may issue guidelines for the purposes of the first paragraph. The guidelines²⁶ were issued in July 2025 and contain particular measures²⁷ to protect minors. These guidelines serve as a benchmark for the Commission to assess whether the Member States comply with Article 28, par. 1 of the DSA. However, following these guidelines is not mandatory for social media platforms, and does not automatically ensure compliance with the obligations under the DSA.²⁸

Some examples of the circumstances under which a platform can be considered accessible to minors are stated in Recital 71 of the DSA. One of the examples portrays a situation where *„the online platform already processes personal data of the recipients of its service revealing their age for other purposes.”* This can constitute a problem in relation to the strict rules of GDPR on the re-purposing of personal data.²⁹

²⁴ SEKWENZ, Marie-Therese – WAGNER, Ben – PARKIN, Simon: “It is unfair, and it would be unwise to expect the user to know the law!” – Evaluating reporting mechanisms under the Digital Services Act. In: *ACMF AccT 2025 - Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, (2025), p. 541. Available at: <https://resolver.tudelft.nl/uuid:e992f10b-51ee-4f48-b62d-1b31a6850a46>.

²⁵ Article 28 par. 1 of the DSA.

²⁶ The guidelines were issued as an annex to the Communication to the Commission No. C(2025) 4764 final, Approval of the content on a draft Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online. The guidelines are available at: <https://ec.europa.eu/newsroom/dae/redirection/document/118226>. [accessed: September 2025].

²⁷ The guidelines contain measures aimed to protect minors, such as recommendation to use effective age verification measures, prohibition from downloading or taking screenshots of content posted by minors or setting children’s account as private by default.

²⁸ As stated in the press release, informing about the issuance of the guidelines. Available at: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>. [accessed: September 2025].

²⁹ NOVOVIĆ, Miloš: *The EU Digital Services Act (DSA): A Commentary*. Netherlands: Kluwer Law International B. V., 2024, p. 132. ISBN: 978-94-035-1077-4.

Furthermore, under Article 28, par. 2 of the DSA, social media platforms are prohibited from displaying advertisements on the basis of profiling³⁰ while using personal data of a user who is a minor. This applies only in cases where the social media platform is “*aware with reasonable certainty*” that the user is a child. This measure aims to protect children from targeted marketing and profiling. Nevertheless, the DSA does not specify any measures to verify whether the user is a minor. This rule also probably excludes cases of targeted marketing in situations where a social media platform learns about the minor’s interests in other ways, rather than by profiling them.³¹

Finally, Articles 34 and 35 of the DSA set out obligations for risk assessment and the subsequent implementation of appropriate mitigation measures. The risk assessment, according to Article 34 of the DSA, shall be conducted at least once a year, and it should also assess the dissemination of illegal content, as well as “*any actual or foreseeable negative effects in relation to minors*”.³² This means that the social media platforms are specifically obliged to assess whether there are any systematic risks in the design and functioning of their service, that could have negative effects on children.³³

Article 35 of the DSA must be read in conjunction with Article 34 of the DSA, since social media platforms should put in place “*reasonable, proportionate and effective mitigation measures tailored to identified risks*”³⁴ on the basis of the risk assessment conducted in accordance with Article 34 of the DSA.³⁵ A non-exhaustive list of the measures to prevent risks is in Article 35 of the DSA.³⁶ They also include measures to protect minors, such as processes for content moderation (aimed mainly at hate speech or cyber violence), targeted measures to protect children’s rights (like parental control or age verification measures), and other similar measures. However, the DSA does not specify what can be considered as illegal content, so its definition falls within the full competence of the Member States. Since the definitions provided

³⁰ Profiling is defined in article 4 par. 4 of the GDPR as “*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*”

³¹ WOLTERS, Pieter – ZUIDERVEEN BORGESIOUS, Frederik: The EU Digital Services Act: what does it mean for online advertising and adtech? In: *International Journal of Law and Information Technology*, vol. 33, (2025), p. 24. Available at: <https://doi.org/10.1093/ijlit/eaaf004>.

³² Article 34, par. 1, letter d) of the DSA.

³³ Article 34 par. 1 of the DSA.

³⁴ Article 35, par. 1 of the DSA.

³⁵ WILMAN, Folkert – KALÉDA, Sualius Lukas – LOEWENTHAL, Paul-John: The EU Digital Services Act: a commentary. Oxford: Oxford University Press, 2024, p. 257. ISBN: 978-0-19-889284-7.

³⁶ *Ibidem*, p. 269.

by the Member States are not harmonised, this can lead to potential problems with the enforcement of this obligation.³⁷

In the following part of the article, we will focus on the General Data Protection Regulation. This regulation already stipulates in Recital 38 that children's personal data shall be specifically protected, since they are not always fully aware of the "*risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*".³⁸ This special protection is reflected mainly in Articles 8 and 12 of the GDPR, but Article 17 can also play a special role in the protection of minors and their personal data.

Article 8 of the GDPR establishes an obligation for information society services³⁹ to obtain explicit consent from children when processing their personal data. If a minor is below the age limit, parents should give their consent for processing their personal data. The child needs to be at least 16 years old, but Member States have the possibility to set the age limit lower, however, it cannot be less than 13 years old. This could constitute an issue with cross-border cases of this type, because the social media platform will not be able to refer only to the age limit in the Member State where it is established.⁴⁰

It is important to point out that this article applies only to cases where the information society service is offered directly to the child, and where the legal basis for processing their personal data is the consent of the data subject.⁴¹ This constitutes a limitation on the impact of this provision, especially (but not limited to) social media platforms. If a child registers on a social media platform, they are concluding a contract with the social media platform. Consequently, the obligation in Article 8, par. 1 of the GDPR does not apply in these cases, since the minor's

³⁷ HUSOVEC, Martin – ROCHE LAGUNA, Irene: Digital services act: a short primer. SSRN, 2022. Available at SSRN: <https://dx.doi.org/10.2139/ssrn.4153796>.

³⁸ Recital 38 of the GDPR.

³⁹ Information society service is defined in article 1, par. 1, letter b) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

⁴⁰ PERSANO, Federica: GDPR and children rights in EU data protection law. In: *Eur. J. Privacy L. & Tech.*, vol. 32, special issue, (2020), p. 41, ISSN 2704-8012. Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/ejplt2020&div=8&id=&page=>.

⁴¹ According to article 6 par. 1 letter a) of the GDPR.

personal data is being processed based on the fulfilment of a contractual relationship,⁴² and not on the basis of consent.⁴³

Article 8, par. 2 of the GDPR states that the data controller is obliged to make “reasonable effort” to verify whether the parental consent has been given or authorised, considering available technology.⁴⁴ However, the regulation does not set out specific measures for parental consent verification, neither the age verification, which constitutes its weak point.⁴⁵

Moving on to Article 12 of GDPR, this provision states that communication with minors about their personal data processing must be in clear and plain language. This provision aims to remove at some level the power imbalances between the data controller and a particular audience, like minors.⁴⁶

Lastly, the right to be forgotten, contained in Article 17 of the GDPR, is cited by some authors as a measure for the removal of sharenting content.⁴⁷ The right to erasure gives data subjects the possibility to have their data erased, for reasons⁴⁸ specified in Article 17. Even though it is stated as one of the ways to erase sharenting content, the real possibility for a child to exercise this right under Article 17 must be questioned. Several issues could stand in the way, such as the possibility for the minor to register on the social media platform (which they cannot do when they are younger than 13 years old), the child’s knowledge of their possibilities to exercise this right, and the lack of financial resources to afford the assistance of a legal professional, if the parents are not willing to erase the sharenting content.⁴⁹

⁴² As defined in article 6, par. 1, letter b) of the GDPR.

⁴³ DLOUHÝ, Vojtěch: Článek 8, Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti. In: Obecné nařízení o ochraně osobních údajů, 1. Vydání, Praha: C. H. Beck, 2021, s. 368. ISBN: 978-80-7400-815-3.

⁴⁴ Article 8, par. 2 of the GDPR.

⁴⁵ PERSANO, Federica: GDPR and children rights in EU data protection law. In: *Eur. J. Privacy L. & Tech.*, vol. 32, special issue, (2020), p. 37-38, ISSN 2704-8012. Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/ejplt2020&div=8&id=&page=>.

⁴⁶ GREEN, Daniel: Strategic Indeterminacy and Online Privacy Policies: (Un) informed Consent and the General Data Protection Regulation. In: *International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique*, vol. 38, issue 2, (2025): 701-729., p. 707. Available at: <https://doi.org/10.1007/s11196-024-10132-4>.

⁴⁷ LENDVAI, Gergely Ferenc: Sharenting as a regulatory paradox—a comprehensive overview of the conceptualization and regulation of sharenting. In: *International Journal of Law, Policy and the Family*, vol 38, issue 1, (2024), p. 12. Available at: <https://doi.org/10.1093/lawfam/ebae013>.

⁴⁸ Article 17, par. 1 of the GDPR specifies situations in which the data subject has a right to erasure, such as when the personal data are no longer necessary for the purposes for which they were collected.

⁴⁹ LENDVAI, Gergely Ferenc: Sharenting as a regulatory paradox—a comprehensive overview of the conceptualization and regulation of sharenting. In: *International Journal of Law, Policy and the Family*, vol 38, issue 1, (2024), p. 13-14. Available at: <https://doi.org/10.1093/lawfam/ebae013>.

Finally, the Audiovisual Media Services Directive constitutes another important pillar in relation to the protection of children on social media platforms. The AVMSD is applicable to all services providing audiovisual content (such as YouTube or TikTok).⁵⁰ It sets out several measures aimed at protecting children from harmful advertising and inappropriate content, such as the prohibition of targeted advertising for alcohol beverages to minors,⁵¹ age verification measures,⁵² parental controls,⁵³ or the prohibition of using their personal data for commercial purposes, including profiling or targeted advertising.⁵⁴

However, the effectiveness of the protection under the AVMSD depends heavily on its transposition to national legislation, but also on the enforcement of the specific obligations.⁵⁵

Conclusions

To conclude, it is safe to say that the European Union has moved forward in protecting children on social media platforms, mostly by adopting the Digital Services Act and the AVMSD. The GDPR also contains some provisions that are specific to the protection of children's personal data on social media platforms. Returning to the first part of this article, which assessed the risks for children on social media platforms, these legal acts address primarily the risks of harmful and inappropriate content, the processing personal data, as well as targeted marketing and profiling of minors. Cyberbullying and online sexual abuse remain unregulated by the European Union's digital legislation, so it is left to Member States to regulate these issues individually.

In May 2022, the European Commission proposed a regulation laying down rules to prevent and combat child sexual abuse.⁵⁶ Ongoing debates about this proposal criticise the potential impact on fundamental rights, as well as the proportionality of the proposed measures in relation to end-to-end encrypted communication or online anonymity.⁵⁷

⁵⁰ Article 1, par. 1, letters a) and aa) of the AVMSD.

⁵¹ Article 9, par. 1, letter e) of the AVMSD.

⁵² Article 6a, par. 1 and article 28b, par. 3, letter f) of the AVMSD.

⁵³ Article 28b, par. 3, letter h) of the AVMSD.

⁵⁴ Article 6a, par. 2 and article 28b, par. 3 of the AVMSD.

⁵⁵ VERDOODT, Valerie – LIEVENS, Eva – CHATZINIKOLAOU, Argyro: The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?. In: *Media and Communication*, vol. 11, issue 4, (2023), p. 155. ISSN: 2183–2439. Available at: <https://doi.org/10.17645/mac.v11i4.7059>.

⁵⁶ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, COM/2022/209 final.

⁵⁷ DUSHI, Desara: Does the end justify the means? The European Commission's proposed regulation laying down rules to prevent and combat child sexual abuse. In: *International Journal of Law and Information Technology*, vol. 31, (2024), p. 19. Available at: <https://doi.org/10.1093/ijlit/eaao27>.

Another issue, mentioned earlier in this article, is the issue of (in)effective age verification. In 2025, a study⁵⁸ was conducted by the Technological University Dublin, evaluating age verification methods on popular social media platforms. Its results showed that the methods currently used by social media platforms to verify the age of their users allow minors to bypass restrictions by entering misleading information about their age.⁵⁹ This may result in the inefficiency of the provisions mentioned earlier, which are conditioned by the awareness of the social media platforms about the age of their users.

It is also worth noting that the problem of sharenting is not explicitly addressed in any of the above-mentioned legal acts. Even though some authors state that the right to erasure in the GDPR can be used as a tool to remove this kind of content, it remains an insufficient measure, taking into account its practical application by the minors. Other issues have been addressed in the article, such as the limited scope of some provisions or the challenges related to the enforcement of the obligations, especially considering obligations laid down by the directives. Some provisions may also become hard to enforce when legislative responses differ across various Member States. The definition of illegal content can serve as an example that can lead to difficulties in the enforcement of the obligations set out by the Digital Services Act. The DSA can also face enforcement challenges due to its enforcement regime which combines public and private enforcement.⁶⁰

Even though the European Union is moving forward with the regulation of the social media platforms, keeping in mind that minors require specific protection, there are still several areas and risks that remain unresolved or insufficiently addressed by the legislation.

List of references

1. BANSAL, Suhans, et al.: Cyberbullying and mental health: past, present and future. In: *Frontiers in Psychology*, vol. 14 (2024), p. 14. Available at: <https://doi.org/10.3389/fpsyg.2023.1279234>.
2. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).

⁵⁸ ELTAHER, Fatmaelzahraa, et al.: The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media, Conference papers, 442, Technological University Dublin (2025). Available at: <https://doi.org/10.21427/rj5h-9450>.

⁵⁹ *Ibidem*, p. 10.

⁶⁰ HUSOVEC, Martin: Principles of the Digital Services Act. Oxford: Oxford University Press, 2024, p. 417. ISBN: 978-0-19-288245-5.

3. DUSHI, Desara: Does the end justify the means? The European Commission's proposed regulation laying down rules to prevent and combat child sexual abuse. In: *International Journal of Law and Information Technology*, vol. 31, (2024). Available at: <https://doi.org/10.1093/ijlit/eaee027>.
4. ELTAHER, Fatmaelzahraa, et al.: The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media, Conference papers, 442, Technological University Dublin, (2025). Available at: <https://doi.org/10.21427/rj5h-9450>.
5. GREEN, Daniel: Strategic Indeterminacy and Online Privacy Policies:(Un) informed Consent and the General Data Protection Regulation. In: *International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique*, vol. 38, issue 2, (2025), p. 701-729. Available at: <https://doi.org/10.1007/s11196-024-10132-4>.
6. HUSOVEC, Martin – ROCHE LAGUNA, Irene: Digital services act: a short primer. SSRN, 2022. Available at SSRN: <https://dx.doi.org/10.2139/ssrn.4153796>.
7. HUSOVEC, Martin: Principles of the Digital Services Act. Oxford: Oxford University Press, 2024. ISBN: 978-0-19-288245-5.
8. LENDVAI, Gergely Ferenc: Sharenting as a regulatory paradox—a comprehensive overview of the conceptualization and regulation of sharenting. In: *International Journal of Law, Policy and the Family*, vol 38, issue 1, (2024), p. 13-14. Available at: <https://doi.org/10.1093/lawfam/ebae013>.
9. LIVINGSTONE, Sonia – STOILOVA, Mariya – NANDAGIRI, Rishita: Children's data and privacy online: growing up in a digital age: an evidence review, London: London School of Economics and Political Science(2019). Available at: <http://eprints.lse.ac.uk/id/eprint/101283>.
10. NOVOVIĆ, Miloš: The EU Digital Services Act (DSA): A Commentary. Netherlands: Kluwer Law International B. V., 2024, p. 121. ISBN: 978-94-035-1077-4.
11. OECD: Children in the Digital Environment: Revised Typology of Risks. OECD Digital Economy Papers, no. 302, (2021). Available at: <https://doi.org/10.1787/9b8f222e-en>.
12. PERSANO, Federica: GDPR and children rights in EU data protection law. In: *Eur. J. Privacy L. & Tech.*, vol. 32, special issue, (2020), p. 32 – 42. ISSN 2704-8012. Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/ejplt2020&div=8&id=&page=>.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

14. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
15. SEKWENZ, Marie-Therese – WAGNER, Ben – PARKIN, Simon: "It is unfair, and it would be unwise to expect the user to know the law!" –Evaluating reporting mechanisms under the Digital Services Act. In: *ACMF AccT 2025 - Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, (2025), p. 532 – 546. Available at: <https://resolver.tudelft.nl/uuid:e992f10b-51ee-4f48-b62d-1b31a6850a46>.
16. SMITH, Peter K., et al.: Cyberbullying: Its nature and impact in secondary school pupils. In: *Journal of child psychology and psychiatry*, vol. 49, issue 4 (2008).376-385., p. 376. Available at: <https://doi.org/10.1111/j.1469-7610.2007.01846.x>.
17. UNICEF Innocenti: Global Office of Research and Foresight, Childhood in a Digital World: Screen time, skills and mental health. UNICEF Innocenti, Florence, (2025). Available at: <https://www.unicef.org/innocenti/reports/childhood-digital-world>.
18. UŘIČAŘ, Miroslav – RÁMIŠ, Vladan a kol.: Obecné nařízení o ochraně osobních údajů. 1. vydání. Praha: C. H. Beck, 2021. 1414 s. ISBN 978-80-7400-815-3.
19. VERDOODT, Valerie – LIEVENS, Eva – CHATZINIKOLAOU, Argyro: The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?. In: *Media and Communication*, vol. 11, issue 4, (2023), p. 151-163. ISSN: 2183–2439. Available at: <https://doi.org/10.17645/mac.v11i4.7059>.
20. WILMAN, Folkert –KALÉDA, Sualius Lukas – LOEWENTHAL, Paul-John: The EU Digital Services Act: a commentary. Oxford: Oxford University Press, 2024. 567 p. ISBN: 978-0-19-889284-7.
21. WOLTERS, Pieter – ZUIDERVEEN BORGESIUŠ, Frederik: The EU Digital Services Act: what does it mean for online advertising and adtech? In: *International Journal of Law and Information Technology*, vol. 33, (2025). Available at: <https://doi.org/10.1093/ijlit/eaaf004>.

Contact details

Mgr. Lucia Rybanová

rybanova3@uniba.sk

Comenius University Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property Law.

THE DAY POLITICAL ADS DIED: META'S BAN, EU REGULATION AND THE LESSONS FROM ROMANIA¹

Soňa Juhásová²

Abstract: Meta's decision to suspend political advertising in the EU from October 2025 reflects the company's concerns over the complexity and legal uncertainty of complying with the EU Regulation on the Transparency and Targeting of Political Advertising (TTPA). This article briefly outlines the key provisions of the TTPA and offers a critical perspective on its design. It then examines how a blanket ban on sponsored political advertising may impact transparency and equality of political competition online, with particular focus on the implications for smaller and emerging political actors. The analysis then turns to the recent Romanian presidential election, which was annulled due to widespread online manipulation. This case illustrates the risks posed by unregulated or insufficiently regulated digital campaigns, while highlighting the lessons that should be learned for the future of electoral integrity. The article concludes by offering recommendations for aligning EU regulatory objectives with practical compliance measures to safeguard the democratic process while ensuring fair and transparent political communication in the digital sphere.

Key words: Elections, Political Advertising, TTPA, Targeting

Introduction

On the 25th of July 2025, Meta announced that it would suspend all sponsored political, social and electoral advertising in the EU from October 2025. By their own words, the decision comes as an "*unintended consequence of burdensome regulation*."³ The regulation referred to is the new Transparency and Targeting of Political Advertising Regulation (TTPA), which entered into force on the 9th of April

¹ Funded by the EU NextGenerationEU through the Slovak Republic's Recovery and Resilience Plan under project no. 17Ro5-04-V01-00002.

² Comenius University, Faculty of Law, Department of IT and IP Law.

³ META Platforms, Inc. *Ending political, electoral and social issue advertising in the EU*. [online] Meta Newsroom 9. july 2025 [accessed 20.09. 2025]. Available at: <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>.

2024.⁴ This means that it will no longer be possible to purchase promotion of political content through paid advertising. While political messages will still circulate organically through the algorithms, the removal of paid promotion has the potential to reshape the landscape of online campaigning, raising questions about transparency, equality of political opportunity, and the unintended consequences of regulatory design.

This article adopts a qualitative, doctrinal and analytical approach combined with case study analysis. The legal framework is examined through close reading of the key provisions of the TTPA, complemented by secondary literature, academic commentary, and policy documents. The main contribution of this article is to analyse and assess the possible impacts of Meta's withdrawal from political advertising on transparency and electoral integrity. It also seeks to suggest how EU rules can be made more workable.

The article proceeds in several steps. First, it outlines the core provisions of the TTPA. It then turns to examine Meta's decision to withdraw from political advertising. The next section focuses on scholarly criticism of the TTPA, in particular, the questions of scope, competence, and enforcement. The case study of the annulment of Romanian elections is then introduced to highlight the risks of unregulated digital campaigning. Furthermore, the article considers the wider possible consequences of Meta's ban, mainly the loss of transparency tools and algorithmic amplification. The article concludes with recommendations for aligning EU regulatory ambition with practical compliance mechanisms, supported by reflections on the potential role of the Digital Services Act (DSA).

The TTPA overview

The TTPA is a response to previous cases of data abuse and manipulative microtargeting practices.⁵ Notoriously known is the scandal of Cambridge Analytica (CA), where the company had harvested Facebook users' data without their consent. The data were later used to create psychological profiles and behavioural models of millions of voters. Consequently, these profiles allowed CA to run highly targeted political ads, aiming to exploit people's personalities, fears, and preferences.⁶ This

⁴ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

⁵ STEPHENSON, Randall – RINCEANU Johanna – BOVERMANN Marc André: Regulating political advertising in the EU: transparency without accountability. In: *Eucrim: the European Criminal Law Associations' forum*, (1), 2025, pp.90-97.

⁶ HERN, Alex. Cambridge Analytica: how did it turn clicks into votes? [online] *The Guardian*, 6 May 2018 [accessed 24 September 2025]. Available at: <<https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>>.

behaviour has resulted in the suspicion of interference with the Brexit referendum and the US presidential election.⁷ Therefore, the explanatory memorandum to the TTPA emphasises that it aims to “*reduce the scope of problematic targeting tactics*.”⁸ The European Commission, relying on Article 114 TFEU, justified its intervention by pointing to both market and democratic concerns.⁹ The impact assessment identified several shortcomings in the existing framework: the absence of a common EU definition of political advertising, wide divergences in national rules, insufficient transparency obligations, and the risk of misuse of algorithmic targeting. This fragmented regulatory environment created what the European Commission described as a “*patchwork of national rules*,” which not only hampered oversight but also undermined public trust in electoral processes.¹⁰

Firstly, the TTPA establishes a broad concept of political advertising. It is characterized by two main types: a) messages by, for, or on behalf of a political actor, and b) messages that can influence and are designed to influence the outcome of an election or referendum, voting behaviour, or a legislative or regulatory process.¹¹ The latter type is sometimes called “*issue ads*”¹² and should be understood as messages that are directly sponsored by politicians, or are designed to have political effects.¹³ This means that content can still be considered as political advertising even though

⁷ CHAN, Adrian. Cambridge Analytica and our lives inside the surveillance machine. [online] *The New Yorker*, 21 March 2018 [accessed 24 September 2025]. Available at: <<https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine>>; KANG, Cecilia – FRENKEL, Sheera. Facebook says Cambridge Analytica harvested data of up to 87 million users. [online] *The New York Times*, 4 April 2018 [accessed 24 September 2025]. Available at: <<https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>>; ROSENBERG, Matthew – CONFESSORE, Nicholas – CADWALLADR, Carole. How Trump consultants exploited the Facebook data of millions. [online] *The New York Times*, 17 March 2018 [accessed 24 September 2025]. Available at: <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>.

⁸ European Commission, TTPA Proposal, Explanatory Memorandum.

⁹ VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p. 193.

¹⁰ European Commission, ‘TTPA Impact Assessment’, p. 6.

¹¹ TTPA, Art. 3/2.

¹² NENADIĆ, Iva – BLEYER-SIMON, Konrad. Issue-based advertising. [online] European Digital Media Observatory, 2021 [accessed 24 September 2025]. Available at: <<https://cadmus.eui.eu/handle/1814/74326>>; VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p.184.

¹³ ESKENS, Sjoerd. The role of the Regulation on the transparency and targeting of political advertising and European Media Freedom Act in the EU’s anti-disinformation strategy. In: *Computer Law & Security Review*, Vol. 58 (2025), p. 5.

it does not come from a mouth of the political actor.¹⁴ Moreover, it explicitly excludes certain types of messages such as official government communications, non-remunerated editorial content, or personal political opinions.¹⁵

Secondly, there are transparency and labelling obligations. Key provisions are Articles 11 and 12, which require all providers to clearly label all political advertisements as such, indicating the sponsor, relevant election/process, and if and how targeting techniques were used.¹⁶ TTPA also establishes a European archive for online political advertising to ensure public access to these advertisements and their transparency information.¹⁷

Thirdly, targeting techniques involving the processing of personal data is permitted only under certain conditions. It strictly prohibits profiling based on special categories of personal data (e.g., political opinions, ethnicity)¹⁸ and only permits the use of other personal data if explicitly consented to political advertising purposes.¹⁹ Crucially, the TTPA bans the use of such techniques to target individuals who are at least one year below the national voting age.²⁰ Additionally, operators employing these techniques must adopt and publicize internal policies describing their methods, maintain records of their usage and parameters, conduct annual risk assessments on fundamental rights, and provide transparent information to individuals about the logic and parameters of the targeting, as well as offering equivalent service alternatives if consent is refused.²¹

Lastly, the TTPA introduces significant financial sanctions for violations. These may amount to up to 6% of the annual income or budget of the advertiser or service provider, or 6% of their global turnover from the previous financial year.²²

¹⁴ VAN DRUNEN, Max – HELBERGER, Natali – SCHULZ, Wolfgang – DE VREESE, Claes. The EU is going too far with political advertising! [online] *DSA Observatory*, 16 March 2023 [accessed 24 September 2025]. Available at: <https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/>.

¹⁵ TTPA, Art. 1 /2, 3.

¹⁶ TTPA, Art. 11-12.

¹⁷ TTPA, Art. 13.

¹⁸ TTPA, Art. 18.

¹⁹ TTPA, Art. 18/1 b).

²⁰ Ibid.

²¹ TTPA, Art. 19.

²² TTPA, Art. 25.

Meta's reasoning

Meta's reasoning comes down to legal uncertainty and regulatory complexity under the TTPA.²³ As outlined above, the regulation requires detailed labelling of political ads, the maintenance of transparency notices, and the storage of advertisements, while also imposing strict limits on targeting techniques. Thus, Meta claims that the TTPA will greatly limit how certain ads can reach desired audiences, and as a result, the content shown to users will be less relevant.²⁴

Furthermore, they argued that meeting these obligations across 27 Member States, each with its own electoral laws, would create a high degree of regulatory fragmentation and expose the platform to substantial legal risks and potential sanctions.²⁵ Rather than invest in compliance systems that might still prove insufficient, Meta opted for the safest course of action: a blanket suspension of sponsored political advertising in the EU, even though this decision could significantly reshape the landscape of online political campaigning.

Critical perspectives on the TTPA

Firstly, it has been pointed out that the definition of political advertising is exceptionally broad.²⁶ As mentioned above, Article 3(2) extends the scope to „*issue ads*“ which are liable to influence the outcome of an election. According to Hoznagel, „*the resulting broad scope would be in line with the lawmakers' intention to de-amplify disinformation blending with user-generated content, such as Kremlin trolls and the*

²³ META Platforms, Inc. *Ending political, electoral and social issue advertising in the EU*. [online] *Meta Newsroom* 9. July 2025 [accessed 20.09. 2025]. Available at: <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>.

²⁴ Ibid.

²⁵ Ibid.

²⁶ LINDROOS-HOVINHEIMO, Susanne. The proposed EU regulation on political advertising has good intentions, but too wide a scope. [online] *European Law Blog*, 23 February 2022 [accessed 24 September 2025]. Available at: <<https://www.europeanlawblog.eu/pub/the-proposed-eu-regulation-on-political-advertising-has-good-intentions-but-too-wide-a-scope/release/1>>. VAN DRUNEN, Max – HELBERGER, Natali – SCHULZ, Wolfgang – DE VREESE, Claes. The EU is going too far with political advertising! [online] *DSA Observatory*, 16 March 2023 [accessed 24 September 2025]. Available at: <<https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/>>.

like.”²⁷ However, there are concerns that this „catch-all approach“ would cover all kinds of legitimate political critique, which is quintessential in a public debate.²⁸ It was argued that this broad interpretation could potentially interfere with the freedom of expression.²⁹ The European Court of Human Rights (ECtHR) emphasized that a narrow scope of restrictions is awarded for political speech since it deserves the greatest protection in a democratic society.³⁰–Given the exceptionally broad definition, the TTPA could impose a disproportionate number of obligations, including financial and administrative burden for a wide range of content which is not political advertising *per se*, but meets the condition that it can influence the outcome of an election and is therefore subject to regulation.³¹ This interpretation risks capturing issue-based advocacy by NGOs, trade unions, or civil society organisations that were never intended to be regulated in the same way as professional political campaigns.³²

This illustrates the central tension in the TTPA: while intended to combat covert manipulation and disinformation, the vague criterion of being “*liable to influence*” creates legal uncertainty, risks over-compliance, and may have a chilling effect on lawful public-interest communication, which would be excessively overburdened by regulatory obligations.

Another line of criticism concerns the Commission’s reliance on the internal market competence under Article 114 TFEU as the legal basis for the TTPA – or the so-called “competence creep”.³³ The Commission justifies intervention by pointing to the fragmentation of national rules and the supposed obstacles this creates for cross-

²⁷ HOLZNAGEL, Daniel. Political advertising and disinformation: *The EU Draft Regulation on Political Advertising Might De-Amplify Political Everyday-User Tweets - and Become a Blueprint for Stronger Online Platform Regulation*. [online] *Verfassungsblog*, 23 March 2023 [accessed 24 September 2025]. Available at: <<https://verfassungsblog.de/political-advertising-and-disinformation/>>.

²⁸ LINDROOS-HOVINHEIMO, Susanne. The proposed EU regulation on political advertising has good intentions, but too wide a scope. [online] *European Law Blog*, 23 February 2022 [accessed 24 September 2025]. Available at: <<https://www.europeanlawblog.eu/pub/the-proposed-eu-regulation-on-political-advertising-has-good-intentions-but-too-wide-a-scope/release/1>>.

²⁹ Ibid.

³⁰ ECtHR, *Sanchez v. France* [GC], para. 146.

³¹ LINDROOS-HOVINHEIMO, Susanne. The proposed EU regulation on political advertising has good intentions, but too wide a scope. [online] *European Law Blog*, 23 February 2022 [accessed 24 September 2025]. Available at: <<https://www.europeanlawblog.eu/pub/the-proposed-eu-regulation-on-political-advertising-has-good-intentions-but-too-wide-a-scope/release/1>>.

³² VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p. 184.

³³ DE WITTE, Bruno. Exclusive Member State competences – is there such a thing? In: GARBEN, Sacha – GOVAERE, Inge (eds.): *The division of competences between the EU and the Member States: reflections on the past, the present, and the future*. Portland, OR: Hart Publishing, 2017, p. 69.

border providers of political advertising services.³⁴ Yet, the impact assessment offers little evidence of a functioning internal market for such services that is genuinely hindered by regulatory divergence. Instead, the reasoning blends economic and non-economic objectives, including the protection of democracy and public trust.³⁵ Therefore, critics argue that the Commission's justification for intervention, relying on Art. 114 TFEU is weak, since "*mere finding of disparities and abstract risks of obstacles to the exercise of fundamental (market) freedoms, however, is not sufficient to trigger the internal market competence.*"³⁶ According to this, the TTPA could be viewed as stretching the internal market rationale well beyond its original economic intentions.³⁷

Moreover, the TTPA could be seen as expanding EU competences into a sensitive area traditionally reserved for Member States, which have diverse electoral systems and democratic visions.³⁸ In this regard, the ECtHR has emphasized the lack of consensus in the sphere of political advertising and has "*declined to recommend a common position on the issue.*"³⁹ The reasoning comes down to "*particularly complex balancing of interests, and is tied to national culture and political history.*"⁴⁰ Therefore, a uniform approach cuts through this diversity, creating tension with core aspects of national sovereignty, an area where the ECtHR and Council of Europe have historically been reserved in standardization efforts.⁴¹

Lastly, serious doubts also persist as to whether the TTPA will be effective in practice, since it is faced with some application, monitoring, and enforcement challenges. As Nikiforov observes, the TTPA "*falls short in reducing the impact of human and*

³⁴ European Commission, 'TTPA Impact Assessment', 6.

³⁵ European Commission: Directorate-General for Communication and Leyen, U. v. d., *Political guidelines for the next European Commission 2019-2024 – Opening statement in the European Parliament plenary session 16 July 2019 ; Speech in the European Parliament plenary session 27 November 2019*, Publications Office of the European Union, 2020, <<https://data.europa.eu/doi/10.2775/101756>>.

³⁶ CJEU, Tobacco Advertising C-376/98, 05.01.2000, para. 84.

³⁷ VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p.197.

³⁸ Ibid, pp.188-189.

³⁹ ECtHR, Animal Defenders International v United Kingdom, para. 123.

⁴⁰ DOBBER, Tom – Ó FATHAIGH, Ronan – ZUIDERVEEN BORGESIU, Frederik J. The regulation of online political micro-targeting in Europe. *Internet Policy Review*, Vol. 8, No. 4 (2019), p. 14.

⁴¹ VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p. 189.

automated bias in the reviewing of content,”⁴² leaving persistent vulnerabilities in moderation systems that rely heavily on under-resourced human reviewers and imperfect AI tools. Moreover, enforcement is left largely to national regulators, many of whom lack the resources or institutional expertise to oversee complex cross-border digital campaigning, since some Member States previously lacked any regulation⁴³ of political campaigning.⁴⁴ This creates the risk of uneven application and weak oversight. Taken together, these factors cast doubt on whether the TTPA’s transparency and targeting provisions can be fully realised and act as a safeguard of democratic integrity.

Lessons from Romania and possible impact of the ban

As outlined above, the TTPA certainly has its flaws and weak points. However, the question arises if online political advertising would be better off in a less regulated environment, which will be the case after Meta’s ban. The reactions so far have not been very favourable to this scenario. For instance, Irish MEP Ríordáin has stated that this decision is “*a dark day for democracy and will result in a massive increase in disinformation and electoral manipulation from sinister forces*.”⁴⁵

The annulment of the 2024 Romanian presidential elections by the Constitutional Court provides an example of how unregulated digital campaigning can undermine democratic processes. TikTok, despite banning paid political advertising⁴⁶ has played a key role in influencing the Romanian elections. Tens of thousands of fake accounts, many operated from outside Romania, were created to flood the platform to promote one largely unknown far-right candidate, Călin Georgescu. Consequently, by abusing TikTok’s own algorithms, the candidate received disproportionate

⁴² NIKIFOROV, Liubomir. Transparency in targeting of political advertising: challenges remain. [online] SSRN, 1 November 2024 [accessed 24 September 2025]. Available at: <<https://ssrn.com/abstract=5054430>>.

⁴³ CAPPELLO, Maja. (ed.), *Media coverage of elections: the legal framework in Europe*, IRIS Special, European Audiovisual Observatory, Strasbourg, 2017.

⁴⁴ VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), p. 191.

⁴⁵ Ó RÍORDÁIN, Aodhán. Meta political ad ban opens the gates for disinformation. [online] *Labour.ie*, 29 July 2025 [accessed 24 September 2025]. Available at: <<https://labour.ie/news/2025/07/29/meta-political-ad-ban-opens-the-gates-for-disinformation/>>.

⁴⁶ TIKTOK. TikTok ads policy: politics, government and elections. [online] *TikTok Business Help Center*, [accessed 24 September 2025]. Available at: <<https://ads.tiktok.com/help/article/tiktok-ads-policy-politics-government-and-elections#anchor-1-o>>.

visibility compared to competitors, while the financing behind his promotion remained opaque and unreported.⁴⁷

The Constitutional Court of Romania has emphasized that the elections were manipulated *“through the non-transparent use of digital technologies and artificial intelligence in the electoral campaign in violation of the electoral legislation, and through the funding from unreported sources of the electoral campaign, including the online one.”*⁴⁸ It further underlined that the free expression of the vote had been violated because voters were misinformed in a campaign where one candidate was *“aggressively promoted carried out by circumventing national legislation and abusing the algorithms of social media platforms.”*⁴⁹

Thus, a major concern raised by Meta’s withdrawal is that in an unregulated online environment, foreign interference and the spread of disinformation could intensify.⁵⁰ As we have seen in the case of the Romanian election, TikTok’s own ban on political advertising did not prevent such manipulation; instead, it pushed electoral influence into unregulated, muddy waters that were far more difficult to monitor or control. Now that Meta has joined the *“no political ads club”*, there is reason to fear that such behaviour will become increasingly widespread and will distort online political campaigning.

Furthermore, the withdrawal from sponsored political advertising may amplify the role of platform algorithms. Research has consistently shown that algorithms, prioritise divisive content which triggers strong emotional reactions, particularly anger and fear.⁵¹ This form of “rage-bait” content is more likely to be recommended, shared, and promoted organically because it keeps users engaged for longer. Crucially, since users are repeatedly exposed to content that aligns with their current views and intensifies their emotional responses, this form of organic dissemination

⁴⁷ LOFTUS, Alex. EU investigates TikTok over alleged Russian meddling in Romanian vote. [online] *BBC News*, 17 December 2024 [accessed 24 September 2025]. Available at: <<https://www.bbc.com/news/articles/cm2v13nz2020>>.

⁴⁸ Constitutional Court of Romania, RULING No 32 of 6 December 2024 on the annulment of the electoral process for the election of the President of Romania in 2024, para. 11.

⁴⁹ *Ibid.*, para. 14.

⁵⁰ Ó RÍORDÁIN, Aodhán. Meta political ad ban opens the gates for disinformation. [online] *Labour.ie*, 29 July 2025 [accessed 24 September 2025]. Available at: <<https://labour.ie/news/2025/07/29/meta-political-ad-ban-opens-the-gates-for-disinformation/>>.

⁵¹ BRADY, William J. – et al. Emotion shapes the diffusion of moralized content in social networks. In: *Proceedings of the National Academy of Sciences*, Vol. 114, No. 28 (2017), pp. 7313–7318.; MILLI, Smitha – CARROLL, Micah – WANG, Yike – PANDEY, Sashrika – ZHAO, Sebastian – DRAGAN, Anca D. Engagement, user satisfaction, and the amplification of divisive content on social media. In: *PNAS Nexus*, Vol. 4, No. 3 (March 2025).

fosters echo chambers and progressively radicalizes existing beliefs.⁵² The danger is that such dynamics privilege **hateful, polarising, and negative messaging** over substantive debate, will further distort public discourse and undermine the integrity of democratic deliberation.⁵³

Moreover, Meta's ban on sponsored political advertising is likely going to negatively impact emerging political actors and NGOs, since these groups often rely on paid promotion to gain visibility. Established parties can use their existing networks and followings to ensure organic reach, but new subjects frequently use small-scale, low-budget ads to circulate often non-sensational material.⁵⁴ Yet, as explained above, this type of content rarely performs well under algorithmic conditions that privilege negative emotions. Therefore, smaller actors risk being invisible in the noisy online environment, while more extreme voices profit from the organic amplification of divisive material.

To summarize, banning political advertising does not remove the risks of manipulation, but instead drives them into opaque and unaccountable channels. Meta's decision risks recreating these vulnerabilities on a much larger scale, depriving regulators, journalists, and citizens of transparency tools while amplifying the dominance of algorithmic content spreading. Therefore, the case from Romania demonstrates that regulation is not only desirable but necessary to safeguard electoral integrity in the digital age.

Recommendations and conclusion

As illustrated above, neither Meta's withdrawal from political advertising nor the TTPA in its current form offer a fully satisfactory response to the challenges of online political campaigning. Ultimately, the EU must align its transparency goals with practical compliance mechanisms. The lesson for the EU is twofold: under-regulation enables disinformation and manipulation, while over-regulation risks pushing platforms out, reducing transparency and limiting political participation.

However, this dynamic should not be viewed as a binary choice. Between these extremes lies a policy and institutional middle ground, where public authorities can actively shape platform behaviour through incentives, enforcement, and cooperation. The DSA already obliges very large online platforms such as Meta to assess and mitigate risks to public discourse and electoral processes and oversight by

⁵² JAVED, Usama – JAVED, Umer. The influence of social media algorithms on political polarization and public opinion. In: *Online Media and Society*, Vol. 4, No. 2 (2023), pp. 44–52.

⁵³ O'DONOGHUE VELIKIĆ, Clare. Meta's ban on political ads will mean less transparency and more slop for users. [online] *Irish Examiner*, 30 July 2025 [accessed 24 September 2025]. Available at: <<https://www.irishexaminer.com/opinion/commentanalysis/arid-41678339.html>>.

⁵⁴ Ibid.

the European Board for Digital Services.⁵⁵ Stronger enforcement of these provisions could help close gaps left by the TTPA and ensure that electoral systemic risks are addressed while maintaining democratic oversight.

Moreover, while Meta's decision will significantly limit political advertising on the largest platforms (Facebook and Instagram), the TTPA remains applicable to a wide range of other actors. Many smaller platforms, online publishers, and intermediaries still engage in paid promotion of political or issue-based content. Therefore, the TTPA's transparency, labelling, and targeting provisions remain not only relevant but crucial for maintaining accountability in this segment of the digital ecosystem.

To conclude, Meta's decision to suspend political advertising in the EU from October 2025 symbolises the consequence of complex regulation: faced with legal uncertainty and high compliance costs, platforms may choose withdrawal over adaptation. While this avoids legal risk for Meta, it deprives European democracy of valuable transparency tools and channels for pluralistic political communication. The increase in disinformation, the disadvantage to smaller actors and the shift toward algorithmic amplification all run counter to the very objectives of the TTPA. Thus, the TTPA risks achieving the opposite of what it intended to do. Yet, this outcome is not inevitable. By clarifying definitions, preserving oversight tools, supporting smaller actors, strengthening national regulators, and addressing the structural role of algorithms, the EU can align transparency objectives with practical compliance. Only such a balanced, middle-ground approach can ensure that online political communication genuinely strengthens, rather than undermines, democratic integrity in Europe.

Bibliography

1. BRADY, William J. – et al. Emotion shapes the diffusion of moralized content in social networks. In: *Proceedings of the National Academy of Sciences*, Vol. 114, No. 28 (2017), pp. 7313–7318.
2. CAPPELLO, Maja. (ed.), *Media coverage of elections: the legal framework in Europe*, IRIS Special, European Audiovisual Observatory, Strasbourg, 2017.
3. CJEU, Tobacco Advertising C-376/98, 05.01.2000. ECLI :EU:C:2000:544.
4. Constitutional Court of Romania, RULING No. 32 of 6 December 2024 on the annulment of the electoral process for the election of the President of Romania in 2024.
5. DE WITTE, Bruno. Exclusive Member State competences – is there such a thing? In: GARBEN, Sacha – GOVAERE, Inge (eds.): *The division of competences between the EU and the Member States: reflections on the past, the present, and the future*. Portland, OR: Hart Publishing, 2017, pp.59-73. ISBN 978-1-50991-348-0.

⁵⁵ DSA, Art. 34/1 c), 35.

6. DOBBER, Tom – Ó FATHAIGH, Ronan – ZUIDERVEEN BORGESIOUS, Frederik J. The regulation of online political micro-targeting in Europe. *Internet Policy Review*, Vol. 8, No. 4 (2019), pp. 1–22.
7. ECtHR, Animal Defenders International v. United Kingdom, app.no. 48876/08, 22.03. 2013.
8. ECtHR, Sanchez v. France [GC], app. no. 45581/15, 15.05. 2023.
9. ESKENS, Sjoerd. The role of the Regulation on the transparency and targeting of political advertising and European Media Freedom Act in the EU's anti-disinformation strategy. In: *Computer Law & Security Review*, Vol. 58 (2025), pp. 1–15.
10. European Commission, Impact Assessment Report Accompanying the document Proposal for a Regulation Of The European Parliament and of the Council on the transparency and targeting of political advertising, SWD(2021) 355 final. Available at: <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0355>>.
11. European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on the transparency and targeting of political advertising, Explanatory memorandum, COM(2021) 731 final. Available at: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0731>>.
12. European Commission: Directorate-General for Communication and Leyen, U. v. d., *Political guidelines for the next European Commission 2019-2024 – Opening statement in the European Parliament plenary session 16 July 2019 ; Speech in the European Parliament plenary session 27 November 2019*, Publications Office of the European Union, 2020, <<https://data.europa.eu/doi/10.2775/101756>>.
13. HERN, Alex. Cambridge Analytica: how did it turn clicks into votes? [online] *The Guardian*, 6 May 2018 [accessed 24 September 2025]. Available at: <<https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>>.
14. HOLZNAGEL, Daniel. Political advertising and disinformation: *The EU Draft Regulation on Political Advertising Might De-Amplify Political Everyday-User Tweets - and Become a Blueprint for Stronger Online Platform Regulation*. [online] *Verfassungsblog*, 23 March 2023 [accessed 24 September 2025]. Available at: <<https://verfassungsblog.de/political-advertising-and-disinformation/>>.
15. CHAN, Adrian. Cambridge Analytica and our lives inside the surveillance machine. [online] *The New Yorker*, 21 March 2018 [accessed 24 September 2025]. Available at: <<https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine>>.

16. JAVED, Usama – JAVED, Umer. The influence of social media algorithms on political polarization and public opinion. In: *Online Media and Society*, Vol. 4, No. 2 (2023), pp. 44–52.
17. KANG, Cecilia – FRENKEL, Sheera. Facebook says Cambridge Analytica harvested data of up to 87 million users. [online] *The New York Times*, 4 April 2018 [accessed 24 September 2025]. Available at: <<https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html>>.
18. LINDROOS-HOVINHEIMO, Susanne. The proposed EU regulation on political advertising has good intentions, but too wide a scope. [online] *European Law Blog*, 23 February 2022 [accessed 24 September 2025]. Available at: <<https://www.europeanlawblog.eu/pub/the-proposed-eu-regulation-on-political-advertising-has-good-intentions-but-too-wide-a-scope/release/1>>.
19. LOFTUS, Alex. EU investigates TikTok over alleged Russian meddling in Romanian vote. [online] *BBC News*, 17 December 2024 [accessed 24 September 2025]. Available at: <<https://www.bbc.com/news/articles/cm2v13nz2020>>.
20. META Platforms, Inc. *Ending political, electoral and social issue advertising in the EU*. [online] *Meta Newsroom* 9. July 2025 [accessed 20.09. 2025]. Available at: <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>.
21. MILLI, Smitha – CARROLL, Micah – WANG, Yike – PANDEY, Sashrika – ZHAO, Sebastian – DRAGAN, Anca D. Engagement, user satisfaction, and the amplification of divisive content on social media. In: *PNAS Nexus*, Vol. 4, No. 3 (March 2025).
22. NENADIĆ, Iva – BLEYER-SIMON, Konrad. Issue-based advertising. [online] European Digital Media Observatory, 2021 [accessed 24 September 2025]. Available at: <<https://cadmus.eui.eu/handle/1814/74326>>.
23. NIKIFOROV, Liubomir. Transparency in targeting of political advertising: challenges remain. [online] SSRN, 1 November 2024 [accessed 24 September 2025]. Available at: <<https://ssrn.com/abstract=5054430>>.
24. Ó RÍORDÁIN, Aodhán. Meta political ad ban opens the gates for disinformation. [online] *Labour.ie*, 29 July 2025 [accessed 24 September 2025]. Available at: <<https://labour.ie/news/2025/07/29/meta-political-ad-ban-opens-the-gates-for-disinformation/>>.
25. O'DONOGHUE VELIKIĆ, Clare. Meta's ban on political ads will mean less transparency and more slop for users. [online] *Irish Examiner*, 30 July 2025 [accessed 24 September 2025]. Available at: <<https://www.irishexaminer.com/opinion/commentanalysis/arid-41678339.html>>.

26. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.
27. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
28. ROSENBERG, Matthew – CONFESSORE, Nicholas – CADWALLADR, Carole. How Trump consultants exploited the Facebook data of millions. [online] *The New York Times*, 17 March 2018 [accessed 24 September 2025]. Available at: <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>.
29. STEPHENSON, Randall – RINCEANU Johanna – BOVERMANN Marc André: Regulating political advertising in the EU: transparency without accountability. In: *Eucrim: the European Criminal Law Associations' fórum*, (1), 2025, pp.90-97.
30. TIKTOK. TikTok ads policy: politics, government and elections. [online] *TikTok Business Help Center*, [accessed 24 September 2025]. Available at: <<https://ads.tiktok.com/help/article/tiktok-ads-policy-politics-government-and-elections#anchor-1-0>>.
31. VAN DRUNEN, Max – HELBERGER, Natali – SCHULZ, Wolfgang – DE VREESE, Claes. The EU is going too far with political advertising! [online] *DSA Observatory*, 16 March 2023 [accessed 24 September 2025]. Available at: <https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/>.
32. VAN DRUNEN, Max Zeno – HELBERGER, Natalie – Ó FATHAIGH, Ronan. The beginning of EU political advertising law: unifying democratic visions through the internal market. In: *International Journal of Law and Information Technology*, Vol. 30, No. 2 (2022), pp. 181–205.

Contact details

Mgr. Soňa Juhášová

juhasova69@uniba.sk

Comenius University, Faculty of Law, Department of IT and IP Law

RETHINKING AUTOMATED VEHICLES REGULATION USING THE REGULATORY SANDBOX

Stela Košťálová¹

Abstract: The capacity of traditional regulation in the automotive sector to address innovations is limited by the pace and complexity of technologies. The rise of automated technologies in vehicles exposes the limits of legal frameworks that are slow to adapt to dynamic advancements. The legal framework in the field of automated vehicles must remain effective, regulation must account for dynamics of technological development while ensuring protection of individual rights and public safety. This article explores the possibilities for changing the rigid regulatory approach without causing harm, using a regulatory sandbox. The regulatory sandbox offers a controlled environment for testing the new technologies under the regulatory oversight. The aim of this article is to demonstrate how the experience of regulatory sandbox can positively impact the regional or global regulation of automated vehicles. This advantage ensures that risks are managed in real time, making sandboxes a more effective regulatory tool in an era of rapid transformation.

Keywords: regulatory sandbox, automated vehicles, adaptive regulation, digital policy

Introduction

In the last century, the automotive industry has undergone a profound digital transformation driven by rapid technological development and intense competition between the manufacturers. The innovations are focused on road safety aiming to reduce fatal consequences of human error. Meanwhile internet connection has become standard feature in the automated vehicles. Together with innovation connected to the internet comes along risks, that can cause cybersecurity threats to malfunctions, which must be prevented. Confronted with these challenges, the protentional benefits are notable because approximately 3 700 people daily lost their lives in human caused accidents.² Automated vehicles represent some of the most complex issues withing the field of digital law. They uniquely integrate multiple

¹ Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava.

² UNECE: Règlements ONU applicables aux véhicules concernant la sécurité routière: méthode d'analyse coûts avantages. New York: UNECE, 2021. 87 p.

dimensions of digital legal frameworks, encompassing not only functional safety and cybersecurity but also intricate concerns in data protection, artificial intelligence and beyond. The convergence of these varied aspects within a single technology creates an unprecedented legal landscape, challenging our existing legal frameworks and pushing its boundaries. This paper examines the limitations in existing automated vehicles regulatory frameworks with a brief overview of the regulation on the international and European Union law level. Then the discussion will shift to elaborate on concept of regulatory sandboxes, their definition, benefits and the stages commonly employed in their implementation. To illustrate the practical application of this regulatory tool, the German experience with the regulatory sandbox will be further discussed.

Regulation plays an important role in shaping how automated driving systems can be tested and deployed across jurisdictions. Integrating a theory of regulation allows us to move beyond viewing rules as isolated commands and instead to understand regulation as a dynamic system shaped by multiple actors, instruments, and sources of authority. A complex interplay of legal rules, market dynamics, technological design, and social norms together determine how is innovation governed in the digital age. Two frameworks are particularly useful in capturing complex character of regulation, one from Lessig and second from the authors Yeung and Ranchordás.

Lawrence Lessig's modalities of regulation identifies four modalities:

1. Law,
2. Market,
3. Norms, and
4. Architecture.³

Law operates through formal rules enforced by sanctions. Market shapes conduct through price and competition. Norms reflect the social expectations. Architecture, whether digital code or physical design, structures what is technically possible, giving rise to the "code is law." These modalities interact continuously, ensuring that regulation extends far beyond statutes and decision of courts on regulatory gaps.

On the other side, regulatory framework from Yeung and Ranchordás complements this analysis by classifying regulatory tools according to their underlying techniques or sources of influence:

1. Command,
2. Competition,
3. Communication,
4. Code, and

³ LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Book, 1999. p. 71.

5. Community.⁴

Command refers to binding legal mandates. Competition harnesses market forces. Communication emphasizes transparency and information disclosure. Code embeds rules into technological design. Community underscores self-regulation and peer influence.

Lessig's modalities and the classification of regulatory tools highlight that regulation is inherently plural, relying on overlapping and often hybrid mechanism. This integrated perspective is especially valuable in information technology law, where complex technologies such as artificial intelligence, blockchain, and automated vehicles cannot be governed by law alone, but require coordinated engagement across legal, social, and technical sector.

The regulation of new technologies confronts the paradox formulated by David Collingridge, commonly referred to as the *Collingridge Dilemma*⁵. At the early stages of technological development, the lawmaker faces the danger of regulating based on incomplete knowledge, thereby constraining innovation with rules that may later prove incompatible with technological realities. However, at advanced stages as the technology has become widely available, intervention becomes expensive and in certain circumstances irreversible.⁶ This dilemma has implications for information technology law, where the pace of innovation often passes the capacity of traditional regulation.

The Limits of Existing (AV) Regulation

The regulation of automated vehicle shows the profound challenges that arise when rapidly evolving technologies interact with traditional legal frameworks. Regulator must address new risks, uncertainties and obsolescence in outdated laws⁷ while automated vehicles evolves fast. Conventional approaches to liability, safety and security, rooted in human decision-making and hierarchical enforcement. It struggles to accommodate automated systems within the automated vehicles that make decisions, collect vast quantities of personal data, and operates across multiple jurisdictions. Regulatory responses must therefore address complex questions of accountability, data protection, and ethical decision-making, while fostering innovation and public trust. This context highlights the relevance of adaptive approaches, such as regulatory sandboxes, which allow controlled experimentation

⁴ YEUNG, Karen, RANCHORDÁS, Sofia: An Introduction to Law and Regulation. Cambridge: Cambridge University Press, 2024. p. 168.

⁵ See COLLINGRIDGE, David: The Social Control of Technology. London: Francis Pinter, 1980.

⁶ COLLINGRIDGE, David: The Social Control of Technology. London: Francis Pinter, 1980. p. 19.

⁷ BENNETT MOSES, Lyria: How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target. In: Law, Innovation and technology, 2013, vol. 5. p. 7.

under the supervision of competent authorities, enabling regulators and innovators to collaboratively refine safety standards, formulate how to define liability, and develop governance mechanism suitable for automated vehicles. Adopting a flexible approach, collaborative oversight, and capacity for continuous learning, regulatory frameworks can ensure that automated vehicles contribute to societal welfare without compromising legal certainty or public safety. This is the shift from traditional regulatory tools, rigid regulation to experimental governance in the era of digital transformation.

European Union law and international law constitute fundamental pillars shaping national legal frameworks and ensuring member states' commitment to implement norms and fulfill international obligations. From the perspective of international law on automated vehicles are foundational the **Geneva Convention on Road Traffic** and the **Vienna Convention on Road Traffic**, but conventions also standardising road traffic regulation and driver eligibility. These conventions have brought order to the road traffic in the 20th century but today they seem to not follow the advancements in the automotive sector. Currently, there is a draft of **Convention on the use of automated vehicles in traffic**⁸ prepared to supplement the Geneva Convention on Road Traffic and the Vienna Convention on Road Traffic in the light of new technologies integrated in automated vehicles. Technical harmonisation has further advanced through the **1958 Agreement** with annexed UN Regulations No. 1-164 and the **1998 parallel Agreement** on Global Technical Regulation. This advancement in the regulation has covered road traffic needs in 20th century but nowadays are still absents the new features of motor vehicles in these frameworks. The slow legislative process of the drafted Convention on the use of automated vehicles in traffic highlights the need for flexible frameworks such as regulation sandbox integrated in the traditional legislative to bridge the gap between rapid technological progress and slower legislative process.

At the European level, the international regulation is directly integrated in the European Union's law⁹ and complementing through the **General Safety**

⁸ UNECE: Proposal for a draft report of the Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic for its second term. [online]. Geneva, 19. February 2024, 4 p. [cit. 2025-09-01]. Available at: <https://unece.org/sites/default/files/2024-02/ECE-TRANS-WP.1-GE3-2024-3e.pdf>.

⁹ See Recital 21 of the General Safety Regulation; Council Decision No. 2013/456/EU of 22 July 2013 amending Decision 97/836/EC with a view to accession by the European Community to the Agreement of the United Nations Economic Commission for Europe concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted to and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions (Revised 1958 Agreement) In: *Official Journal of the European Union* L 245, p. 1; Council Decision No. 2013/454/EU of 22 July 2013 amending Decision 2000/125/EC concerning the

Regulation¹⁰, the Regulation on Approval and Market Surveillance of Motor Vehicles¹¹ and the Commission Implementing Regulation for type-approval of Automated Driving Systems¹² which extend harmonisation and safety requirements for automated mobility. There are also additional layer reflecting the cybersecurity of vehicles through **NIS2 Directive**, the **Cyber Resilience Act** or the security of personal data through **GDPR**, reflecting not only the functional safety but also the security of the vehicle.

The Regulatory Sandbox Conception

The contrast between traditional regulatory approaches and innovative mechanism such as regulatory sandbox reflects a profound shift in regulation. Traditional regulation has long been rooted in a classic concept of regulation. This concept of regulation is characterised by rigid legal rules, uniform application, and ex post enforcement through sanctions. While such an approach offers certainty and predictability, it has proven increasingly inadequate to the governance of fast technological advancement. Regulatory sandboxes embody a more experimental paradigm of control. It provides a supervised and flexible environment in which regulators and innovators collaborate. This transformation represents a shift from rigidity to adaptability, from hierarchical authority to collaborative governance, and from risk-aversion to a more balanced risk-management compliance. Therefore, regulatory sandboxes do not negate the rule of law¹³ but rather reform the role of regulatory authority in a manner that aligns with the pace and unpredictability of technological innovation.

conclusion of the Agreement concerning the establishing of global technical regulations for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles (Parallel Agreement) In: *Official Journal of the European Union* L 245, p. 25.

¹⁰ Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (General Safety Regulation).

¹¹ Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

¹² Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS).

¹³ RANCHORDÁS, Sofia: Experimental Regulations and Regulatory Sandboxes: Law without Order? In: University of Groningen Faculty of Law Research Paper Series No. 10 (2021). p. 22.

Regulatory Sandbox is a mechanism that enables innovators to test new products and services under the supervision of a competent authority.¹⁴ This regulatory tool has many advantages. Firstly, regulatory sandboxes provide a **controlled environment** that is suited to the technology and designed for it. Secondly, they facilitate **continuous regulatory oversight**, enabling monitoring in present and make evidence-based adjustments. Thirdly, regulatory sandbox operates for a **limited period of time**. Fourthly, it **protects participants from penalties for potential breaches while testing** the technology, thereby fostering innovation development. Finally, regulatory sandboxes **create economic opportunities** by encouraging investment and experimentation within legally and ethically defined parameters. In European Parliament was formulated that regulatory sandbox has a dual function, on the one hand, it supports the development of companies and at the same time, this sandboxing experimentation helps legislators to shape regulatory frameworks accurate.¹⁵ Regulatory sandbox is a regulatory tool that is a mutually beneficial for both sides and ultimately provides citizens with a solution in which they had the opportunity to participate. At the end of the day, this tool can bring the best solution to the market.

As the regulatory sandbox represents a flexible mechanism that enables the controlled testing of new technologies prior to their full-scale deployment. It establishes a structured legal framework that allows companies to trial automated vehicles under the supervision of the regulatory authority without the immediate risk of sanctions.

The regulatory sandbox is often structured into three phases:

1. **Preparatory phase,**
2. **Testing phase,** and
3. **Final phase.**¹⁶

In the **preparatory phase** the regulator assesses applicants' eligibility through the organisational¹⁷, legal and technical aspects of the proposed technology. Applicant must submit prior detailed documentation covering the description, its risk management, analysis of its legal aspects and financial plan. Following evaluation, the regulator may schedule a meeting to agree on the testing plan. During the

¹⁴ ATTREY, Angela – LESHER, Molly - LOMAX, Christopher: The Role of sandboxes in promoting flexibility and Innovation in the digital age. Paris: OECD, 2020. p. 7.

¹⁵ European Parliamentary Research Service: Artificial intelligence act and regulatory sandboxes. Brusel: European Parliamentary Research Service, 2022. p. 2.

¹⁶ OECD: Regulatory sandboxes in artificial intelligence. In: OECD Digital Economy Papers. Paris: OECD Publishing, 2023, No. 356. p. 15; NBS. Regulatory Sandbox. [online]. Bratislava: NBS. [cit. 2025-09-01]. Available at: <https://nbs.sk/en/financial-market-supervision1/fintech/regulatory-sandbox/>.

¹⁷ RANCHORDÁS, Sofia: Experimental Lawmaking in the EU: Regulatory Sandboxes. In: University of Groningen Faculty of Law Research Paper Series No. 12 (2021). p. 15.

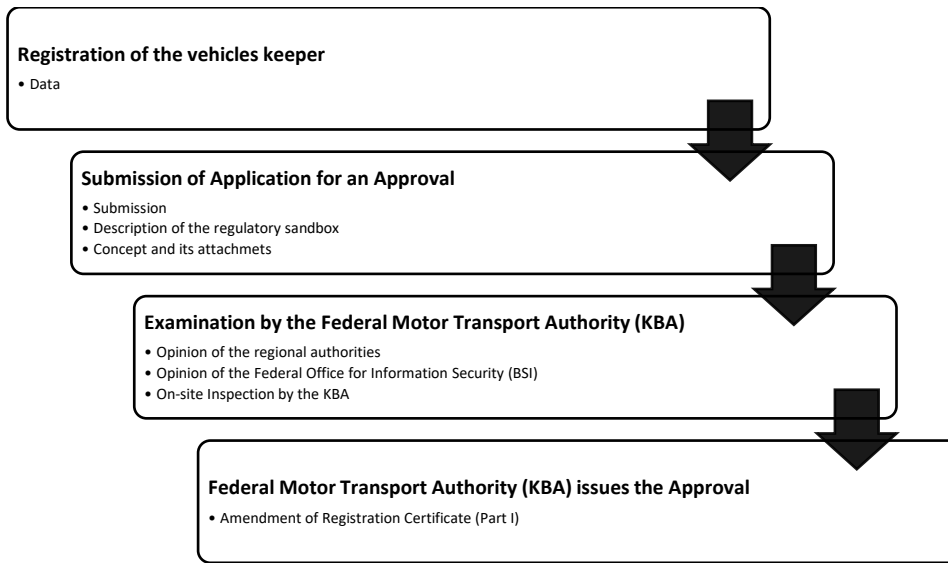
testing phase, the proposed innovation is implemented according to the agreed plan, with participants reporting in agreed period to the regulator and collaborating on adjustments. This includes the development of incident response mechanism. This phase is determined by mutual agreement. The **final phase** requires submission of a comprehensive report within a certain period of test completion and the implementation of conclusions under the regulator's supervision.

One of the most effective ways to demonstrate the potential of regulatory sandboxes is to analyse concrete examples that succeeded. The German **project RABus** stands out as remarkable example conducted between 2020 and 2023.¹⁸ In this project they test the technical, organisational and societal preconditions for integration of highly automated minibuses into public transport under real road traffic conditions. The RABus projects aim is the deployment of highly automated vehicles up to SAE Level 4 of Automation. This project consisted of two regulatory sandboxes in Friedrichshafen and Mannheim. In both cities the project addressed different urban context and own infrastructure. The first phase of the project deployment started with the technical development of automated minibuses Mercedes-Benz eVito, modifications of infrastructure in public spaces, approval procedures and structured legal assessment. The vehicles operated with automated driving system equivalent to SAE Level 2 of Automation. Legal assessment was approved pursuant to §1(1) of the Road Traffic Act¹⁹ in conjunction with §16(3) of the Autonomous Driving Act²⁰.

¹⁸ See WEINRICH, Ulrike et al. Abschlussbericht RABus (Phase 1): Reallabor für den Automatisierten Busbetrieb im ÖPNV in der Stadt und auf dem Land. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, 39 p.

¹⁹ Road Traffic Act. BGBl. I p. 310, 919. [Straßenverkehrsgesetz]

²⁰ Autonomous Driving Act. BGBl. I p. 986. [Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen]



Graph No. 1
Type-Approval Process²¹

All of it was followed by the implementation of proactive strategies to strengthen public trust and academic evaluation of this project. This first phase demonstrated that regulatory sandboxes on automated vehicles depend on following aspects:

- **Interplay of data quality,**
- **Supervisory tools, and**
- **Careful adaptation of the operational environment** of the highly automated minibus.²²

A clear definition of data quality and selection of relevant sensor data is proved to be essential deployment of highly automated minibuses. The use of metadata enabled more precise filtering and analysis of datasets.²³ The project underlines the importance of shared responsibility model, showing that safe operation is not solely

²¹ Gleiss Lutz Hootz Hirsch PartmbB Rechtsanwälte: RABus (Phase 1) Erprobungsgenehmigung nach §1i StVG i.V.m. §16 AFGBV. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, p. 29.

²² WEINRICH, Ulrike et al. Abschlussbericht RABus (Phase 1): Reallabor für den Automatisierten Busbetrieb im ÖPNV in der Stadt und auf dem Land. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, p. 36-37.

²³ WEINRICH, Ulrike et al. Abschlussbericht RABus (Phase 1): Reallabor für den Automatisierten Busbetrieb im ÖPNV in der Stadt und auf dem Land. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, p. 36-37.

the responsibility of vehicle manufacturers or operators. Public authorities and infrastructure providers also share liability by shaping the conditions for risk reduction. Therefore, the RABus project represents a great example of how regulation can facilitate innovation while safeguarding the rule of law.

Conclusion

Regulatory sandbox is an evolving component of a responsive regulatory approach, balancing technological advancement with the safety and security. While the existing pieces of legislation may appear to establish a comprehensive legal framework for motor vehicles, aligned with both international and European Union's law, the reality is more complex. At this phase of technological development, the ex-ante nature of traditional regulation cannot address legal challenges posed by the automated vehicles.

Integration of regulatory sandbox as a regulatory tool represents not an experiment, but a tool to support innovation safely. Automated vehicles as a technology pose interdisciplinary challenges, from safety and liability concerns to ethical dilemmas. Traditional regulatory tools are often rigid and retrospective, what is not compatible with the dynamic of the technologies. In comparison with the traditional regulatory tool such as pieces of legislation, the regulatory sandboxes offer a controlled but still flexible environment to create new solutions for an adaptive regulation. The success of regulatory sandbox in the context of automated vehicles hinges upon their careful design and governance.

The regulatory sandboxes have emerged as a promising complementary governance mechanism. By establishment of controlled environments in which technological application can be tested under the supervision of regulators, sandboxes strike a careful balance. Regulatory sandboxes provide the necessary oversight and legal guidance to mitigate foreseeable risks, while preserving the experimental space essential for learning and its adaption to a responsible innovation. Instead of postponing regulation, the regulatory sandbox enables a form of a proactive governance that moderates the rigidity of early intervention with the wisdom of empirical knowledge. This complementary approach to traditional lawmaking offers a balanced approach between premature restriction and delayed response.

Bibliography

1. ATTREY, Angela - LESHER, Molly - LOMAX, Christopher: The Role of sandboxes in promoting flexibility and Innovation in the digital age. Paris: OECD, 2020. 26 p.

2. BENNETT MOSES, Lyria: How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target. In: Law, Innovation and Technology, No. 1 (2013), p. 1-20.
3. COLLINGRIDGE, David: The Social Control of Technology. London: Frances Pinter, 1980. 192 p. ISBN 0-903804-63-2.
4. European Parliamentary Research Service: Artificial intelligence act and regulatory sandboxes. Brusel: European Parliamentary Research Service, 2022. 6 p.
5. Gleiss Lutz Hootz Hirsch PartmbB Rechtsanwälte: RABus (Phase 1) Erprobungsgenehmigung nach §1i StVG i.V.m. §16 AFGBV. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, 32 p.
6. LESSIG, Lawrence: Code and Other Laws of Cyberspace. New York: Basic Books, 1999. 320 p. ISBN 046503912X.
7. OECD: Regulatory sandboxes in artificial intelligence. In: OECD Digital Economy Papers. Paris: OECD Publishing, 2023, No. 356.
8. RANCHORDÁS, Sofia: Experimental Regulations and Regulatory Sandboxes: Law without Order? In: University of Groningen Faculty of Law Research Paper Series No. 10 (2021).
9. RANCHORDÁS, Sofia: Experimental Lawmaking in the EU: Regulatory Sandboxes. In: University of Groningen Faculty of Law Research Paper Series No. 12 (2021).
10. UNECE: Règlements ONU applicables aux véhicules concernant la sécurité routière: méthode d'analyse coûts avantages. New York: UNECE, 2021. 87 p.
11. UNECE. Proposal for a draft report of the Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic for its second term. [online]. Geneva, 19. February 2024, 4 p. [cit. 2025-09-01]. Available at: <https://unece.org/sites/default/files/2024-02/ECE-TRANS-WP.1-GE3-2024-3e.pdf>.
12. WEINRICH, Ulrike et al. Abschlussbericht RABus (Phase 1): Reallabor für den Automatisierten Busbetrieb im ÖPNV in der Stadt und auf dem Land. Stuttgart: Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart, 2025, 39 p.
13. YEUNG, Karen - RANCHORDÁS, Sofia: An Introduction to Law and Regulation. Cambridge: Cambridge University Press, 2024. 422 p. ISBN 9781009379007.

Contact details

Mgr. Stela Košťálová

stela.kostalova@flaw.uniba.sk

Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava

TRESTNOPRÁVNÝ PRESAH VYBRANÝCH ZAKÁZANÝCH PRAKTÍK PODĽA AKTU O UMELEJ INTELIGENCII¹

CRIMINAL LAW ASPECTS OF SELECTED PROHIBITED PRACTICES UNDER THE ARTIFICIAL INTELLIGENCE ACT

Marek Kordík², Petra Dražová³

Abstrakt: Príspevok stručne analyzuje vybrané zakázané praktiky podľa Aktu o umelej inteligencii s pohľadu trestnoprávnej zodpovednosti a naplnenia znakov jednotlivých možných skutkových podstát trestných činov. Príspevok taktiež stručne analyzuje možnosti trestnoprávnej zodpovednosti jednotlivých subjektov podieľajúcich sa na vývoji, nasadení alebo prevádzke konkrétneho počítačového systému využívajúceho umelú inteligenciu v Európskej únii, a to z pohľadu fyzických ako i právnických osôb a možnosti uplatnenia compliance programov. Súčasne analyzuje jednotlivé výnimky zo zakázaných praktík a predpoklady ich splnenia, pričom v zmysle prameňov rozširuje výklad určitých výnimiek aj na iné konania ako len trestné stíhanie, a to najmä konania o európskom zatýkacom rozkaze, mutatis mutandis i konanie o medzinárodnom zatýkacom rozkaze. Príspevok vychádza z normatívneho znenia relevantných ustanovení samotného Aktu o umelej inteligencii, ako i z jeho recitálov, ďalej i z vnútroštátnych prameňov trestného práva hmotného, z Usmernenia Európskej komisie k zakázaným praktikám, judikatúry Súdneho dvora EÚ k používaným pojmom podľa Aktu o umelej inteligencii ako i ďalších relevantných prameňov.

Kľúčové slová: umelá inteligencia, zakázané praktiky, skutková podstata, trestné právo, trestná zodpovednosť

¹ Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002. Spoluautori sú riešiteľmi projektu Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality, financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002.

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra trestného práva, kriminológie a kriminalistiky.

³ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva.

Abstract: The paper provides a concise analysis of selected prohibited practices under the Artificial Intelligence Act, exploring their implications for criminal liability and the elements of potential individual criminal offences. The paper also briefly considers the potential criminal liability of individual entities involved in the development, deployment, or operation of a specific computer system using artificial intelligence in the European Union, from the perspective of both natural and legal persons, and the possibility of applying compliance programs. Concurrently, it undertakes an analysis of individual exceptions to prohibited practices and the conditions for their fulfilment. In accordance with the sources, it extends the interpretation of certain exceptions to proceedings other than criminal proceedings, in particular proceedings on European arrest warrants, *mutatis mutandis*, and proceedings on international arrest warrants. The contribution is grounded in the normative wording of the relevant provisions of the Artificial Intelligence Act itself, as well as its recitals, and also on national sources of substantive criminal law, the European Commission's Guidelines on Prohibited Practices, the case law of the Court of Justice of the European Union on the terms used in the Artificial Intelligence Act, and other relevant sources.

Key words: artificial intelligence, prohibited practices, elements of crimes, criminal law, criminal liability

Úvod

Využívanie umelej inteligencie prináša mnoho výhod, avšak možno ju aj zneužiť na manipulatívne praktiky, ktoré sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv ukotvených v Charte základných práv EÚ vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.⁴ Zákaz uvedených praktík je ustanovený v čl. 5 AI Aktu.

V zmysle recitálu 26 AI Aktu sú jednotlivé ustanovenia o zakázaných praktikách založené na rizikovo orientovanom prístupe a majú zohľadniť hrozbu zneužitia systémov umelej inteligencie využitím ľudskej zraniteľnosti. Je potrebné zdôrazniť, že zakázané praktiky sa nevzťahujú iba na vysokorizikové systémy využívajúce umelú inteligenciu podľa čl. 6 ods. 1 s poukazom na Prílohu III AI Aktu, ale na všetky systémy

⁴ Recitál 28 Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (ďalej ako „AI Akt“).

uvádzané na trh,⁵ do prevádzky⁶ alebo týkajúce sa používania konkrétnych systémov.⁷ Zakázané praktiky sa uplatňujú od 2. februára 2025, čo môže v budúcnosti zohrať určitý vplyv, avšak primárne toto ustanovenie nemá vplyv na časovú pôsobnosť a retroaktivitu Trestného zákona, ako vnútroštátnej normy, podľa ktorej sa posudzuje trestnosť skutku.⁸ Uplatňovanie článku 5 AI aktu si bude vyžadovať posúdenie od prípadu k prípadu, pri ktorom bude v jednotlivých situáciách potrebné náležite zohľadniť konkrétne špecifiká.⁹

Využívanie podprahových techník, účelovo manipulatívnych alebo klamlivých techník a využívanie zraniteľností užívateľov podľa čl. 5 ods. 1 písm. a), písm. b) AI Aktu

Prvým druhom zakázaných praktík systémov umelej inteligencie je využívanie manipulatívnych praktík podľa čl. 5 ods.1 písm. a) AI Aktu s nasledovnými znakmi:

- existencia podprahovej techniky¹⁰ mimo vedomia osoby, resp. účelovo manipulatívnej alebo klamlivej techniky;
- (kumulatívne) s motívom prijať neracionálne pudové rozhodnutie, ktoré *a contrario* nie je založené na informovanom rozhodnutí;¹¹

⁵ Podľa čl. 3 ods. 10 AI Aktu uvádzaním na trh sa rozumie dodanie systému AI s cieľom distribuovať ho alebo používať ho na trhu Únie v rámci komerčnej činnosti, či už za odplatu alebo bezodplatne.

⁶ Podľa čl. 3 ods. 11 AI Aktu sa uvádzanie do prevádzky systému AI určenie na prvé použitie nasadzujúcemu subjektu alebo na vlastné použitie v Únii na jeho zamýšľaný účel, čo zahŕňa tak dodanie na prvé použitie tretím stranám, ako aj vlastný vývoj a nasadenie.

⁷ Podľa čl. 3 ods.12, ods. 13 AI Aktu sa používaním rozumie používanie alebo nasadenie systému v ktoromkoľvek okamihu jeho životného cyklu po jeho uvedení na trh alebo do prevádzky.

⁸ § 2 ods. 1 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej ako „TZ“).

⁹ Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, s. 7. (ďalej ako „**Usmernenia Komisie**“). Dostupné na: [Commission publishes the Guidelines on prohibited artificial intelligence \(AI\) practices, as defined by the AI Act. | Shaping Europe's digital future](#) [navštívené dňa 05.09.2025].

¹⁰ Podprahovou technikou je akýkoľvek postup, spočívajúci v signáloch a podnetoch (najmä zvukových, obrazových, video, resp. ich kombináciou, časová manipulácia, nasmerovanie pozornosti), ktoré nie vedome vnímané ľudskými zmyslami. Podprahové techniky musia byť schopné ovplyvňovať správanie spôsobom, pri ktorom si osoba neuvedomuje takýto vplyv, spôsob jeho fungovania ani jeho účinky na rozhodovanie alebo formovanie hodnôt a názorov danej osoby. In.: Usmernenia Komisie, s. 26.

¹¹ AI Akt nedefinuje pojem „informované rozhodnutie“, avšak v zmysle Usmernenia si vyžaduje pochopenie a znalosť relevantných informácií vrátane dostupných možností, rizík a prínosov každej voľby, možných účinkov systému umelej inteligencie na správanie a prípadne ďalších kontextových informácií, ktoré sú dôležité pre rozhodovanie alebo správanie osoby. In: Usmernenie Komisie, s. 31.

- príčinná súvislosť medzi podprahovou technikou mimo vedomia osoby alebo účelovo manipulatívnu, resp. klamlivou technikou a prijatím neinformovaného rozhodnutia;
- odôvodnený predpoklad spôsobenia značnej ujmy prijatím neinformovaného rozhodnutia.¹²

Pre naplnenie znakov zakázanej praktiky musia byť súčasne splnené všetky štyri podmienky a musí existovať hodnoverná príčinná súvislosť medzi použitými technikami, podstatným narušením správania osoby a značnou ujmu, ktorú uvedené správanie spôsobilo alebo je odôvodnené predpokladať, že spôsobí.¹³ Pod značnou ujmu sa rozumie fyzická, psychická, finančná a ekonomická ujma, ktorá sa v určitých prípadoch môžu spájať so širšou spoločenskou ujmu, ak sú porušené hodnoty Únie.

Druhou skupinou zakázaných praktík systémov s umelou inteligenciou je využívanie manipulatívnych praktík podľa čl. 5 ods.1, písm. b) AI Aktu s nasledovnými znakmi:

- využitie zraniteľnosti¹⁴ osoby z dôvodu jej veku, zdravotného stavu, ekonomickej alebo sociálnej situácie s cieľom ovplyvniť jej správanie;
- odôvodnený predpoklad spôsobenia značnej ujmy osobe ovplyvnením jej správania.

Na rozdiel od prvej skupiny zakázaných praktík nemusí ísť o podprahové techniky, ktorými sa má ovplyvniť rozhodovanie, ale zneužíva sa zraniteľnosť osoby na ovplyvnenie jej rozhodovania. Zmyslom zákazu uvedených praktík je ochrana pred oslabovaním a narúšaním samostatnosti rozhodovania a slobodnej voľby osôb tak, že si poškodení neuvedomujú, že sú zavádzaní alebo hoci s vedomím vlastného zavádzania, nie sú schopní ovládať svoje rozhodnutie alebo takejto technike odolávať.¹⁵ Z uvedeného vyplýva, že tieto techniky zneužívajú vek, zdravotný stav, ekonomickú situáciu, sociálne postavenie a osobnosť poškodeného na dosiahnutie želaného rozhodnutia.

V súlade s kontinentálnou školou teórie práva a občianskeho práva, možno informované rozhodnutie definovať ako „*vedomý, slobodný a vážny prejav vôle vyvolať zamýšľaný právny úkon.*“ In: KNAP, Viktor: Teorie práva. 1. vydání, Praha: C.H.Beck. 1995. s. 142. ISBN 80-7179-028-1. Dobrú definíciu poskytuje Lazar, keď uvádza, že „*vôľu možno prejaviť akýmkoľvek spôsobom, ktorý umožňuje poznanie jej obsahu.*“ In: LAZAR, Ján a kol.: Občianske právo hmotné. Všeobecná časť. Bratislava: Iura edition, 2006, s. 115-116. ISBN 80-8078-084-6.

¹² Nie je potrebné, aby poskytovateľ alebo subjekt nasadzujúci systém umelej inteligencie mal úmysel spôsobiť značnú ujmu, pokiaľ takáto ujma vyplýva z manipulatívnych alebo zneužívajúcich praktík využívajúcich AI. In: Recitál 29 AI Aktu.

¹³ Usmernenia Komisie, s. 25.

¹⁴ Zraniteľnosť možno chápať ako kognitívne, emocionálne, fyzické a iné formy náchylnosti, ktoré môžu ovplyvniť schopnosť jednotlivca alebo skupiny osôb prijímať informované rozhodnutia alebo inak ovplyvňovať ich správanie. In: Usmernenia Komisie, s. 35.

¹⁵ Recitál 29 AI Aktu.

Zákaz mieri najmä na praktiky poškodzujúce spotrebiteľov. Netýka sa zákonných postupov v súvislosti s liečbou duševných chorôb, fyzickej rehabilitácie, ak sú v súlade s platnými lekáorskými predpismi (napr. súhlas pacienta alebo jeho právneho zástupcu) alebo reklamy, ktorá je v súlade so zákonom.¹⁶

Z uvedeného vyplýva, že tieto postupy môžu naplňať aj skutkovú podstatu trestného činu, resp. skutkové podstaty viacerých trestných činov. V prvom rade môže ísť o trestný čin úžery podľa § 235 ods. 1, písm. a), ods. 2 TZ nakoľko sa týmto ustanovením chráni možnosť správneho rozhodovania v majetkových záležitostiach i samotný majetok.¹⁷ Dôvodom je neekvivalentný pomer vzájomného plnenia z týchto záväzkov a porušenie etických princípov zo strany páchatela, ktorý v záujme vlastného obohatenia ťaží z manipulatívnej techniky a neinformovaného rozhodnutia iného. Uvedené dokazovanie samotného nepomeru plnení v neprospech poškodeného tak ako to vyžaduje Trestný zákon v zmysle ustanovenia § 235 ods. 1, písm. a) TZ je možné podľa nášho názoru subsumovať pod spôsobenie závažnej ujmy¹⁸ podľa čl. 5 ods.1, písm. a), písm. b) TZ, súčasne v prípade skutkovej podstaty trestného činu úžery podľa § 235 ods.1, písm. a) TZ ako i zakázanej manipulatívnej praktiky podľa čl. 5 ods. 1, písm. a), písm. b) AI možno v oboch prípadoch hovoriť o ohrozovacom trestnom čine, ktorý na posúdenie trestnosti nevyžaduje spôsobenie následku. Objektívna stránka trestného činu úžery podľa §235 ods. 1, písm. a) TZ, pod ktorú možno subsumovať uvedenú praktiku spočíva v zneužití niečej tiesne, neskúsenosti, rozumovej slabosti alebo niečieho rozrušenia k tomu, aby páchatelovi alebo inému bolo poskytnuté alebo sľúbené plnenie, ktorého hodnota je v hrubom nepomere.¹⁹ Pokiaľ ide o charakter plnenia, musí mať majetkovú (i keď nie peňažnú) hodnotu, podľa terminológie čl. 5 by práve trestný čin úžery pokrýval závažnú majetkovú ujmu.²⁰ Hrubý nepomer je nutné posudzovať z hľadiska súčasných objektívnych výmenných hodnôt oboch plnení. Hodnota vzájomného plnenia sa stanoví podľa rovnakých zásad, ako sa určuje výška škody.²¹ K trestnej zodpovednosti sa vyžaduje, aby medzi zneužitím tiesne, neskúsenosťou, rozumovou slabosťou alebo rozrušením a hrubým nepomerom vzájomného plnenia bola príčinná súvislosť. Pritom jednotlivé uvedené skutočnosti nemusia byť jedinou a

¹⁶ Recitál 29 AI Aktu.

¹⁷ STRÉMY, T.; KURILOVSKÁ, L. a kol.: Trestný zákon, Komentár, II. Zväzok, 1.vydanie. Praha: Wolters Kluwer ČR, 2022, s. 509-510. ISBN 978-80-7676-430-9.

¹⁸ Pre posúdenie značnej ujmy je potrebné vychádzať z posúdenia jej závažnosti, kontextu a kumulatívnych účinkov, rozsahu, intenzity, zraniteľnosti dotknutých osôb, trvanie a nezvratnosť. In: Usmernenia Komisie, s. 37.

¹⁹ STRÉMY, T.; KURILOVSKÁ, L. a kol.: Trestný zákon, Komentár, II. Zväzok, 1.vydanie. Praha: Wolters Kluwer ČR, 2022. s. 511. ISBN 978-80-7676-430-9.

²⁰ Ibid, s.512-513.

²¹ Ibid, s. 513-514.

rozhodujúcou príčinu pre poskytnutie alebo pre sľub takého plnenia, ale stačí, aby tieto okolnosti k tomu spolupôsobili.

Na rozdiel od trestného činu podvodu podľa § 221 TZ, páchatel' trestného činu úžery neuvádza iného do omylu. Predstava poškodeného o podstate jeho konania pri úžere je správna, ale hodnotenie vzájomných plnení je nesprávne. Poškodený teda poskytuje alebo sľubuje plnenie v určitej tiesni, i keď vie, že hodnota je plnenia je k hodnote vzájomného protiplnenia v hrubom nepomere, alebo v dôsledku neskúsenosti, rozumovej slabosti alebo rozrušenia nie schopný zhodnotiť vzájomný pomer oboch plnení. Pri trestnom čine podvodu koná poškodený pod vplyvom svojho omylu alebo omylu inej osoby vyvolaného alebo využitého páchatel'om, bez toho aby konal pod vplyvom tiesne alebo neschopnosti posúdiť dôsledky svojho konania²² Zo subjektívnej stránky sa vyžaduje úmyselné zavinenie. Pre prípustnosť trestného stíhania voči osobe, ku ktorej má poškodený právo odoprieť výpoveď podľa § 130 TP, je nutný súhlas poškodeného podľa § 211 TP. Páchatel'om tohto trestného činu môže byť ktorákoľvek trestne zodpovedná osoba, fyzická i právnická. V § 235 ods. 2 TZ je definovaná druhá relevantná základná skutková podstata trestného činu úžery, ktorá je taktiež naplniteľná uvedenou zakázanou praktikou. Toto ustanovenie primárne chráni plnenia a služby, ktoré sú buď úplne, alebo sčasti regulované zákonom alebo spadajú do ochrany spotrebiteľa, v rámci, ktorých môže dôjsť k zneužitiu dominantného postavenia a podmieňovať plnenie prijatím iných služieb alebo hodnôt, ktoré následne môžu byť v hrubom nepomere.²³

Taktiež môže ísť vo vzťahu k zakázaným praktikám o trestný čin podvodu podľa § 221 TZ, nakoľko objektívna stránka tohto trestného činu spočíva v spôsobení škody a vo využití omylu alebo uvedenia do omylu osoby, pričom môže ísť aj o tretiu osobu, odlišnú od poškodeného. V tomto prípade poškodený na rozdiel od úžery koná v omyle, do ktorého je uvedený, alebo v ktorom je udržiavaný práve zakázanou manipulatívnu technikou. Pojem *uvedenie do omylu* znamená aktívne vedomé predstieranie faktov alebo skutočností, ktoré sú rozporné s realitou. Môže tak konať nielen vo vzťahu priamo k poškodenému, ale aj k iným osobám. Omyl je nezhoda predstavy človeka so skutočným stavom. *Využitie niečieho omylu* je možné definovať tak, že páchatel' svojím konaním omyl nevyvolal, uvedený omyl využije vo svoj prospech. Vzhľadom na subjektívnu stránku tohto trestného činu si páchatel' musí byť vedomý existencie omylu.²⁴ Ak by uvedená zakázaná praktika mala povahu investície, príp. pyramídovej hry (tzv. investičné podvody a Ponziho schémy),

²² R 85/1956.

²³ Príloha č. 1 k zákonu č. 108/2024 Z. z. o ochrane spotrebiteľa a o zmene a doplnení niektorých zákonov obsahuje zoznam praktík, ktoré sa za každých okolností považujú za nekalé.

²⁴ STRÉMY, T.; KURILOVSKÁ, L. a kol.: Trestný zákon, Komentár, II. Zväzok, 1.vydanie. Praha: Wolters Kluwer ČR, 2022. s. 464-465. ISBN 978-80-7676-430-9.

prichádza do úvahy naplnenie znakov skutkovej podstaty kapitálového podvodu podľa § 224 ods. 1 TZ.

Tretia do úvahy prichádzajúca možnosť v súvislosti s analyzovanou zakázanou praktikou, je skutková podstata trestného činu hrubého nátlaku podľa § 190 ods. 1 TZ. Objektívna stránka spočíva v tom, že páchatel' neoprávnene núti iného, aby mu poskytol majetkové alebo nemajetkové plnenie za vnucované služby alebo dokonca len predstierané služby, ktoré poškodenému poskytne. Pričom táto hrozba nemusí smerovať priamo proti napadnutému, môže sa týkať jeho detí, blízkej osoby, ale aj majetku.²⁵ Hrozba inej ťažkej ujmy môže spočívať v hrozbe spôsobenia majetkovej ujmy, vážnej ujmy na cti a dobrej povesti, môže smerovať k rozvratu manželstva, k začatiu trestného stíhania, a to bez ohľadu na to, či poškodený skutočne spáchal trestný čin.²⁶ Alternatívne k trestnému činu hrubého nátlaku, môže byť zakázanou praktikou naplnená skutková podstata trestného činu nátlaku podľa § 192 ods. 1 TZ, keďže práve týmto trestným činom je chránená sloboda rozhodovania jednotlivca. Objektívna stránka spočíva v tom, že páchatel' iného núti, aby niečo konal, opomenul alebo trpel, zneužívajúc jeho hmotnú núdzu alebo naliehavú nemajetkovú potrebu, alebo tieseň vyvolanú jeho nepriaznivými osobnými pomermi. Čin je dokonaný už vykonaním nátlaku (nútenia) za určených okolností. Nie je potrebné, aby páchatel' dosiahol plnenie z tohto záväzku.²⁷

Využívanie systémov s umelou inteligenciou na tzv. *social scoring* podľa čl. 5 ods. 1 písm. c) AI Aktu

Ďalším okruhom zakázaných praktík je tzv. *social scoring* jednotlivcov alebo skupín osôb, ktorý v zmysle čl. 5 ods. 1 písm. c) AI Aktu spočíva v klasifikácii osôb podľa ich sociálneho správania, osobných vlastností, pričom tieto praktiky vedú k segregácii či neférovému zaobchádzaniu v nesúvisiacich situáciách.

Kľúčové pre posúdenie zakázanej praktiky podľa tohto ustanovenia je neodôvodnenosť a neprimeranosť použitia týchto údajov na sociálne bodovanie, keďže boli získané za iným účelom.²⁸ Táto zakázaná praktika sa nevzťahuje na právnické osoby, ktoré sa stanú predmetom sociálneho bodovania,²⁹ iba na fyzické osoby. Táto praktika by za splnenia aj ďalších znakov skutkovej podstaty mohla byť kvalifikovaná ako trestný čin apartheidu a diskriminácie skupiny osôb podľa § 424a TZ. Uvedené by sa však vzťahovalo len na prípady, ak by praktiky sociálneho

²⁵ Porovnaj R 1/1980.

²⁶ R 27/1982.

²⁷ STRÉMY, T.; KURILOVSKÁ, L. a kol.: Trestný zákon, Komentár, II. Zväzok, 1.vydanie. Praha: Wolters Kluwer ČR, 2022. s. 289-291. ISBN 978-80-7676-430-9.

²⁸ Recitál 31 AI aktu

²⁹ Usmernenia Komisie, s. 64.

bodovania smerovali k vylúčeniu takejto osoby a bola by daná príčinná súvislosť medzi sociálnym bodovaním a jeho škodlivým účinkom.³⁰ Segregácia a apartheid sú v zmysle § 424a TZ považované za trestné a využitie zakázanej praktiky, ktorá smeruje k naplneniu uvedených foriem diskriminácie napĺňa objektívnu stránku tohto trestného činu. Zákaz segregácie a apartheidu vyplýva aj z Medzinárodného dohovoru o potlačení a trestaní zločinu apartheidu³¹ a Medzinárodného dohovoru o odstránení všetkých foriem rasovej diskriminácie.³² Objektívna stránka spočíva v uplatňovaní apartheidu alebo systematickej rasovej, etnickej, národnostnej alebo náboženskej segregácie, alebo inej rozsiahlej diskriminácie skupiny osôb, čím sa bráni v uplatňovaní ich základných ľudských práv a slobôd, politických, hospodárskych, kultúrnych a sociálnych práv. Trestnoprávne relevantná forma takejto zakázanej praktiky teda musí segregovať osoby na etnickej, náboženskej, rasovej, rodovej báze, priamo, alebo nepriamo a nie na základe iných, napríklad ekonomických kritérií (dôchodcovia, študenti, nezamestnaní, dlžníci a pod.). V prípade, že by došlo k usmrteniu takejto skupiny osôb, resp. k usmrteniu takejto skupiny osôb na základe takto vytvorenej selekcie, bolo by možné naplniť i skutkovú podstatu medzinárodného zločinu genocídy podľa Rímskeho štatútu.³³

Využívanie systému umelej inteligencie na individuálnu predikciu kriminality na základe profilovania fyzickej osoby podľa čl. 5 ods. 1 písm. d) AI Aktu

Uvedená zakázaná praktika je rizikovým profilovaním osôb, či a s akou pravdepodobnosťou sa v budúcnosti dopustia trestného činu, na základe jej subjektívnych charakteristík a osobnostných vlastností³⁴ a nie trestnoprávne relevantných konaní, alebo opomenutí. Posúdenie rizika musí byť založené aspoň na jednej z činností, a to buď profilovanie fyzickej osoby alebo posúdenie osobnostných vlastností a charakteristík fyzickej osoby.³⁵ Zákaz sa vzťahuje len na prediktívne modely umelej inteligencie, ktoré slúžia na posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin na základe hore uvedených

³⁰ Ibid.

³¹ Vyhláška ministra zahraničných vecí č. 116/1976 Zb. o Medzinárodnom dohovore o potlačení a trestaní zločinu apartheidu.

³² Vyhláška ministra zahraničných vecí č. 95/1974 Zb. o Medzinárodnom dohovore o odstránení všetkých foriem rasovej diskriminácie.

³³ DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE, Office of the Prosecutor of the ICC, March 3, 2025, s. 15. Dostupné na: [250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf](#) [navštívené dňa 04.09.2025].

³⁴ Napr. národnosť a etnický pôvod, výška úverov, vlastníctvo majetku, vzdelanie a sociálny status, adresa, počet detí a pod.

³⁵ Usmernenia Komisie, s. 69.

činností³⁶ a nevzťahuje sa na analýzy historických údajov a štatistík kriminality s cieľom lepšieho využívania síl a prostriedkov.³⁷ V súlade s prezumpciou nevinoty by sa fyzické osoby mali vždy posudzovať podľa ich skutočného správania. Fyzické osoby by sa nikdy nemali posudzovať podľa správania predpokladaného umelou inteligenciou výlučne na základe ich profilovania, osobnostných čŕt alebo charakteristík.³⁸ Uvedené sa nevzťahuje na automatizované rizikové analýzy rizika predchádzania podvodov a posudzovania neobvyklých obchodných operácií³⁹ a taktiež na právnické osoby, s výnimkou jednoosobových entít.⁴⁰

Uvedená zakázaná praktika podľa čl. 5, ods. 1, písm. d) AI Aktu môže v zásade naplňať znaky skutkových podstát trestného činu krivého obvinenia podľa § 345 TZ, alebo trestného činu ohovárania podľa § 373 TZ. Vo vzťahu k zneniu tejto zakázanej praktiky je potrebné pri skúmaní trestnosti vyriešiť otázku, či súčasná právna úprava trestného činu krivého obvinenia a trestného činu ohovárania umožňujú postihovať výrok, obsahom ktorého je vyslovenie pravdepodobnosti spáchania trestného činu v budúcnosti, čo však nateraz v právnej doktríne rozpracované nie je. Súčasne je problematické vo vzťahu k subjektívnej stránke týchto trestných činov, že ide o vedomé šírenie nepravdy, čo v kontexte rizikovej predikcie spáchania trestného činu na základe algoritmu je mimoriadne sporné.⁴¹ Ako pravdepodobné sa javí riešenie v podobe subsumpcie takéhoto konania pod „segregačnú“ skutkovú podstatu podľa § 424a TZ, ktorá bola analyzovaná vyššie, vrátane jej trestnoprávnej kvalifikácie v slovenskom právnom poriadku.

K výnimkám použitia zakázaných praktík v súvislosti so systémami umelej inteligencie

Vo všeobecnosti možno uviesť, že AI Akt považuje za výnimku z uvedených zakázaných praktík tie, ktoré sú právom dovolené využívať najmä zložkami presadzujúcimi právo pri plnení ich úloh, ako je tvorba rizikových analýz a predikcie páchania trestnej činnosti. resp. škálovanie osôb podľa všeobecných charakteristík pre účely rôznych identikitov, databáz častí tvare, očí, vlasov, pier a pod.⁴² AI Akt sa neuplatňuje na oblasti týkajúce sa národnej bezpečnosti, a to bez ohľadu na typ subjektu.⁴³ Pod národnou bezpečnosťou sa rozumie záujem na ochrane základných

³⁶ Ibid.

³⁷ Europol, AI and policing: The benefits and challenges of artificial intelligence for law enforcement, s. 15-16. Dostupné na: [AI-and-policing.pdf](#) [navštívené dňa 18.09.2025].

³⁸ Recitál 42 AI Aktu.

³⁹ Recitál 42 AI Aktu.

⁴⁰ Usmernenia Komisie, s. 85.

⁴¹ Napr. R 63/1991.

⁴² Recitál 30 AI Aktu.

⁴³ Rozsudok SD EÚ vo veci C-511/18, C-512/18 a C-520/18 *La Quadrature du Net a i.*, bod 13.

funkcií štátu a základných záujmov spoločnosti, zahŕňa prevenciu a potláčanie aktivít, ktoré môžu vážne destabilizovať základné politické, ústavné, hospodárske alebo sociálne štruktúry krajiny a najmä priamo ohroziť spoločnosť, obyvateľstvo alebo samotný štát, akými sú napríklad teroristické aktivity.⁴⁴ Národná bezpečnosť nezahŕňa napríklad činnosti súvisiace s bezpečnosťou cestnej premávky⁴⁵ alebo organizáciou či výkonom spravodlivosti.⁴⁶

Vo vzťahu k biometrickej identifikácii platí, že táto je možná iba v súlade s čl. 5 ods. 1, písm. h), body i) až iii) AI Aktu, pričom uvedené výnimky netvoría právny základ týchto systémov. Právnym základom je vnútroštátny predpis upravujúci podmienky využívania tohto biometrického systému. Ak takýto predpis neexistuje, je používanie systému na diaľkovú identifikáciu od 1.2.2025 zakázané.⁴⁷ Vo vzťahu k bodu i) a iii) výnimiek je zrejmé, že ide o identifikáciu známej osoby resp. určiteľnej osoby, ktorej totožnosť sa má zistiť⁴⁸ a ktorej údaje sa porovnávajú voči údajom napr. z bezpečnostných kamier s použitím diaľkovej biometrickej identifikácie, s jasným cieľom stotožniť túto osobu, a to i pre potreby vyšetrovania. Súčasne ide o reaktívny prístup na skutočnosť predpokladanú v danom ustanovení. Výnimka formulovaná v bode ii) analyzovaného ustanovenia AI Aktu je vágnejšia, avšak v zmysle výkladu Súdneho dvora musí ísť o konkrétne skutočnosti a nie všeobecnú prevenciu pred určitou hrozbou z dôvodu „zhoršenia bezpečnostnej situácie.“⁴⁹ Uplatnenie uvedeného systému biometrickej identifikácie v reálnom čase navyše okrem výnimiek uvedených v písm. h), obsahuje ďalšie poistky, ktoré by mali brániť jeho zneužitiu vo forme primeranosti nebezpečnej vzniknutej situácie a primeranosti následkov pre dotknutých jednotlivcov.⁵⁰ Súčasne je v zmysle čl. 5 ods. 3 AI Aktu pre použitie tejto výnimky súhlas nezávislého justičného orgánu alebo nezávislého správneho regulačného orgánu a to len po nevyhnutnú dobu, pričom tento súhlas, resp. príkaz je navyše možné vydať len po vykonaní rizikovej analýzy podľa čl. 27, ibaže vec neznesie odklad.⁵¹

Záver

Vzhľadom na tú skutočnosť, že v súčasnej dobe systémy využívajúce umelú inteligenciu nemajú právnu subjektivitu a jej zavedenie do každodenného života je

⁴⁴ Ibid.

⁴⁵ Rozsudok SD EÚ vo veci C-439/19 *Latvijas Republikas Saeima*, bod 68.

⁴⁶ Rozsudok SD EÚ vo veci C-204/21, *Európska komisia proti Poľsku*, bod 319.

⁴⁷ Čl. 5 ods. 5 AI Aktu.

⁴⁸ Čl. 2 ods. 3 AI Aktu

⁴⁹ Rozsudok SD EÚ vo veci C-203/15, *Tele 2 Sverige*, bod 117-119; rozsudok SD EÚ vo veci C-511/18, C-512/18, 520/18 *La Quadrature*, bod 150.

⁵⁰ Čl. 5, ods. 2 AI Aktu.

⁵¹ Čl. 5 ods. 3 AI Aktu.

pomerne komplikované, s viacerými možnými prístupmi,⁵² resp. limitmi⁵³ budeme aj naďalej identifikovať ako možné trestne zodpovedné subjekty fyzické a právnické osoby a systém s umelou inteligenciou bude vnímaný ako nástroj trestného činu.⁵⁴ Vo vzťahu k trestne zodpovednej fyzickej osobe pôjde najmä o administrátora systému, alebo tvorca, resp. testera daného systému s prvkami umelej inteligencie, ktorý vyvíjal alebo sa podieľal na vývoji systému s umelou inteligenciou, ktorá sa dopustila konania majúceho znaky skutkovej podstaty niektorého z hore uvedených trestných činov. Z pohľadu určenia trestnej zodpovednosti fyzickej osoby za konanie systému umelej inteligencie je určujúce, že hore uvedené trestné činy sú úmyselné, čo z pohľadu naplnenia skutkovej podstaty konkrétneho činu vo vzťahu k fyzickej osobe znamená, že takýto páchatel' by musel vedome tvoriť tento počítačový systém za účelom realizácie zakázanej praktiky⁵⁵ alebo my musel byť aspoň uzrozumený s tým, že takto vytvorený systém, alebo takto testovaný systém vykazuje prvky zakázaných praktík, ktoré porušia záujem chránený Trestným zákonom a je s týmto výsledkom uzrozumený.⁵⁶ Na naplnenie trestnosti trestného činu⁵⁷ vo vzťahu k právnickej osobe sa vyžaduje, aby bolo jednak preukázané, že právnická osoba konala prostredníctvom niektorej z osôb podľa § 4 ods. 1 a 2 ZoTZPO a súčasne, že konala prostredníctvom systému s umelou inteligenciou, tak ako predpokladá objektívna stránka skutkovej podstaty trestného činu. Napríklad v súvislosti s trestným činom podvodu, ak by právnická osoba v čase uzatvorenia záväzku konala s tým, že poškodeného uvádza prostredníctvom počítačového systému s umelou inteligenciou do omylu alebo využíva jeho omyl, aby sa tak obohatila na jeho škodu⁵⁸. Vo vzťahu k trestnej zodpovednosti právnických osôb⁵⁹ platí možnosť nepričítania trestného činu v prípade efektívneho compliance programu,⁶⁰ ktorý by spĺňal náležitosti podľa ZoTZPO, ale najmä posúdenie rizík a ich hodnotenie najmä v zmysle. Pre úplnosť uvádzame, že AI Akt však pripúšťa tento druh vyvinenia výlučne

⁵² METEŇKANYČ, M. O.; GYURÁSZ, Z. Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s.76-82. ISBN: 978-80-7160-667-3.

⁵³ VAN DEN HOVEN VAN GENDEREN, R. Legal Personhood in the age of the artificially intelligent robots; In: Research Handbook on the Law of Artificial Intelligence. Cheltenham, UK: Edward Elgar Publishing, 2018, s. 224 a nasl. ISBN: 978-17-8643-904-8.

⁵⁴ § 60 ods. 1 TZ

⁵⁵ § 15 písm. a) TZ - priamy úmysel.

⁵⁶ § 15, písm. b) TZ - nepriamy úmysel.

⁵⁷ Všetky trestné činy, okrem trestného činu krivého obvinenia a trestného činu ohovárania rozoberané vyššie sú pričítateľné v zmysle §3 ZoTZPO aj právnickej osobe (§190, §221, §224. §235, §424a).

⁵⁸ Zakázaná praktika podľa čl. 5 ods. 1 písm. a), písm. b) AI Aktu.

⁵⁹ Právnické osoby, ktoré nespádajú do definície §5 ods. 1 ZoTZPO

⁶⁰ § 4 ods. 3 v spojení s ods. 7 ZoTZPO.

pri manipulatívnych a klamlivých technikách podľa čl. 5 ods.1 písm. a), písm. b) AI Aktu, ak „*narušenie správania obete nie je možné predpokladať, ak narušenie vyplýva z faktorov mimo systému AI, ktoré nie sú pod kontrolou poskytovateľa alebo nasadzujúceho subjektu, konkrétne faktorov, ktoré poskytovateľ systému AI alebo subjekt nasadzujúci systém AI nemôže odôvodnene predvídať, a teda zmiernovať.*“⁶¹ Súčasne sa javí ako zbytočné túto tému rozoberať vo vzťahu k tzv. excesom z výnimiek, ktoré sa z povahy veci budú vzťahovať na subjekty voči ktorým je trestná zodpovednosť vylúčená v zmysle § 5 ods. 1 ZoTZPO. Avšak v prípade právnických osôb, ktoré nespádajú do čl. 5 ods. 1 ZoTZPO a ktoré súčasne vytvorili, nasadili, prevádzkujú alebo poskytujú takýto systém v Európskej únii, naplňajúci znaky zakázanej praktiky, hoci i pre subjekt podľa § 5 ods. 1 ZoTZPO, nemožno vylúčiť trestnú zodpovednosť takejto právnickej osoby.

Zoznam použitej literatúry:

1. DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE, Office of the Prosecutor of the ICC, March 3, 2025, s. 15. Dostupné na: [250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf](#).
2. Europol, AI and policing: The benefits and challenges of artificial intelligence for law enforcement, Dostupné na: [AI-and-policing.pdf](#).
3. KNAP, V.: Teorie práva. 1. vydání, Praha: C.H.Beck. 1995. ISBN 80-7179-028-1.
4. LAZAR, J. a kol.: Občianske právo hmotné- Všeobecná časť. Bratislava: Iura edition, 2006, ISBN 80-8078-084-6.
5. MATYS, K. Trestní zákon-komentář. ORBIS, Praha: ORBIS, 1975, ISBN: 508-21-856.
6. MATYS, K.; Trestný zákon-komentár. Bratislava: OBZOR, 1978.; ISBN: 65-075-78.
7. METEŇKANYČ, M. O., GYURÁSZ, Z. Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022,. ISBN: 978-80-7160-667-3.
8. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).
9. Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 333/2002 Z. z.
10. R 85/1956.
11. R63/1991.

⁶¹ Recitál 29 AI Aktu.

12. Rozsudok Súdneho dvora z 22. júna 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504.
13. Rozsudok Súdneho dvora z 5. júna 2023, C-204/21, EU:C:2023:442 Komisia/Polsko.
14. Rozsudok Súdneho Dvora EÚ vo veci C-203/15, Tele 2 Sverige.
15. Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18 La Quadrature.
16. STRÉMY, T.; KURILOVSKÁ, L. a kol.: Trestný zákon, Komentár, II. Zväzok, 1.vydanie. Praha: Wolters Kluwer ČR, a.s., 2022, ISBN 978-80-7676-430-9.
17. Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu stanovených v nariadení (EÚ) 2024/1689 z 29.7.2025, Dostupné na: [Guidelines on prohibited artificial intelligence practices established by Regulation EU 2024/1689 AI Act Slovak 3mP9dTPmycBiuhqnN6dcPoPxB8 11 8644.PDF](#)
18. VAN DEN HOVEN VAN GENDEREN, R. Legal Personhood in the age of the artificially intelligent robots; In: Research Handbook on the Law of Artificial Intelligence. Cheltenham, UK: Edward Elgar Publishing, 2018, ISBN: 978-17-8643-904-8.
19. Vyhláška ministra zahraničných vecí č. 116/1976 Zb. o Medzinárodnom dohovore o potlačení a trestaní zločinu apartheidu.
20. Vyhláška ministra zahraničných vecí č. 95/1974 Zb. o Medzinárodnom dohovore o odstránení všetkých foriem rasovej diskriminácie.
21. Zákon č. 300/2005 Z. z. Trestný zákon.
22. Zákon č. 91/2016 Z. z o trestnej zodpovednosti právnických osôb.

Kontaktné údaje

doc. JUDr. Marek Kordík, PhD. LL.M.

marek.kordik@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

Katedra trestného práva, kriminológie a kriminalistiky

Mgr. Petra Dražová, PhD.

petra.drazova@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

Ústav práva informačných technológií a práva duševného vlastníctva

PROBLEMATIKA VZDIALENÉHO VODIČA Z POHLĎADU TRESTNÉHO ČINU NEPOSKYTNUTIA POMOCI PODĽA §178 TZ SLOVENSKEJ REPUBLIKY¹

THE ISSUE OF REMOTE DRIVER FROM THE POINT OF VIEW OF CRIMINAL OFFENCE OF FAILURE TO RENDER ASSISTANCE ACCORDING TO §178 OF THE CRIMINAL CODE OF SLOVAK REPUBLIC

Zoltán Gyurász²

Abstrakt: Článok sa zaoberá komplexnou právnou analýzou nového fenoménu vzdialeného vodiča a jeho prepojením s trestným činom neposkytnutia pomoci podľa § 178 slovenského trestného zákona. Hoci povinnosť poskytnúť pomoc bola dlho chápaná v kontexte fyzicky prítomných vodičov na mieste dopravnej nehody, nárast diaľkovo ovládanéj mobility radikálne spochybňuje túto paradigmu. Osobitná pozornosť sa venuje scenárom, v ktorých sa prevádzkovateľ diaľkovo ovládaného motorového vozidla zapletie do nehody, ale zostáva priestorovo vzdialený od miesta nebezpečenstva, čo vyvoláva zložité otázky o tom, či takáto osoba má objektívnu a vynútiteľnú možnosť poskytnúť pomoc zraneným osobám. Umiestnením analýzy do širšieho rámca medzinárodných dohovorov, porovnávacích zahraničných predpisov a absencie slovenskej judikatúry článok poukazuje na medzery v doktríne aj na riziko normatívnej neistoty. Štúdia skúma, do akej miery môže byť diaľkový vodič trestne zodpovedný za opomenutie – či už tým, že nezahájil núdzové protokoly, neoznámil záchranné služby alebo neaktivoval technické bezpečnostné mechanizmy, ktoré mohli zachrániť život alebo znížiť škody.

Kľúčové slová: Právo informačných technológií, Slovenské právo, Trestný zákon, Vzdialený vodič

Abstract: The article undertakes a comprehensive legal analysis of the emerging phenomenon of the remote driver and its intersection with the

¹ Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 17R05-04-V01-00002 (Competence Center for Regulation of Cybersecurity, Privacy Protection and Cybercrime).

² Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University Bratislava, Bratislava, Slovakia

offence of failure to render assistance under Section 178 of the Slovak Criminal Code. While the duty to provide aid has long been understood in the context of physically present drivers at the scene of a traffic accident, the rise of teleoperated mobility radically challenges this paradigm. Particular attention is given to scenarios in which the operator of a remotely controlled motor vehicle is involved in an accident but remains spatially distant from the site of danger, raising complex questions about whether such an individual has an objective and enforceable opportunity to provide assistance to injured persons. By situating the analysis within the broader framework of international conventions, comparative foreign regulation, and the absence of Slovak jurisprudence, the article highlights both doctrinal gaps and the risk of normative uncertainty. The study explores the extent to which a remote driver may be held criminally liable for omission — whether by failing to initiate emergency protocols, notify rescue services, or activate technical safety mechanisms — that could have preserved life or reduced harm.

Key words: Information technology law, Slovak law, Criminal law, Remote driver

Intraduction

The rapid technological development of automated and semi-automated driving systems has introduced new paradigms into both transport practice and legal scholarship.³ Even though, most of the spotlight is taken by the topic of fully automated and the possibility of autonomous vehicles⁴ a particularly noteworthy innovation is the concept of the remote driver.⁵ By definition a remote driver is an individual who does not physically occupy the vehicle but rather controls it or intervenes in its operation from a distance through teleoperation technologies.

While the model of remote driver promises efficiency and safety benefits, it simultaneously raises profound questions for many domains of law even for criminal law. Among these issues is the question of whether, and under what circumstances,

³ See. Sever, Tina - Contissa, Giuseppe. Automated driving regulations – where are we now? *Transportation Research Interdisciplinary Perspectives*. Volume 24. 2024. ISSN 2590-1982. pp 2- 19. Or We published a comprehensive monography about issues of legal issues of automated vehicles in Andraško, Jozef a kol. *Právne aspekty automatizovaných vozidiel*. 2023. 978-80-8232-038-4. p 332.

⁴ Carolina, Diaz-Piedra - Belen Liedo, Miguel Núñez de Prado-Gordillo, M Jesus Caurcel, Leandro L. Di Stasi. Ethical and legal challenges of automated driving: The prioritization of socio-political values. *Transportation Research Procedia*. Volume 72. 2023. ISSN 2352-1465. pp. 2449-2456.

⁵ See. Hoffmann, Thomas - Prause, Gunnar. On the Legal and Economic Implications of Tele-Driving. *Machines*. 2023. pp 9-11.

a remote driver may be held criminally liable for the failure to render assistance under § 178 of the Slovak Republic's Criminal Code.

The provision of § 178 of the Slovak Republic's Criminal Code is grounded in the overarching principle of solidarity and the protection of human life and health, criminalizes the omission of assistance in situations where intervention is both necessary and feasible without causing significant risk to the individual providing aid.⁶ The prevailing tradition of §178 predicated on the assumption of a physical presence at or in the immediate closeness of the scene of an accident. However, in the context of remote operation, the spatial and situational context undergoes a fundamental transformation. The remote driver is not physically present at the accident site, may lack direct sensory perception of the victims, and may be constrained by technological limitations in exercising the expected duty of assistance. These altered conditions present challenges to the traditional doctrinal elements of the offense, including the immediacy of the danger, the feasibility of intervention, and the threshold of personal risk. From a normative perspective, the central issue is whether the existing interpretation of §178 can be sufficiently extended to encompass remote drivers, or whether new statutory formulations are required.

This tension underscores the broader challenge of adapting criminal law to the realities of digital and automated mobility. The discourse surrounding remote drivers and § 178 exemplifies the potential problems in the prevailing legal framework. Moreover, it prompts a reevaluation of how conventional notions such as omission, proximity, and assistance ought to adapt in response to technological advancements.⁷ The subsequent analysis will therefore examine the doctrinal contours of §178, assess its applicability to remote drivers, and propose interpretative and legislative pathways for addressing this emerging legal issue.

Criminal offence of failure to render assistance according to §178 of the criminal code of Slovak republic

According to §178 of the criminal code of Slovak republic, in the event that a driver involved in a traffic accident and neglects to provide necessary assistance to an individual who has suffered injury, even though such assistance is not hazardous to

⁶ See. Burda, Eduard - Čentěš, Jozef a kol. Trestný zákon. Osobitná časť. Komentár. II. diel. 1. vydanie. Praha: C. H. Beck, 2011, pp. 1608.

⁷ Ibid. For the questions of conventional notions.

the driver or others, the driver shall be sentenced to up to of three years of imprisonment.⁸

At its core, § 178 criminalizes the omission of assistance where:

- an individual finds another in imminent danger to life or serious bodily integrity,
- such assistance can be rendered without exposing the potential helper to serious danger, and
- the omission is not otherwise justified.

The challenge in the light of the thesis of the article lies in transposing these elements to the context of a remote driver who is spatially absent from the accident site yet legally deemed a driver.

Driver in the light of remote-control

The Convention on Road Traffic, signed on September 19, 1949, in Geneva (hereinafter referred to as the "Geneva Convention")⁹ and the Convention on Road Traffic, signed on November 8, 1968, in Vienna (hereinafter referred to as the "Vienna Convention")¹⁰ form the basis of road traffic legislation for many national legal systems around the world. The establishment of these legal frameworks is predicated on the premise of enhancing the harmonization of road traffic regulations, thereby promoting enhanced safety on global roadways and facilitating the recognition of foreign vehicles and drivers within the international community. The analysis of these international treaties reveals that they regulate the obligations of drivers to comply with road traffic rules, thereby improving road safety.¹¹

As automated driving systems and remote controls are progressively integrated into vehicles, it becomes imperative to address legal concerns surrounding the Geneva Convention and the Vienna Convention. These legal issues include the question of whether the use of such systems is in accordance with the fundamental requirements

⁸ (Originally in Slovak) „Vodič, ktorý po dopravnej nehode, na ktorej mal účasť, neposkytne osobe, ktorá pri nehode utrpela ujmu na zdraví, potrebnú pomoc, hoci tak môže urobiť bez nebezpečenstva pre seba alebo iného, potrestá sa odňatím slobody až na tri roky.“

⁹Geneva Convention. Available at: <https://www.worlddriversassociation.com/pdf/CONVENTION%20ON%20ROAD%20TRAFFIC1949.pdf>.

¹⁰Vienna Convention. Available at: https://treaties.un.org/doc/Treaties/1977/05/19770524%2000-13%20AM/Ch_XI_B_19.pdf.

¹¹ Mörtl, Peter. 2020. Human-Systems Integration for Driving Automation Systems: Holistic approach for driver role integration and automation allocation for European mobility needs, in "International Conference on Human-Computer Interaction". In: Krömker, H. (Ed.). Springer, Cham, pp. 78–88.

stipulated in these international treaties, particularly the requirement that the driver must maintain control of the vehicle.¹²

The term driver is defined in both the Geneva Convention¹³ and the Vienna Convention¹⁴, which also delineate the requirements for drivers and vehicle operation, as well as their obligations in road traffic. The interpretation of the term driver, the requirements for drivers and related obligations will be important for assessing whether the introduction of fully automated vehicles and remote drivers where a system performs certain driving tasks instead of the driver, is not contrary to the Geneva Convention and the Vienna Convention.

Both the Geneva Convention and the Vienna Convention contain provisions requiring drivers to be in control of their vehicles. According to Article 8(5) of the Geneva Convention, drivers are obligated to maintain control of their vehicles or animals at all times. Similarly, Article 8(5) of the Vienna Convention stipulates that drivers must be capable of controlling their vehicles or animals at all times. In regard to the driver's responsibility to maintain control of the vehicle, as outlined in Article 10 of the Geneva Convention, the driver of a vehicle is obligated to "exercise constant control over the vehicle's speed and operate it in a manner that is both appropriate and cautious." A comparable stipulation is delineated in Article 13(1) of the Vienna Convention.

With the advent of new technologies, amendments were required for the conventions. The amendments and supplements made in 2022 to the Vienna Convention permit, firstly, the utilization of vehicles equipped with automated control systems that execute certain or all driving operations in line of the operator. However, these amendments do not stipulate any regulations concerning the operator's engagement in activities other than driving while the system is engaged in its driving functions. However, the introduced provisions do not address matters pertaining to remote drivers.

Driver in the light of remote-control – Germany

In July of 2025, the German Federal Ministry of Transport promulgated the *Straßenverkehr-Fernlenk-Verordnung* coming into force on 1 December 2025, which for the first time establishes a legal framework for the testing and limited operation

¹² Rodríguez-Alcázar, J., Bermejo-Luque, L., Molina-Pérez, A., 2021. Do automated vehicles face moral dilemmas? A plea for a political approach. *Philosophy & Technology*, 34, 811–832.

¹³ According to the provisions stipulated in the Geneva Convention art 8 sec 1. the term driver is defined as "any person who drives a vehicle, including bicycles, or leads a pack, draft, or riding animal or herd or flock on a road, or who actually physically controls them."

¹⁴ According to the Vienna Convention, Art 8 sec 4 the term driver is defined as "any person who drives a motor vehicle or other vehicle (including a bicycle) or who drives cattle individually or in herds or flocks or a beast of burden, draft animal or riding animal on a road."

of remotely controlled vehicles on public roads.¹⁵ Under this new ordinance, Germany permits a five-year trial phase intended to balance innovation with safety and legal clarity.

The regulation sets detailed requirements for the control center infrastructure, reflecting that the teleoperator must receive precise real-time data and possess interfaces equivalent in functionality to in-vehicle controls. The draft also prescribes obligations on the registered keeper for maintenance, system integrity checks, safety fallback modes, and detection of operator unavailability. The goal of the regulation is twofold. To enable innovation in mobility while at the same time preserving safety, responsibility, and legal clarity. Germany frames teleoperated driving as a bridge technology between traditional in-vehicle driving and full autonomous driving especially Level 4 and higher, allowing remote takeover or control especially in complex traffic situations or during transitions.¹⁶ The regulation emphasizes redundant communication channels, fallback safe stop functionality, strict control of latency, and demands for operator proficiency and technical infrastructure to ensure that remote driving does not produce unacceptable risks.¹⁷ The German case offers a rich comparative template. It reveals how a legal system might map classical duties of conduct onto a technologically displaced agent and provides concrete regulatory mechanisms for balancing safety, liability, and innovation.

In the Slovak context, the German model invites careful reflection on how § 178 might or might not be interpreted to encompass remote operators, and at what stage legislative reform might become necessary.

Criminal offence of failure to render assistance according to §178 of the criminal code of Slovak republic in light of remote drivers

The decision to treat the teleoperator as the *driver* for all purposes of traffic law directly addresses the definitional ambiguity that could otherwise obstruct liability analysis.

Another gap concerns the immediacy of danger as the remote operator's perception is mediated by sensors and data feeds. Delays, blind spots, or transmission failures

¹⁵Verordnung über Ausnahmen von straßenverkehrsrechtlichen Vorschriften für ferngelenkte Kraftfahrzeuge (Straßenverkehr-Fernlenk-Verordnung — StVFernLV). Available at: <https://www.recht.bund.de/bgbl/1/2025/176/VO.html>

¹⁶ For the issue of levels of automatization see. Sever, Tina – Contissa, Giuseppe. Automated driving regulations – where are we now? Transportation Research Interdisciplinary Perspectives. Volume 24. 2024. ISSN 2590-1982. pp 3.

¹⁷ Krempf, Stefan. Federal government creates legal basis for the use of remote-controlled cars. 2025. Available at: <https://www.heise.de/en/news/Federal-government-creates-legal-basis-for-the-use-of-remote-controlled-cars-10504883.html>

may prevent the operator from acquiring the knowledge necessary to trigger the duty under § 178.¹⁸

At present, neither Slovak jurisprudence nor case-law provides guidance on the applicability of § 178 of the Criminal Code to the figure of the remote driver. The provision, which criminalizes the failure to render assistance, has historically been interpreted with reference to conventional road traffic accidents involving physically present drivers and bystanders. Judicial decisions and scholarly commentary consistently presuppose a situational framework in which the individual confronted with another's imminent danger is physically at or near the scene, capable of direct intervention through first aid or immediate protective acts. The emergence of remote driving, by contrast, creates a novel constellation: the operator is legally responsible for vehicle control but spatially absent from the site of potential harm, raising profound questions as to whether and how the statutory duty of assistance may extend to such actors.

This question engenders legal uncertainty for both operators and victims, thereby undermining the normative clarity of criminal law. Until the field of jurisprudence engages directly with these issues, the interpretative gap must be addressed through proactive judicial reasoning or, more reliably, through legislative clarification.¹⁹

Conclusion

The remote driver represents a noteworthy intersection of technological innovation and criminal law in the field of mobility. While the Slovak Republic's current legal framework, particularly § 178 of the Criminal Code, was designed to address situations involving physically present drivers, the emergence of teleoperation technologies introduces a new and complex set of responsibilities. Remote drivers occupy a hybrid role: they are legally treated as drivers but are physically absent from the site of potential danger. This creates a significant doctrinal tension, as the traditional assumptions underlying the duty to render assistance—physical proximity, direct sensory perception, and immediate ability to intervene—are fundamentally transformed.

A comparative analysis of regulatory frameworks reveals that the German *Straßenverkehr-Fernlenk-Verordnung* marks a notable development in which regulatory systems are beginning to acknowledge and address the distinct risks associated with teleoperated driving. By establishing strict technical requirements,

¹⁸ See. Collingwood, Lisa,. Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law*, 2017. pp, 32–45.

¹⁹ See. Goodall, Noah. Machine ethics and automated vehicles, in "Road vehicle automation, lecture notes in mobility". In: Meyer, G., & Beiker, S. (Eds.). Springer International Publishing Switzerland. 2014. pp. 93–102.

safety redundancies, and legal obligations for teleoperators, Germany positions remote driving as a transitional technology that bridges conventional driving and fully autonomous systems. This development establishes a valuable model for Slovakia, but also reveals the limits of criminal liability when applied to actors who are displaced from the physical scene of the accident. If § 178 is not clearly adapted by statutory means, the section risks being stretched beyond its doctrinal coherence or becoming underinclusive in the face of novel harms.

The challenge, therefore, is twofold. On the one hand, the law must maintain its protective function and ensure that individuals in life-threatening situations receive assistance, regardless of the driver's remote operation status. Conversely, the principle of culpability dictates that liability should not be imposed in cases where the remote operator lacks the factual or technical capacity to intervene effectively. In this regard, the jurisprudential vacuum in Slovakia is unsustainable. Without judicial engagement or legislative reform, legal certainty for both operators and victims remains compromised.

The emergence of remote driving is indicative of a broader shift in criminal law towards technologically mediated responsibilities. It prompts us to reexamine fundamental legal concepts such as omission, proximity, and the feasibility of assistance. We must consider whether these notions can be meaningfully reinterpreted or if new legal categories are necessary. The future of § 178 may depend on this choice. In order to maintain its responsiveness to technological change while safeguarding its normative foundations, Slovak law must move beyond the assumption of physical presence and articulate a coherent framework for duties of assistance in the digital age. The debate initiated by remote drivers extends far beyond traffic law, touching upon the adaptability of criminal law itself in the face of disruptive innovation.

Zoznam použitej literatúry

1. Andraško, Jozef a kol. Právne aspekty automatizovaných vozidiel. 2023. pp 332.
2. Burda, Eduard - Čentěš, Jozef .a kol. Trestný zákon. Osobitná časť. Komentár. II. diel. 1. vydanie. Praha: C. H. Beck, 2011, pp. 1608.
3. Carolina Diaz-Piedra, Belen Liedo, Miguel Núñez de Prado-Gordillo, M Jesus Caurcel, Leandro L. Di Stasi. Ethical and legal challenges of automated driving: The prioritization of socio-political values. Transportation Research Procedia. Volume 72. 2023. ISSN 2352-1465. pp. 2449-2456.
4. Collingwood, Lisa,. Privacy implications and liability issues of autonomous vehicles. Information & Communications Technology Law, 2017. pp, 32–45.

5. Geneva Convention. Available at:
<https://www.worlddriversassociation.com/pdf/CONVENTION%20ON%20ROAD%20TRAFFIC1949.pdf>.
6. Goodall, Noah. Machine ethics and automated vehicles, in "Road vehicle automation, lecture notes in mobility". In: Meyer, G., & Beiker, S. (Eds.). Springer International Publishing Switzerland, . 2014. pp. 93–102.
7. Hoffmann, Thomas - Prause, Gunnar. On the Legal and Economic Implications of Tele-Driving. Machines. 2023. pp 9-11.
8. Krempf, Stefan. Federal government creates legal basis for the use of remote-controlled cars. 2025. Available at: <https://www.heise.de/en/news/Federal-government-creates-legal-basis-for-the-use-of-remote-controlled-cars-10504883.html>
9. Mörtl, Peter. 2020. Human-Systems Integration for Driving Automation Systems: Holistic approach for driver role integration and automation allocation for European mobility needs, in "International Conference on Human-Computer Interaction". In: Krömker, H. (Ed.). Springer, Cham, pp. 78–88.
10. Rodríguez-Alcázar, J., Bermejo-Luque, L., Molina-Pérez, A. Do automated vehicles face moral dilemmas? A plea for a political approach. Philosophy & Technology. 2021. 811–832.
11. Sever, Tina - Contissa, Giuseppe. Automated driving regulations – where are we now? Transportation Research Interdisciplinary Perspectives. Volume 24. 2024. ISSN 2590-1982. pp 2- 19.
12. Verordnung über Ausnahmen von straßenverkehrsrechtlichen Vorschriften für ferngelenkte Kraftfahrzeuge (Straßenverkehr-Fernlenk-Verordnung — StVFernLV). Available at: <https://www.recht.bund.de/bgb1/1/2025/176/VO.html>
13. Vienna Convention. Available at:
https://treaties.un.org/doc/Treaties/1977/05/19770524%2000-13%20AM/Ch_XI_B_19.pdf.

Kontaktné údaje

JUDr. Zoltán Gyurász, PhD.

zoltan.gyurasz@flaw.uniba.sk

Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University Bratislava, Bratislava, Slovakia

IMPLEMENTAČNÉ VÝZVY CYBER RESILIENCE ACT: 5 DIMENZIÍ IMPLEMENTÁCIE

APPLICATION CHALLENGES OF THE CYBER RESILIENCE ACT: FIVE DIMENSIONS OF IMPLEMENTATION

Miroslav Sorkovský¹

Abstrakt: Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 o kybernetickej odolnosti predstavuje nový rámec kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, ktorý zásadným spôsobom mení požiadavky na kybernetickú odolnosť produktov s digitálnymi prvkami v Európskej únii. Prijatie aktu o kybernetickej odolnosti reflektuje rastúce kybernetické hrozby a dlhodobé zlyhanie trhu zabezpečiť primeranú úroveň ochrany. Implementácia však prináša viacero praktických aplikačných výziev, ktoré presahujú čisto právnu alebo technickú rovinu. Predkladaný článok identifikuje päť vybraných implementačných výziev: právne a regulačné, technické, ekonomické a trhové, organizačné a praktické, ako aj akademické a etické, ktoré sa objavujú pri implementácii nariadenia. Cieľom je prispieť k lepšiemu porozumeniu regulačného rámca a upozorniť regulované subjekty a ďalších adresátov nariadenia na zásadný vplyv, ktorý bude mať nariadenie o kybernetickej odolnosti na ich procesy, technológie, ekonomické modely i organizačné štruktúry. Článok zdôrazňuje, že úspešná implementácia nebude len otázkou splnenia formálnych povinností, ale vyžaduje si strategickú transformáciu a dlhodobý prístup ku kybernetickej odolnosti.

Kľúčové slová: Akt o kybernetickej odolnosti, kybernetická bezpečnosť, produkt s digitálnymi prvkami,

Abstract: Regulation (EU) 2024/2847 of the European Parliament and of the Council on cyber resilience establishes a new cybersecurity framework for products with digital elements, fundamentally reshaping the requirements concerning their cyber resilience in the European Union. The adoption of the Cyber Resilience Act reflects both the increasing scale of cyber threats and the persistent market failure to ensure an adequate level of protection. Its implementation, however, raises a number of practical challenges that transcend purely legal or technical considerations. This article identifies five

¹ Právnická fakulta Univerzity Komenského v Bratislave

selected dimensions of implementation challenges—legal and regulatory, technical, economic and market-related, organizational and practical, as well as academic and ethical—that arise in the application of the Regulation. The objective is to contribute to a deeper understanding of the regulatory framework and to alert regulated entities and other addressees of the Regulation to the significant impact that the Cyber Resilience Act will have on their processes, technologies, economic models, and organizational structures. The article emphasizes that successful implementation will not merely be a matter of formal compliance, but will require strategic transformation and a long-term approach to cyber resilience.

Key words: Cyber Resilience Act (CRA); cybersecurity; product with digital elements.

Úvod

Dňa 23. októbra 2024 prijal Európsky parlament a Rada nariadenie číslo 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (Akt o kybernetickej odolnosti, Cyber Resilience Act, ďalej v texte len CRA), ktorý sa bude v plnom rozsahu uplatňovať od 11. decembra 2027, s dvoma výnimkami, a to notifikácie orgánov posudzovania zhody (kapitola IV CRA) a ohlasovacej povinnosti výrobcov (čl. 14 CRA). Tieto sa budú uplatňovať už od júna, respektíve septembra 2026². Cieľom CRA je zabezpečiť vysokú úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami a ich integrovaných riešení spracovania údajov na diaľku³. Zároveň s uvedeným je cieľom odstrániť prekážky voľného pohybu produktov s digitálnymi prvkami⁴.

CRA stanovuje pravidlá sprístupňovania produktov s digitálnymi prvkami na trhu s cieľom zaistiť ich kybernetickú bezpečnosť⁵, stanovuje základné požiadavky kybernetickej bezpečnosti na návrh, vývoj a výrobu produktov s digitálnymi prvkami a povinnosť hospodárskych subjektov v súvislosti s týmito produktmi, pokiaľ ide o kybernetickú bezpečnosť⁶. Zároveň stanovuje základné požiadavky kybernetickej bezpečnosti na procesy riešenia zraniteľnosti zavedené výrobcami s cieľom zaistiť kybernetickú bezpečnosť produktov s digitálnymi prvkami počas predpokladného

² čl. 71. ods. 2 Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)

³ recitál 11 CRA

⁴ recitál 14 CRA

⁵ čl. 1 písm a) CRA

⁶ čl. 1 písm. b) CRA

obdobia použitia produktov a povinnosti hospodárskych subjektov v súvislosti s týmto procesmi⁷ a pravidlá dohľadu nad trhom, vrátane monitorovania a presadzovania pravidiel na požiadaviek⁸.

V CRA je definovaný rozsah pôsobnosti tak pozitívnym, ako aj negatívnym vymedzením. Pozitívne vymedzenie je ustanovené v čl. 2 ods. 1, pričom podľa tohto vymedzenia sa CRA uplatňuje na produkty s digitálnymi prvkami sprístupnenými na trhu, ktorých zamýšľaný účel alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti⁹. Negatívne vymedzenie je definované v čl. 2 ods. 2-7, pričom CRA sa napríklad neuplatňuje na niektoré produkty s digitálnymi prvkami, ktoré sú regulované sektorovo¹⁰.

Predkladaný článok využíva kvalitatívnu právnu a interdisciplinárnu analýzu, ktorá kombinuje: normatívnu právnu analýzu – skúmanie textu CRA v spojení s relevantnými právnymi aktmi (NIS²¹¹, AI Act¹², CSA¹³) a súvisiacimi dokumentmi Európskej komisie (Impact Assessment Reports¹⁴). Komparatívny prístup – identifikácia vzájomného pôsobenia CRA so sektorovými reguláciami, pričom sa hodnotí riziko duplicít, právnej neistoty a regulačného „prekrytia“. Doktrínálnu a literárnu analýzu – aktuálny stav vedeckých štúdií a článkov, ktoré hodnotia CRA v kontexte európskeho práva kybernetickej bezpečnosti. Koncepčnú reflexiu – posúdenie CRA ako nástroja na dosiahnutie vyššej úrovne kybernetickej bezpečnosti EÚ a implementačné výzvy spojené s jeho aplikáciou. Cieľom využitej metodológie je poskytnúť právno-teoretickú a prakticko-aplikačnú reflexiu implementačných

⁷ Čl 1 písm c) CRA

⁸ Čl 1 písm d) CRA

⁹ Čl 2 ods. 1 CRA

¹⁰ Príkladom sú produkty s digitálnymi prvkami upravenými podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro, atď.

¹¹ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

¹² Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

¹³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).

¹⁴ Cyber Resilience Act - Impact assessment. Dostupný na <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment>

výziev. Uvedené má abíciu odzrkadliť sa v cieľoch predkladaného článku, ktorými sú poskytnutie systematického prehľadu implementačných výziev CRA a prispieť k lepšiemu porozumeniu toho, aký zásadný vplyv bude mať táto regulácia na prax regulovaných subjektov. Zameriava sa na firmy, startupy, malé a stredné podniky, ale aj na nadnárodné korporácie, ktorým má uľahčiť orientáciu v nových povinnostiach a odhaliť praktické dôsledky pre ich interné procesy, technologické nastavenia, compliance mechanizmy a obchodné modely. budovaním kultúry súladu. Článok má zároveň ambíciu upozorniť aj ďalších adresátov nariadenia, vrátane orgánov dohľadu, regulačných autorít a akademickej obce, na interdisciplinárny charakter CRA a potrebu úzkej spolupráce medzi právnou, technickou a ekonomickou sférou.

Napriek tomu, že CRA bol schválený v októbri 2024 a plne vstúpi do účinnosti až v decembri 2027, analýzou CRA sa už zaoberali viacerí autori, pričom ich práce sú východiskom pre spracovanie tohto článku: CHIARA (2022)¹⁵, (2024)¹⁶ a (2025)¹⁷, BURRI a ZIHLMANN (2023)¹⁸, ECKHARDT a KOTOVSKAIA (2023)¹⁹, RUOHONEN a TIMMERS (2024)²⁰, SCHMITTNER a kol (2024)²¹, BRIGHI a ADINOLFI (2025)²²,

¹⁵ CHIARA, Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. In: *International Cybersecurity Law Review*, Roč. 3, (2022), s. 1 – 18. DOI: <https://doi.org/10.1365/s43439-022-00067-6>.

¹⁶ CHIARA, Pier Giorgio: Towards a right to cybersecurity in EU law? The challenges ahead. In: *Computer Law & Security Review*, Vol. 53, (2024), s. 1-9, 105961. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.105961>

¹⁷ CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? In: *European Journal of Risk Regulation*, Roč. 16, č. 2 (2025), s. 469 – 483. doi:10.1017/err.2025.9

¹⁸ BURRI, Mira – ZIHLMANN, Zaira: The EU Cyber Resilience Act – An Appraisal and Contextualization. In: *EuZ – Zeitschrift für Europarecht*, (2023), DOI: <https://doi.org/10.36862/eiz-euz015>.

¹⁹ ECKHARDT, Philipp – KOTOVSKAIA, Anastasia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. In: *International Cybersecurity Law Review*, Vol. 4, 2023, s. 147 – 164. Dostupné na <https://doi.org/10.1365/s43439-023-00084>

²⁰ RUOHONEN Jukka - TIMMERS Paul: Vulnerability Coordination Under the Cyber Resilience Act, In: *Computer Science*, 2024, 14 s. Dostupné na <https://doi.org/10.48550/arXiv.2412.06261>

²¹ SCHMITTNER, Christoph – VELEDAR, Orges – FASCHANG, Thomas – MACHER, Georg – BRENNER, Egon: Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. In: YILMAZ, Murat – CLARKE, Paul – RIEL, Andreas – MESSNARZ, Richard – GREINER, Christian – PEISL, Thomas (eds.): *Systems, Software and Services Process Improvement. EuroSPI 2024. Communications in Computer and Information Science*, vol. 2179. Cham: Springer, 2024, s. 390 – 404 DOI: https://doi.org/10.1007/978-3-031-71139-8_26.

²² BRIGHI, Raffaella – ADINOLFI, Giovanna: EU Cybersecurity Policies in Cyber-Physical Ecosystems: Challenges and Perspectives. In: *European Journal of Risk Regulation*, Roč. 16, č. 2 (2025), s. 466 – 478. Dostupné na doi:10.1017/err.2025.10026

NYGARD, a KATSIKAS (2025)²³, O GRADY (2025)²⁴, RAJAMÄKI a kol. (2025)²⁵, RAMPÁŠEK a kol. (2025)²⁶, SHAABAN a SCHMITTNER (2025)²⁷, TEODORESCU a kol. (2025)²⁸.

Prvá dimenzia - právne a regulačné výzvy

Kľúčovým pojmom CRA je “produkt s digitálnymi prvkami”, ktorý je definovaný ako „softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne”²⁹. CRA zároveň prináša kategorizáciu produktov s digitálnymi prvkami podľa tzv. risk based approach, teda prístupu k ich kategorizácii podľa ich kybernetickobezpečnostnej rizikovosti. CRA definuje kybernetickobezpečnostné riziko ako “potenciál straty alebo narušenia v dôsledku incidentu a má byť vyjadrené ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu incidentu”³⁰. V súvislosti s uvedeným rozoznáva CRA produkty s digitálnymi prvkami bez rizika, dôležité produkty s digitálnymi prvkami, uvedené v prílohe III, ktoré sú ďalej klasifikované do tried I a II a kritické produkty, ktoré sú uvedené v prílohe IV CRA. Viac k risk based approach kategorizácii produktov s digitálnymi prvkami viď

²³ NYGARD, Arne Roar – KATSIKAS, Sokratis: Digital supply chain security for power sector operators in the light of the new EU directives and regulation. In: Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics, (2025), s. 70 – 80.

²⁴ O'GRADY Stephan: The Cyber Resilience Act: A Five Alarm Fire. Portland: Newstex 2025. Dostupné na <https://www.proquest.com/blogs-podcasts-websites/cyber-resilience-act-five-alarm-fire/docview/3236971601/se-2>

²⁵ RAJAMÄKI, Jyri – HÄMÄLÄINEN, Timo – RIIHIJÄRVI, Janne – KANGAS, Olli-Pekka – LAJUNEN, Antti – KERTTULA, Olli: Navigating the Cyber Resilience Act: Implications for the Dynamo Horizon Project. In: Proceedings of the European Conference on Cyber Warfare and Security, (2025), s. 891 – 902. Dostupné na <https://www.proquest.com/conference-papers-proceedings/navigating-cyber-resilience-act-implications/docview/3244083252/se-2>

²⁶ RAMPÁŠEK, Michal – MESARČÍK, Matúš – ANDRAŠKO, Jozef: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: Computer Law & Security Review, Vol. 56, (2025), 19 s., 106093. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.106093>.

²⁷ SHAABAN, Abdelkader Magdy – SCHMITTNER, Christoph: A ThreatGet-Based Framework for Aligning System Security with the Cyber Resilience Act. In: TÖRNGREN, Martin – BÜRKNER, Paul – et al. (eds.): Computer Safety, Reliability, and Security: SAFECOMP Workshops 2025. Cham: Springer, 2025, s. 101 – 114. Dostupné na <https://doi.org/10.1007/978-3-032-02018-5>

²⁸ TEODORESCU, Cosmin A. – VASILE, Ionut – STANCIU, Oana: The Evolution of Mobile Cybersecurity Regulations in the European Union. In: Management & Marketing. Challenges for the Knowledge Society, Roč. 20, č. 1 (2025), s. 52 – 63. Dostupné na doi: <https://doi.org/10.2478/mmcks-2025-0004>

²⁹ čl. 3 ods. 1 CRA

³⁰ čl. 3 ods 37 CRA

napr. pojednanie autora CHIARA (2025)³¹ alebo RAMPÁŠEK a kol. (2025)³². Aplikačnou výzvou a zároveň problematickou oblasťou sa stáva všeobecná a široká definícia pojmu produktu s digitálnymi prvkami a právna neistota s tým súvisiaca pre regulované subjekty. Uvedená kritika nie je v teoretickej praxi nová a bola vznesená a rozpracovaná napr. autormi BURRI a ZIHLMANN (2023)³³ a RAJAMÄKI a kol. (2025)³⁴. Analogicky k uvedenému sa javí ako veľká výzva a riziko interpretačných nejasností využívanie všeobecných a široko interpretovateľných pojmov (založených napr. na všeobecnom pojme primeranosti) ako sú napríklad uvedené v čl. 5, ods 1, čl. 8 ods. 1, čl. 13 ods. 7, 8, 14, čl. 14 ods. 8, 15. ods. 5, čl. 27 ods. písm. b), atď. Až prax a predovšetkým rozhodnutia Súdneho dvora EÚ bližšie zadefinuje široko interpretovateľné pojmy a ustanovenia.

Osobitnou právnou a regulačnou výzvou je skutočnosť, že CRA bude dopĺňaná a spresňovaná delegovanými a vykonávacími aktami Európskej komisie. Týmto legislatívnym postupom sa základné nariadenie stáva iba „kostrou“, ktorej obsah a praktická uplatniteľnosť budú determinované až ďalšími predpismi. Z pohľadu právnej istoty to predstavuje vážnu výzvu.

CRA ako právny rámec zavádza horizontálne požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a zaraďuje sa do existujúceho právneho rámca EÚ, ktorý nastavuje pravidlá a reguluje kybernetickú bezpečnosť. V tejto súvislosti bude v tomto článku predložená ako právna a regulačná výzva synergia CRA so smernicou NIS 2, nariadením CSA a AI Actom.

Vzťah medzi CRA a smernicou NIS 2 je jedným z najvýraznejších príkladov možného „prekrytia“ regulačných rámcov. CRA sa zameriava na bezpečnostné požiadavky priamo spojené s produktmi s digitálnymi prvkami počas celého ich životného cyklu, zatiaľ čo NIS 2 kladie dôraz na organizačné a procesné opatrenia dôležitých a kľúčových subjektov. V recitáloch 11 a 12, CRA poskytuje výklad pomyslenej hranice v regulácii a vzťahu medzi CRA a NIS 2, avšak tento rozdiel v teoretickej rovine pôsobnosti sa v praxi môže stierať. Povinnosti výrobcov v oblasti riadenia zraniteľností a ich oznamovania podľa CRA môžu byť obsahovo totožné s

³¹ CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? In: *European Journal of Risk Regulation*, Roč. 16, č. 2 (2025), s. 473 – 474 Dostupné na doi:10.1017/err.2025.9

³² RAMPÁŠEK, Michal – MESARČÍK, Matúš – ANDRAŠKO, Jozef: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: *Computer Law & Security Review*, Vol. 56, (2025), s 6, 106093. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.106093>.

³³ BURRI, Mira – ZIHLMANN, Zaira: The EU Cyber Resilience Act – An Appraisal and Contextualization. In: *EuZ – Zeitschrift für Europarecht*, (2023), DOI: <https://doi.org/10.36862/eiz-euz015>. s B16-B17.

³⁴ RAJAMÄKI, Jyri – HÄMÄLÄINEN, Timo – RIIHIJÄRVI, Janne – KANGAS, Olli-Pekka – LAJUNEN, Antti – KERTTULA, Olli: Navigating the Cyber Resilience Act: Implications for the Dynamo Horizon Project. In: *Proceedings of the European Conference on Cyber Warfare and Security*, (2025), s. 892 – 893.

povinnosťami dôležitých a kľúčových subjektov podľa NIS 2. Kľúčovou otázkou je, či CRA možno chápať ako *lex specialis* pre výrobky s digitálnymi prvkami a NIS 2 ako *lex generalis* pre regulované subjekty, alebo či budú oba nástroje aplikované kumulatívne. CRA zároveň prináša nové práva a povinnosti jednotke CSIRT určenej za koordinátora v súlade s článkom 14 ods. 7 CRA. Ku vzťahu CRA a NIS 2 viď tiež ECKHARDT a KOTOVSKAIA (2023)³⁵ a RAMPÁŠEK a kol. (2025)³⁶.

Vzájomný vzťah medzi CRA a CSA je možné identifikovať napríklad v dvoch rovinách, uznávanie certifikácie podľa CSA a stanovením právomocí Agentúre Európskej únie pre kybernetickú bezpečnosť (ďalej len ENISA), zriadenej CSA. V článku 27 odseku 8 CRA sa uvádza, že produkty s digitálnymi prvkami a postupy zavedené výrobcom, pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa CSA, sa považujú za produkty a postupy v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I CRA, pokiaľ sa na tieto požiadavky vzťahuje EÚ vyhlásenie o zhode alebo európsky certifikát kybernetickej bezpečnosti, alebo ich časti. CRA teda uznáva za uvedených predpokladov EÚ vyhlásenie o zhode alebo certifikát v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa CSA. Pri uvedenom je však potrebné poukázať, že EÚ vyhlásenie o zhode v zmysle čl. 53 odseku 4 a certifikácie v zmysle čl. 56 odseku 2 CSA sú dobrovoľné pokiaľ sa v práve Únie alebo práve členského štátu nestanovuje inak. Ďalšiu synergiu CRA a CSA je možné evidovať v posilnení právomocí agentúry ENISA a to vo vzťahu zlepšovaniu zručností v kyberneticky odolnom digitálnom prostredí (čl. 10 CRA), ohlasovacích povinnosti výrobcov (čl. 14 CRA), dobrovoľné mu oznamovaniu (čl. 15 CRA), zriadeniu jednotnej oznamovacej platformy (čl. 16 CRA), dohľadom nad trhom a presadzovaním práva (kapitola V CRA) a hodnotením a preskúmaním CRA v zmysle článku 70 CRA.

Niektoré produkty s digitálnymi prvkami môžu byť zároveň klasifikované podľa čl. 6 AI Actu aj ako vysokorizikové systémy AI. Uvedené vytvára predpoklady potreby synergie CRA a AI Actu. V čl. 12 CRA sú stanovené pravidlá pre produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti CRA a ktoré sú klasifikované ako vysokorizikové systémy AI. Takto určené produkty sa považujú za produkty spĺňajúce požiadavky kybernetickej bezpečnosti stanovené v článku 15 AI Actu ak tieto produkty spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I CRA, procesy zavedené výrobcom sú v súlade so základnými

³⁵ ECKHARDT, Philipp – KOTOVSKAIA, Anastasia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. In: *International Cybersecurity Law Review*, Vol. 4, 2023, s. 147 – 164. Dostupné na <https://doi.org/10.1365/s43439-023-00084>

³⁶ RAMPÁŠEK, Michal – MESARČÍK, Matúš – ANDRAŠKO, Jozef: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: *Computer Law & Security Review*, Vol. 56, (2025), s. 2, 106093. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.106093>.

požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I CRA a dosiahnutie úrovne ochrany kybernetickej bezpečnosti požadovanej podľa článku 15 AI Actu je preukázané v EÚ vyhlásení o zhode vydanom podľa CRA³⁷. Na uvedené produkty s digitálnymi prvkami sa uplatňuje príslušný postup posudzovania zhody stanovený v článku 43 AI Actu. Na účely uvedeného posudzovania sú notifikované osoby, ktoré sú kompetentné kontrolovať zhodu vysokorizikových systémov AI podľa AI Actu kompetentné kontrolovať aj zhodu vysokorizikových systémov AI, ktoré patria do rozsahu pôsobnosti CRA, s požiadavkami uvedenými v prílohe I CRA za predpokladu, že súlad týchto notifikovaných osôb s požiadavkami stanovenými v článku 39 CRA bol posúdený v kontexte postupu notifikácie podľa AI Actu.³⁸

Výnimkou k uvedeným pravidlám vysokorizikových systémov AI, ktoré sú zároveň produktmi s digitálnymi prvkami, sú dôležité produkty s digitálnymi prvkami uvedené v prílohe III CRA, ktoré podliehajú postupom posudzovania zhody uvedeným v článku 32 ods. 2 písm. a) a b) a článku 32 ods. 3 CRA a kritické produkty s digitálnymi prvkami uvedené v prílohe IV CRA, ktoré musia zároveň získať európsky certifikát kybernetickej bezpečnosti podľa článku 8 ods. 1 CRA alebo ak ho nemajú, ktoré podliehajú postupom posudzovania zhody podľa článku 32 ods. 3 CRA a na ktoré sa uplatňuje postup posudzovania zhody založený na vnútornej kontrole uvedenej v prílohe VI k AI Actu, podliehajú postupom posudzovania zhody podľa CRA, pokiaľ ide o základné požiadavky kybernetickej bezpečnosti stanovené v CRA³⁹.

Druhá dimenzia - technické výzvy

Technické výzvy spojené s implementáciou CRA sú priamo odvodené od jeho cieľa zabezpečiť, aby produkty s digitálnymi prvkami spĺňali minimálne požiadavky na kybernetickú bezpečnosť počas celého svojho životného cyklu. Základným pilierom je koncepcia *security by design* a *secure by default*⁴⁰, ktorá od výrobcov vyžaduje, aby kybernetickú bezpečnosť integrovali už vo fáze návrhu a aby produkty uvádzali na trh s nastaveniami, ktoré garantujú primeranú ochranu bez toho, aby sa používatelia museli spoliehať na dodatočnú konfiguráciu. K uvedenému vid' aj CHIARA (2022)⁴¹ a RAMPÁŠEK a kol. (2025)⁴². Táto požiadavka je technicky

³⁷ čl. 12 ods. 1 CRA

³⁸ čl. 12 ods. II CRA

³⁹ čl. 12 ods. 3 CRA

⁴⁰ recitál 32 CRA

⁴¹ CHIARA, Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. In: *International Cybersecurity Law Review*, Roč. 3, (2022), s. 6. DOI: <https://doi.org/10.1365/s43439-022-00067-6>.

⁴² RAMPÁŠEK, Michal – MESARČÍK, Matúš – ANDRAŠKO, Jozef: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: *Computer Law & Security*

mimoriadne náročná, keďže výrobné cykly, najmä v spotrebnej elektronike, sú nastavené na rýchle inovácie a minimalizáciu nákladov, čo vedie k obmedzenej pozornosti venovanej robustnosti softvéru či hardvérových komponentov. Ďalším problémom je integrácia týchto zásad do vývojových procesov typu DevSecOps a CI/CD (priebežná integrácia kódu/priebežné *automatické* nasadzovanie do produkcie). CRA predpokladá, že bezpečnosť bude zabudovaná do každého kroku vývoja, od návrhu, testovania až po priebežné aktualizácie⁴³. V praxi to znamená, že výrobcovia musia zaviesť systematické procesy pre automatizované testovanie, skenovanie kódu a správu zraniteľností. Tento posun je náročný predovšetkým pre startupy, malé a stredné podniky, ktoré nemajú dostatočnú kapacitu alebo expertízu na implementáciu komplexných bezpečnostných opatrení.

Zásadnou technickou otázkou zostáva aj životnosť produktov a dĺžka poskytovania povinných aktualizácií. V zmysle čl. 13 odseku 9 CRA výrobcovia musia zabezpečiť, aby každá bezpečnostná aktualizácia uvedená v bode 8 časti II prílohy I CRA, ktorá bola sprístupnená používateľom počas obdobia podpory, zostala k dispozícii po jej vydaní minimálne 10 rokov alebo počas zvyšku obdobia podpory, podľa toho, čo trvá dlhšie. Štandardná dĺžka podpory produktu je v zmysle čl. 13 odseku 8 CRA 5 rokov. Z technického hľadiska to vyžaduje, aby výrobcovia mali robustnú infraštruktúru pre riadenie aktualizácií, schopnú poskytovať záplaty aj pre produkty, ktoré sú na trhu niekoľko rokov. To otvára otázku nielen technickej uskutočniteľnosti, ale aj hospodárskej únosnosti dlhodobej podpory.

Tretia dimenzia - ekonomické a trhové výzvy

CRA predstavuje zásadný zásah nielen do technických a právnych rámcov, ale aj do samotného fungovania digitálneho trhu v Európskej únii. Jedným z najvýraznejších problémov je disproporčný dopad na startupy, malé a stredné podniky, ktoré často nedisponujú kapacitami ani expertízou na zavedenie komplexných procesov kybernetickej bezpečnosti. Ako upozorňuje SCHMITTNER a kol. (2024)⁴⁴, CRA

Review, Vol. 56, (2025), s. 4, 6 a 10, 106093. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.106093>.

⁴³ SCHMITTNER, Christoph – VELEDAR, Orges – FASCHANG, Thomas – MACHER, Georg – BRENNER, Egon: Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. In: YILMAZ, Murat – CLARKE, Paul – RIEL, Andreas – MESSNARZ, Richard – GREINER, Christian – PEISL, Thomas (eds.): Systems, Software and Services Process Improvement. EuroSPI 2024. Communications in Computer and Information Science, vol. 2179. Cham: Springer, 2024, s. 397 – 400 DOI: https://doi.org/10.1007/978-3-031-71139-8_26.

⁴⁴ SCHMITTNER, Christoph – VELEDAR, Orges – FASCHANG, Thomas – MACHER, Georg – BRENNER, Egon: Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. In: YILMAZ, Murat – CLARKE, Paul – RIEL, Andreas – MESSNARZ, Richard – GREINER, Christian – PEISL,

predpokladá systematické procesy na riadenie zraniteľností, dokumentáciu komponentov a priebežné testovanie bezpečnosti, čo v praxi bude znamenať nutnosť investícií do technických riešení a špecializovaného personálu, ktoré sú pre menšie subjekty finančne i organizačne problematické.

Ekonomickú výzvu predstavuje aj otázka dzovania zhody v zmysle článku 32 CRA. Samotné posudzovanie zhodu bude predstavovať navýšenie finančných nákladov pre regulované subjekty, predovšetkým na startupy, malé a stredné podniky. Aj keď CRA v zmysle článku 33 počíta s podporou pre malé a stredné podniky vrátane startupov, zadaná pomoc je vsúčasnosti veľmi všeobecná a abstraktná.

Ďalším aspektom je možný dopad CRA na inovácie a dynamiku trhu. V širšom trhovom kontexte CRA môže spôsobiť konsolidáciu trhu. Veľké nadnárodné podniky, ktoré už disponujú robustnými bezpečnostnými a compliance oddeleniami, budú schopné absorbovať dodatočné regulačné náklady a dokonca využiť prísnejšiu reguláciu ako konkurenčnú výhodu. Naopak, MSP vrátane startupov môžu byť vytlačené z trhu alebo nútené spoliehať sa na subdodávky a outsourcing bezpečnostných služieb, čo oslabuje ich samostatnosť.

Štvrtá dimenzia - organizačné a praktické výzvy

CRA prináša významné organizačné a praktické výzvy, ktoré zasahujú do každodennej praxe regulovaných subjektov. Jednou z kľúčových výziev je bezpečnosť dodávateľského reťazca. CRA a Smernica 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS ustanovujú, že výrobcovia sú zodpovední nielen za vlastný produkt, ale aj za komponenty pochádzajúce od subdodávateľov. Táto požiadavka posúva dôraz na komplexný manažment tretích strán a vytvára tlak na zavedenie kontrolných mechanizmov naprieč celým dodávateľským reťazcom a vytvorenie due diligence procesov v organizáciách voči subdodávateľom. Ako poukazujú NYGARD a KATSIKAS (2025)⁴⁵ práve bezpečnosť digitálneho dodávateľského reťazca sa stáva najkritickejšou výzvou pre prevádzkovateľov infraštruktúry a výrobcov produktov, pričom CRA ukladá povinnosť posudzovať riziká subdodávateľov a prijímať preventívne opatrenia.

Ďalšou organizačnou a praktickou výzvou je potreba školení a budovania compliance kultúry v organizáciách. CRA zásadne mení spôsob, akým majú regulované subjekty

Thomas (eds.): Systems, Software and Services Process Improvement. EuroSPI 2024. Communications in Computer and Information Science, vol. 2179. Cham: Springer, 2024, s. 397 – 398 DOI: https://doi.org/10.1007/978-3-031-71139-8_26.

⁴⁵ NYGARD, Arne Roar – KATSIKAS, Sokratis: Digital supply chain security for power sector operators in the light of the new EU directives and regulation. In: Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics, (2025), s. 70 – 80.

prístupovať k vývoju, testovaniu a údržbe produktov s digitálnymi prvkami. Praktický dopad implementácie CRA do vnútorných procesov regulovaných subjektov si bude vyžadovať vnútroorganizačnú transformáciu a zavedenie procesov. S tým úzko súvisí aj implementácia vnútropodnikových politík (napríklad politika vývoja softvéru, politika aktualizácií, politika výberu a kontroly subdodávateľov, atď) a interných kontrolných mechanizmov. Zavedenie takýchto politík je však náročné, pretože vyžaduje nielen odborné znalosti, ale aj alokáciu finančných a ľudských zdrojov, ktoré sú pre mnohé regulované subjekty obmedzené.

Piata dimenzia - akademické a etické výzvy

Implementácia CRA prináša aj viaceré akademické a etické výzvy a to predovšetkým vo vzťahu k slobode spotrebiteľa (povinné bezpečnostné aktualizácie) a kybernetickej bezpečnosti, konfliktom medzi reguláciou kybernetickej bezpečnosti a slobodou podnikateľ, spravodlivosťou vo vzťahu k zodpovednosti výrobcov produktov s digitálnymi prvkami, ktorí implementujú komponenty alebo open source softvér do svojich výrobkov. Aplikácia CRA do praxe bude stanovovať otázky, že či príliš prísna regulácia kybernetickej bezpečnosti v priestore EÚ nebude zároveň brzdu inovácií a technologického pokroku a bude vytvárať priestor pre širšiu diskusiu o tom, do akej miery má EÚ regulovať kybernetickú bezpečnosť a tým usmerňovať dynamiku technologického vývoja. V neposlednej rade implementácia CRA a tým aj doplnenie právneho rámca kybernetickej bezpečnosti v priestore EÚ nám poskytuje ďalšie informácie ku skúmaniu otázky „práva na kybernetickú bezpečnosť“ ako základného práva, ktorej sa napríklad venoval vo svojej práci CHIARA (2024)⁴⁶.

Záver

Predkladaný článok analyzuje prostredníctvom 5 dimenzií implementačné výzvy CRA a poukazuje, že aplikácia CRA má nevyhnutne multidimenzálny charakter, pričom právny rámec sa prelína s technickými požiadavkami, ekonomickými dôsledkami, vnútroorganizačnou správou a akademicko-etickými otázkami. Hlavným zistením je, že úspech implementácie nebude výsledkom izolovaného „dodržania“ jednotlivých povinností, ale koordinovaného riadenia naprieč celým životným cyklom výrobkov s digitálnymi prvkami a celou organizáciou regulovaného subjektu. Kľúčová bude materiálna a procesná koherencia s príbuznými právnymi predpismi EÚ (najmä NIS 2 a AI Act) a zároveň včasná, transparentná a predvídateľná tvorba delegovaných a vykonávacích aktov, ktorá zabezpečí právnu istotu adresátov, zamedzí duplicitnej regulačnej záťaži a umožní premeniť normatívne požiadavky na

⁴⁶ CHIARA, Pier Giorgio: Towards a right to cybersecurity in EU law? The challenges ahead. In: Computer Law & Security Review, Vol. 53, (2024), s. 1-9, 105961. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.105961>

prakticky uplatniteľné postupy. Technicky CRA zavádza zásady security-by-design a secure-by-default, ustanovuje povinnosti riadenia zraniteľností, aktualizčných režimov a transparentnosti, pričom naväzuje posudzovanie zhody na klasifikáciu rizika. Ekonomicky a trhovo je zrejmá asymetria dopadov, nakoľko väčší výrobcovia majú kapacitu absorbovať náklady, zatiaľ čo startupy, malé a stredné podniky budú čeliť neúmernej záťaži, s potenciálom konsolidačného efektu. Proporcionalita implementácie a včasná štandardizácia sú preto nevyhnutné na minimalizáciu nákladov posudzovania zhody. Organizačne a prakticky CRA presúva ťažisko na riadenie dodávateľského reťazca (due diligence, zmluvné klauzuly, verifikácia tretích strán), interné politiky a riadenie kompetencií (jasné roly, určenie zodpovednosti). Bez zodpovedajúcej správy, zodpovednosti a kapacít sa formálna zhoda nepremietne do reálnej odolnosti. Akademické a etické aspekty akcentujú rovnováhu medzi bezpečnosťou, inováciou a ochranou základných práv. CRA tak nie je iba ďalším súborom povinností, ale je nástrojom strategickej premeny smerom k predvídateľnej, merateľnej a certifikovateľnej kybernetickej odolnosti.

Zoznam použitej literatúry

1. BRIGHI, Raffaella – ADINOLFI, Giovanna: EU Cybersecurity Policies in Cyber-Physical Ecosystems: Challenges and Perspectives. In: *European Journal of Risk Regulation*, Roč. 16, č. 2 (2025), s. 466 – 478. doi:10.1017/err.2025.10026
2. BURRI, Mira – ZIHLMANN, Zaira: The EU Cyber Resilience Act – An Appraisal and Contextualization. In: *EuZ – Zeitschrift für Europarecht*, (2023), s. 1-45. DOI: <https://doi.org/10.36862/eiz-euz015>.
3. CHIARA, Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. In: *International Cybersecurity Law Review*, Roč. 3, (2022), s. 1 – 18. DOI: <https://doi.org/10.1365/s43439-022-00067-6>.
4. CHIARA, Pier Giorgio: Towards a right to cybersecurity in EU law? The challenges ahead. In: *Computer Law & Security Review*, Vol. 53, (2024), 9 s., 105961. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.105961>
5. CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? In: *European Journal of Risk Regulation*, Roč. 16, č. 2 (2025), s. 469 – 483. doi:10.1017/err.2025.9
6. Cyber Resilience Act - Impact assessment. Dostupný na <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment>
7. ECKHARDT, Philipp – KOTOVSKAIA, Anastasia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2

Directive. In: International Cybersecurity Law Review, Vol. 4, 2023, s. 147 – 164. Dostupné na <https://doi.org/10.1365/s43439-023-00084>

8. Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS
9. Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Text s významom pre EHP)
10. Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).
11. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)
12. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)
13. NYGARD, Arne Roar – KATSIKAS, Sokratis: Digital supply chain security for power sector operators in the light of the new EU directives and regulation. In: Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics, (2025), s. 70 – 80. Dostupný na <https://dl.acm.org/doi/10.1145/3716554.3716565>
14. O'GRADY Stephan: The Cyber Resilience Act: A Five Alarm Fire. Portland: Newstex 2025. Dostupné na <https://www.proquest.com/blogs-podcasts-websites/cyber-resilience-act-five-alarm-fire/docview/3236971601/se-2>
15. RAJAMÄKI, Jyri – HÄMÄLÄINEN, Timo – RIIHIJÄRVI, Janne – KANGAS, Olli-Pekka – LAJUNEN, Antti – KERTTULA, Olli: Navigating the Cyber Resilience Act: Implications for the Dynamo Horizon Project. In: Proceedings of the European Conference on Cyber Warfare and Security, (2025), s. 891 – 902. Dostupné na <https://www.proquest.com/conference-papers-proceedings/navigating-cyber-resilience-act-implications/docview/3244083252/se-2>
16. RAMPÁŠEK, Michal – MESARČÍK, Matúš – ANDRAŠKO, Jozef: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation

- and certification? In: Computer Law & Security Review, Vol. 56, (2025), 17 s., 17106093. ISSN 2212-473X. DOI: <https://doi.org/10.1016/j.clsr.2024.106093>.
17. RUOHONEN Jukka - TIMMERS Paul: Vulnerability Coordination Under the Cyber Resilience Act, In: Computer Science, 2024, 14 s. Dostupné na <https://doi.org/10.48550/arXiv.2412.06261>
 18. SCHMITTNER, Christoph – VELEDAR, Orges – FASCHANG, Thomas – MACHER, Georg – BRENNER, Egon: Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. In: YILMAZ, Murat – CLARKE, Paul – RIEL, Andreas – MESSNARZ, Richard – GREINER, Christian – PEISL, Thomas (eds.): Systems, Software and Services Process Improvement. EuroSPI 2024. Communications in Computer and Information Science, vol. 2179. Cham: Springer, 2024, s. 390 – 404 DOI: https://doi.org/10.1007/978-3-031-71139-8_26.
 19. SHAABAN, Abdelkader Magdy – SCHMITTNER, Christoph: A ThreatGet-Based Framework for Aligning System Security with the Cyber Resilience Act. In: TÖRNGREN, Martin – BÜRKNER, Paul – et al. (eds.): Computer Safety, Reliability, and Security: SAFECOMP Workshops 2025. Cham: Springer, 2025, s. 101 – 114. Dostupné na <https://doi.org/10.1007/978-3-032-02018-5>
 20. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)
 21. Smernica 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS
 22. TEODORESCU, Cosmin A. – VASILE, Ionut – STANCIU, Oana: The Evolution of Mobile Cybersecurity Regulations in the European Union. In: Management & Marketing. Challenges for the Knowledge Society, Roč. 20, č. 1 (2025), s. 52 – 63. Dostupné na doi: <https://doi.org/10.2478/mmcks-2025-0004>

Kontaktné údaje

Mgr. Miroslav Sorkovský
sorkovsky3@uniba.sk

Ústav práva informačných technológií a práva duševného vlastníctva, Právnická fakulta Univerzity Komenského v Bratislave

CRA: KYBERNETICKÁ BEZPEČNOSŤ SMART HODINIEK A OCHRANA DETÍ

CRA: CYBERSECURITY OF SMARTWATCHES AND CHILD PROTECTION

Silvia Kratochvilová¹

Abstrakt: Príspevok analyzuje nový právny predpis Európskej únie – Cyber Resilience Act (CRA), ktorého hlavným cieľom je komplexne posilniť kybernetickú bezpečnosť produktov s digitálnymi prvkami uvádzaných na trh v rámci Európskej únie. Primárne sa zameriava na kybernetickú bezpečnosť detí v digitálnom prostredí, ktoré predstavujú obzvlášť zraniteľnú skupinu používateľov. Príspevok poukazuje na konkrétne bezpečnostné zraniteľnosti detských smart hodín na základe praktických príkladov z minulosti, ktoré odhalili závažné kybernetické riziká spojené s týmito zariadeniami. Skúma, akým spôsobom môže CRA efektívne prispieť k zvýšeniu bezpečnosti prostredníctvom zavedenia záväzných povinností pre výrobcov, dovozcov a distribútorov počas celého životného cyklu produktu. Príspevok konkretizuje v praxi základné požiadavky kybernetickej bezpečnosti stanovené CRA a ich aplikáciu na detské smart hodinky. Osobitná pozornosť je venovaná analýze prepojenosti CRA s ďalšími relevantnými právnymi predpismi, najmä s predpismi na ochranu osobných údajov (GDPR) v kontexte detských smart hodín a ich špecifických funkcionalít. Príspevok hodnotí, ako CRA dopĺňa existujúci právny rámec a aké prínosy, ale aj potenciálne limity, prináša táto nová regulácia pre ochranu detí v digitálnom priestore.

Kľúčové slová: Cyber Resilience Act, kybernetická bezpečnosť, digitálne prvky, detské smart hodinky, osobné údaje

Abstract: The paper analyses the new European Union legal regulation – the Cyber Resilience Act (CRA), whose main objective is to comprehensively strengthen the cybersecurity of products with digital elements placed on the market within the European Union. It primarily focuses on the cybersecurity of children in the digital environment, who represent a particularly vulnerable group of users. The paper highlights specific security vulnerabilities of

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva

children's smartwatches based on practical examples from the past that revealed serious cyber risks associated with these devices. It examines how the CRA can effectively contribute to enhanced security through the introduction of binding obligations for manufacturers, importers, and distributors throughout the entire product lifecycle. The paper concretises in practice the essential cybersecurity requirements established by the CRA and their application to children's smartwatches. Special attention is devoted to analysing the interconnectedness of the CRA with other relevant legal regulations, particularly data protection regulations (GDPR) in the context of children's smartwatches and their specific functionalities. The paper evaluates how the CRA complements the existing legal framework and what benefits, as well as potential limitations, this new regulation brings for child protection in the digital space.

Key words: Cyber Resilience Act, cybersecurity, digital elements, children's smartwatches, personal data

Úvod

Hoci nové nariadenie CRA² dopĺňajúce právne predpisy EÚ týkajúce sa kybernetickej bezpečnosti výrobkov nadobudlo účinnosť už 10.12.2024, jeho plné uplatňovania v EÚ začne až 11.12.2027.³ Dovtedy majú relevantné hospodárske subjekty definované v CRA priestor na zosúladienie svojich produktov s digitálnymi prvkami s požiadavkami CRA. Tento príspevok sa zameriava konkrétne na detské smart hodinky, ktoré taktiež spadajú pod novú reguláciu týkajúcu sa kybernetickej odolnosti produktov s digitálnymi prvkami. Príspevok rozoberá problematiku detských smart hodínok jednak z pohľadu predchádzajúcej právnej úpravy, ktorá sa z pohľadu kybernetickej bezpečnosti a odolnosti produktov ukázala ako nedostatočná, cez GPSR⁴ až po CRA. Keďže rozsah príspevku neumožňuje komplexný pohľad na právnu reguláciu detských smart hodínok, pozornosť je zameraná najmä na novú právnu úpravu, ktorá si kladie za cieľ, okrem iného, vyriešiť

² Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (ďalej aj len „CRA“)

³ S výnimkou, že článok 14 sa uplatňuje od 11. septembra 2026 a kapitola IV (články 35 až 51) sa uplatňuje od 11. júna 2026.

⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS (ďalej aj len „GPSR“)

(i) nízku úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami, vrátane detských smart hodínok, ktorá sa prejavuje rozšíreným výskytom zraniteľnosti a nedostatočným a nekonzistentným poskytovaním bezpečnostných aktualizácií na ich riešenie, ako aj (ii) nedostatočné porozumenie používateľov a ich prístup k informáciám.⁵ Príspevok si kladie za cieľ odpovedať na otázku, či CRA dokáže efektívne eliminovať identifikované kybernetickobezpečnostné zraniteľnosti detských smart hodínok a aké sú prípadné limity tejto regulácie? Dôležitosť zamerania príspevku na detské smart hodinky potvrdzujú štatistické údaje o neustále rastúcom trhu v tomto segmente⁶, pričom primárnou cieľovou skupinou týchto produktov je skupina zraniteľných spotrebiteľov (deti) a ich rodičia⁷. Práve preto je potrebné, aby tieto produkty boli spoľahlivé, bezpečné a neprinášali falošný pocit bezpečia, keďže ako uviedla Nórska spotrebiteľská rada „... *hlavným účelom týchto zariadení je poskytnúť rodičom pokoj, zatiaľ čo sa ich deti voľne hrajú vonku, považujeme za kľúčové, aby dodržiavali primerané štandardy bezpečnosti a ochrany osobných údajov.*“⁸

Nedostatky detských smart hodínok v minulosti

Dôležitosť novej právnej úpravy je možné ilustrovať na zmonitorovaných bezpečnostných nedostatkoch detských smart hodínok, ktoré boli medializované ešte v roku 2017 Nórskou spotrebiteľskou radou (ďalej aj len „NSR“)⁹. NSR analyzovala práva spotrebiteľov konkrétne v súvislosti so štyrmi smart hodinkami pre

⁵ Recitál 1 CRA

⁶ Podľa štatistík Global Market Insights: „*Veľkosť globálneho trhu detských smart hodínok bola v roku 2024 ohodnotená na 11,2 miliardy USD a predpokladá sa, že bude ročne rásť o 8,7 % od roku 2025 do roku 2034. Detské smart hodinky získavajú na popularite, keďže rodičia sa čoraz viac obávajú o bezpečnosť svojich detí a chcú s nimi zostať v kontakte. Rodičia vyhľadávajú technológie s bezpečnostnými funkciami, ako je GPS sledovanie polohy, geofencing a SOS volanie.*“ Global Market Insights. Verified Market Research 2025: Europe Kids Digital Watch Market Market Size, Status & Forecast to 2032. 2025. Dostupné online: <https://www.gminsights.com/industry-analysis/kids-smartwatch-market> Taktiež, podľa SkyQuest: „*Globálny trh s inteligentnými hodinkami pre deti bol v roku 2023 ocenený na 12,2 miliardy USD a očakáva sa, že do roku 2032 vzrastie z 13,4 miliardy USD v roku 2024 na 28,3 miliardy USD, čo predstavuje medziročný rast (CAGR) 9,8 % počas prognózovaného obdobia (2025 – 2032).*“ SkyQuest. Global Kids Smartwatch Market. Report ID: SQMIG20D2215. Január 2025. Dostupné online: <https://www.skyquestt.com/report/kids-smartwatch-market>

⁷ Podľa Nórskej spotrebiteľskej rady „[p]re rodičov malých detí sa túžba zostať v kontakte so svojimi deťmi mohla dostať do konfliktu s názorom, že dieťa je príliš malé na to, aby malo drahý a komplikovaný smartfón. To by mohlo vysvetľovať rastúcu popularitu inteligentných hodínok pre deti, ktoré uľahčujú jednoduchú komunikáciu bez obáv, že deti stratia telefóny.“

⁸ Nórska spotrebiteľská rada: #WatchOut. Analysis of smartwatches for children október 2017. Dostupné online: <https://storageo2.forbrukerradet.no/media/2017/10/watchout-rapport-oktober-2017.pdf>, s. 3

⁹ *Ibidem*.

deti, ktoré boli zakúpené v nórskech obchodoch¹⁰, pričom boli identifikované¹¹ „... vážne bezpečnostné nedostatky, nespoľahlivé bezpečnostné prvky a nedostatočnú ochranu spotrebiteľa.“¹² Ako uviedol Finn Myrstad, riaditeľ digitálnej politiky v NSR „[j]e to veľmi vážne, keď produkty, ktoré sľubujú bezpečnosť detí, ich v skutočnosti vystavujú riziku kvôli slabému zabezpečeniu a funkciám, ktoré nefungujú správne.“¹³ V roku 2018 bolo taktiež v Safety Gate (systém EÚ na rýchlu výmenu informácií o nebezpečných nepotravinových výrobkoch) zverejnené upozornenie o stiahnutí konkrétneho typu detských smart hodín z celého európskeho trhu z dôvodu vážnej kybernetickej zraniteľnosti.¹⁴ Hoci sa autorka príspevku nepodarilo získať údaje týkajúce sa prípadných aktuálnych nedostatkov detských smart hodín, pretrvávajúcu aktuálnosť problému potvrdzujú správy SonicWall¹⁵, podľa ktorých útoky na IoT¹⁶ majú dramaticky stúpajúci charakter (v roku 2023 nárast o 107 % a v roku 2024 nárast o 124 % oproti predchádzajúcemu roku), čo je spôsobené čo raz väčším množstvom zapojených vecí (vrátane detských smart hodín) a ich slabým zabezpečením. Tento alarmujúci trend potvrdzuje, že zraniteľnosť IoT ekosystému, vrátane detských smart hodín, predstavuje rastúcu kybernetickú hrozbu. Taktiež, podľa aktuálnej správy ENISA z októbra 2025, kybernetické hrozby vykazujú jasnú

¹⁰ *Ibidem*.

¹¹ Technickú správu, ktorú si objednala Nórska spotrebiteľská rada, vypracovala IT bezpečnostná spoločnosť Mnemonic

¹² Nórska spotrebiteľská rada: Slabé zabezpečenie GPS hodín pre deti. 18. október 2017. Dostupné online: <https://www.forbrukerradet.no/siste-nytt/elendig-sikkerhet-i-smartklokke-for-barn/>

¹³ Zo správy NSR vyplýva, že boli identifikované okrem iného tieto nedostatky (i) cudzia osoba mohla prevziať kontrolu nad hodinkami a sledovať, odpočúvať a komunikovať s dieťaťom, (ii) mohol byť získaný prístup k údajom o polohe detí v reálnom čase a historickej polohe a osobným údajom, ako aj umožnenie priameho kontaktovania detí bez vedomia rodičov, (iii) dieťa mohlo byť sledované pri jeho pohybe alebo vytvorený dojem, že je niekde, kde nie je, (iv) nespoľahlivosť SOS tlačidla, ktoré upozorní rodičov, ak je dieťa v núdzi, a funkcie geofencingu, ktorá odošle upozornenie vždy, keď dieťa vstúpi alebo opustí určenú oblasť, (v) zhromažďovanie informácií, ktoré by od nich užívateľ nevyhnutne neočakával.

¹⁴ Číslo upozornenia: A12/0157/19, Dostupné online: <https://ec.europa.eu/safety-gate-alerts/screen/webReport/alertDetail/349994?lang=en>. Podľa upozornenia „Mobilná aplikácia sprevádzajúca hodinky má nešifrovanú komunikáciu so svojim backendovým serverom a server umožňuje neoverený prístup k dátam. V dôsledku toho je možné ľahko získať a zmeniť údaje, ako je história polohy, telefónne čísla, sériové číslo.“ a „Škodlivý používateľ môže posilať príkazy na akékoľvek hodinky, takže to volá ďalšie číslo podľa svojho výberu, môže komunikovať s dieťaťom, ktoré má zariadenie, alebo lokalizovať dieťa prostredníctvom GPS.“

¹⁵ Sonicwall. 2025 Cyber Threat Report. The need for speed and strong allies to overcome the cybersecurity battlefield. Dostupné online: <https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report> Sonicwall. 2024 Mid-Year Cyber Threat Report. Actionable insights for evolving threats. Dostupné online: <https://www.tdsynnex.com/na/us/cybersolv/wp-content/uploads/sites/10/2024/11/SonicWall-2024-Mid-Year-Cyber-Threat-Report.pdf>

¹⁶ *Internet of Things* (internet vecí) – prepojené veci a zariadenia pripájajúce sa na internet

koncentráciu v niekoľkých oblastiach, pričom najväčší podiel majú práve mobilné hrozby so 42,4 %, čo poukazuje na to, že mobilné zariadenia (ako sú aj detské smart hodinky) sú naďalej primárnym útočným priestorom.¹⁷

Aký bude mať CRA vplyv na detské smart hodinky?

CRA zavádza úplne novú právnu úpravu zameranú na kybernetickú odolnosť produktov s digitálnymi prvkami (sprístupnených na trh EÚ¹⁸, ktorých zamýšľaný účel alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti¹⁹), za účelom (i) ich uvádzania na trh s menším počtom zraniteľností (a to vzhľadom na zvyšujúci sa počet kybernetických útokov), pričom (ii) ich bezpečnosť musí byť braná výrobcami vážne počas celého životného cyklu. CRA je založené na viacerých prístupoch, konkrétne (i) horizontálnom prístupe, (ii) prístupe založenom na riziku, a (iii) bezpečnosti produktu.²⁰ Horizontálny prístup demonštruje cieľ CRA „... vytvoriť horizontálny regulačný rámec na európskej úrovni s cieľom zabezpečiť vyššiu úroveň kybernetickej bezpečnosti pre spotrebiteľov a podniky“²¹ a „... poskytnúť široké horizontálne požiadavky na kybernetickú bezpečnosť pre produkty.“²² CRA tak predstavuje horizontálnu legislatívu, ktorá harmonizuje kyberneticko-bezpečnostné pravidlá takmer pre všetky produkty s digitálnym prvkom sprístupňované na trh EÚ²³, pričom sa už nespolieha, ako doteraz, na sektorovú legislatívu spôsobujúcu fragmentáciu trhu. V súvislosti s funkciami, ktoré produkty vykonávajú a tým predstavujúcim kyberneticko-bezpečnostným rizikom potom CRA v diferencuje medzi 3 skupinami produktov s digitálnymi prvkami, a to (i) normálne, (ii) dôležité²⁴, a (iii) kritické, pričom zaradenie konkrétneho produktu má dopad najmä na postupy posudzovania

¹⁷ ENISA. ENISA THREAT LANDSCAPE 2025, október 2025. dostupné online: https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_o.pdf

¹⁸ Keďže CRA sa uplatňuje na všetky produkty s digitálnymi prvkami sprístupňované na trh EÚ, má extrateritoriálny charakter a vzťahuje sa aj na výrobcov, distribútorov a dovozcov mimo EÚ.

¹⁹ Čl. 2 ods. 1 CRA

²⁰ CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? European Journal of Risk Regulation. jún 2025;16(2):469–84. s. 471, 475. <http://dx.doi.org/10.2139/ssrn.5050688>

²¹ BELTRÁN, Marta: AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union. Computers & Security. 01. november 2025;158:104628., s. 5. <https://doi.org/10.1016/j.cose.2025.104628>

²² SHAFFIQUE, Mohammed Raiz: Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review. 01. september 2024;54:106009, s. 7. <https://doi.org/10.1016/j.clsr.2024.106009>

²³ *Ibidem*, s. 8

²⁴ Podľa čl. 7 ods. 2 písm. b) CRA sa ďalej delia do triedy I a II

zhody²⁵. Z nedostatkov identifikovaných NSR je zrejmé, že detské smart hodinky, ktorých účelom je priame logické dátové pripojenia k sieti alebo inému zariadeniu²⁶, spĺňajú definíciu dôležitých produktov s digitálnymi prvkami podľa čl. 7 ods. 2 písm. b) CRA, keďže cudzie osoby prostredníctvom nich môžu, okrem iného, manipulovať dieťa a rodiča, narušiť bezpečnosť dieťaťa a spracovanie osobných údajov dieťaťa predstavuje významné riziko pre jeho bezpečnosť a súkromie. Príloha III, trieda I CRA taktiež vyslovene uvádza, že sem patria aj „[p]rodukty na nosenie na tele určené na použitie deťmi a pre deti“.²⁷ Výrobcovia detských smart hodínok majú v zásade tri možnosti postupu posudzovania zhody (i) modul A, bez zapojenia tretej osoby s uplatnením harmonizovaných noriem, spoločných špecifikácií alebo európskych schém certifikácie kybernetickej bezpečnosti, (ii) modul B a C so zapojením tretej strany, ktorá vydá certifikát EU skúšky typu, alebo (iii) modul H so zapojením tretej strany, ktorá posúdi systém kvality výrobcu.²⁸

Povinnosti podľa CRA

Za účelom naplnenia cieľov stanovených v CRA je hospodárskym subjektom uložená celá škála povinností týkajúcich sa výrobkov a ich uvádzania na trh v EÚ. Z dôvodu

²⁵ „... je zrejmé, že akákoľvek klasifikácia ako dôležitý produkt triedy II alebo kritický produkt výrazne zvýši zložitosť získania posúdenia zhody výrobku, keďže vlastné vyhlásenie o zhode na základe harmonizovaných noriem už nie je možné.“ MUECK, Markus – ROBERTS, Taylor - DU BOISPÉAN, Stéphane – GAIE, Christophe. Introduction to the European Cyber Resilience Act. V: Mueck M, Gaie C, editori. European Digital Regulations [Internet]. Cham: Springer Nature Switzerland; 2025 [cit 09. september 2025]. s. 91–110. Available at: https://doi.org/10.1007/978-3-031-80809-8_4, s. 100

²⁶ „Inteligentné hodinky pre deti obsahujú SIM kartu, ktorá im umožňuje pripojiť sa na internet prostredníctvom sietí GSM alebo cez Wi-Fi pripojenie ... Funkcie zariadení sa medzi zariadeniami a aplikáciami líšia, ale všetky inteligentné hodinky v našej štúdii prichádzajú so základnými funkciami GPS, ktoré umožňujú rodičom sledovať pohyb svojich detí v reálnom čase prostredníctvom sprievodnej mobilnej aplikácie. Tieto aplikácie sú pripojené na internet, čo umožňuje množstvo ďalších funkcií.“ Nórska spotrebiteľská rada: #WatchOut. Analysis of smartwatches for children október 2017. Dostupné online: <https://storage02.forbrukerradet.no/media/2017/10/watchout-rapport-october-2017.pdf>, s. 6

²⁷ Návrh vykonávacieho aktu podľa čl. 7 ods. 4 CRA spresňuje produkty na nosenie na tele určené na použitie deťmi alebo pre deti nasledovne: „Osobné nositeľné výrobky, ktoré sú určené na používanie deťmi a pre deti, sú výrobky s digitálnymi prvkami, ktoré môžu byť nosené alebo umiestnené na tele osôb mladších ako 14 rokov, priamo alebo prostredníctvom odevu alebo doplnkov. Táto kategória zahŕňa okrem iného nositeľné zariadenia pre deti.“ Európska Komisia. Commission implementing regulation (EU) on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council. Dostupné online: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_sk

²⁸ Ohľadom posudzovania zhody a európskych štandardov pozri KAMARA, Irene: European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research. 26. december 2024;37(5):1441–60, s. 1442, 1450 a nasl.

rozsahu príspevku bude pozornosť venovaná špeciálne najmä tým, ktoré súvisia s vyššie uvedenými kyberneticko-bezpečnostnými rizikami identifikovanými v súvislosti s detskými smart hodinkami. CRA zavádza pre výrobcov produktov s digitálnymi prvkami jeden z princípov predstavených v oblasti kybernetickej bezpečnosti Aktom o kybernetickej bezpečnosti²⁹, konkrétne *principle of cybersecurity by design and by default*³⁰ (kybernetická bezpečnosť už v štádiu návrhu a ako štandard)³¹. Princíp kybernetickej bezpečnosti „by design“ je premietnutý, hoci nie vyslovene kodifikovaný, najmä v čl. 13 ods. 1 CRA, podľa ktorého musia výrobcovia zaistiť, že produkt bol navrhnutý, vyvinutý a vyrobený v súlade so základnými požiadavkami kybernetickej bezpečnosti podľa Prílohy I CRA. Na tieto účely sú výrobcovia podľa čl. 13 ods. 2 CRA povinní vykonať posúdenie kybernetickobezpečnostných rizík a jeho výsledok zohľadniť už, avšak nie len, pri plánovaní, návrhu a vývoji produktu. Ako uvádza Shaffique „[i]gnorovanie bezpečnostných aspektov z dôvodu obmedzení zdrojov alebo funkčnosti by preto nebolo prípustné.“³² Na uvedené ustanovenia potom nadväzuje v Prílohe I časti I bode 2 písm. b) CRA požiadavka, aby sa produkty s digitálnymi prvkami na základe posúdenia kybernetickobezpečnostných rizík a podľa potreby sprístupňovali na trhu v konfigurácii zabezpečenej na úrovni štandardného nastavenia³³, čo predstavuje princíp bezpečnosti „by default“. Dôležitosť implementácie princípu odôvodňuje ENISA tým, že „[z]načné percento zákazníkov má tendenciu ignorovať bezpečnostné funkcie z dôvodu pohodlia alebo nedostatku technických znalostí; To zvyčajne vedie k zraniteľnostiam, ktorým by sa dalo vyhnúť vhodným používaním bezpečnostných prvkov, ktoré sú už zahrnuté v zariadeniach a produktoch.“ Uvedené posúdenie kybernetickobezpečnostných rizík sú výrobcovia povinní vykonať aj v ďalších fázach, ako je výroba, dodania a údržba produktu s digitálnymi prvkami, a to s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať incidentom

²⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (Akt o kybernetickej bezpečnosti)

³⁰ ENISA. ENISA Advisory Group: Opinion. Consumers and IoT security. September 2019. s. 5. Dostupné online:

https://www.enisa.europa.eu/sites/default/files/all_files/Final%20Opinion%20ENISA%20AG%20Consumer%20IoT%20Perspective%20-09.2019.pdf

³¹ Európska Komisia: Politiky EÚ v oblasti kybernetickej bezpečnosti. Dostupné online: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

³² SHAFFIQUE, Mohammed Raiz: Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review. 01. september 2024;54:106009, s. 10 a 11. <https://doi.org/10.1016/j.clsr.2024.106009>

³³ Pokiaľ sa výrobca a komerčný používateľ v súvislosti s individualizovaným produktom s digitálnymi prvkami nedohodnú inak, vrátane možnosti vrátiť nastavenie produktu na pôvodné.

a minimalizovať ich vplyv, a to aj v súvislosti so zdravím a bezpečnosťou používateľov. Ďalšou povinnosťou je vypracovanie technickej dokumentácie. Výrobcovia sú povinní taktiež určiť obdobie podpory, ktoré má trvať aspoň 5 rokov³⁴ a počas tohto obdobia zaistiť, aby sa zraniteľnosť riešila účinne a v súlade so základnými požiadavkami kybernetickej bezpečnosti, napr. poskytovaním bezpečnostných aktualizácií³⁵ (čl. 13 ods. 8 CRA), ktoré budú k dispozícii aspoň 10 rokov po ich vydaní (čl. 13 ods. 9 CRA). Dátum skončenia obdobia podpory musí byť zrozumiteľne uvedený už v čase nákupu produktu (čl. 13 ods. 19 CRA). CRA stanovuje taktiež informácie a návod pre používateľa, ktoré musia byť priložené k produktom (v tlačenej alebo elektronickej podobe), pričom musia byť jasné, zrozumiteľné, pochopiteľné a čitateľné (čl. 13 ods. 18 CRA). V neposlednom rade zavádza CRA v čl. 14 pre výrobcov dva druhy ohlasovaných udalostí, a to (i) povinnosť ohlásiť každú aktívne zneužitú zraniteľnosť produktu s digitálnymi prvkami, o ktorej sa dozvie, ako aj (ii) každý závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami, o ktorom sa dozvie.

Povinnosti a základné požiadavky v praxi

Hoci je zrejmé, že budúcnosť kybernetickej bezpečnosti týchto špecifických produktov bude závisieť najmä od dôsledného dodržiavania požiadaviek stanovených CRA, autorka zastáva názor, že základné požiadavky kybernetickej bezpečnosti podľa Prílohy 1 CRA pomôžu eliminovať bezpečnostné nedostatky a zabezpečiť základnú funkciu, ktorú rodičia od detských smart hodín oprávnené vyžadujú – ochranu a bezpečnosť ich dieťaťa. Developeri a výrobcovia budú musieť v zmysle princípu kyberbezpečnosť „by design“ už v štádiu návrhu zariadenia poznať a adresovať kybernetickobezpečnostné riziká (ako napríklad riziko kompromitácie mikrofónu), čo predstavuje posun od reaktívneho k proaktívnemu prístupu ku kybernetickej bezpečnosti. Tento systémový posun je dôležitejší než eliminácia jednotlivých konkrétnych zraniteľností, pretože vytvára kultúru bezpečnosti v rámci celého životného cyklu produktu. Implementovanie požiadavky na sprístupňovanie na trhu v zabezpečenej konfigurácii „by default“ a teda v najvyššej úrovni zabezpečenia by mohlo v praxi znamenať najmä deaktivovanie mikrofónu a kamery už v predvolenom nastavení a ich prípadná aktivácia až na základe explicitného súhlasu oprávnenej osoby (zákonného zástupcu maloletého)³⁶. Spracúvané (nie len

³⁴ Pre výnimky pozri čl. 13 ods. 8 CRA

³⁵ Z pohľadu detských smart hodín je dôležité, že podľa Prílohy I, časť II bod 2 CRA, ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií, a to aby používatelia neboli povinní inštalovať nové aktualizácie funkcií výlučne na účely prijímania najnovších bezpečnostných aktualizácií Recital 57 CRA)

³⁶ Príloha I, časť I bod 2. písm. b) CRA

osobné) údaje užívateľov, najmä lokalizačné údaje, textová a hlasová komunikáciu a obrazový záznam budú musieť byť šifrované najmodernejšími mechanizmami, prípadne inými technickými prostriedkami³⁷ a to bez ohľadu na to, či ide o údaje uložené v zariadení alebo ďalej prenášané. Podstatnou bude minimalizácia údajov³⁸, a teda hodinky by už nemali zbierať údaje, ktoré by od nich užívateľ nevyhnutne neočakával, ako napr. zaznamenávanie detailnej histórie pohybu (a nie iba aktuálnu polohu na požiadanie) alebo zbieranie identifikačných údajov zariadení v okolí. Doba uchovávanía zbieraných údajov by mala byť preto taktiež obmedzená, čo by mohlo byť zabezpečené napríklad automatickým mazaním starších údajov. Podstatným prínosom by mala byť povinné poskytovanie bezpečnostných aktualizácií po stanovenú dobu, čím je na výrobcov kladená požiadavka navrhovať produkty s dlhodobou podporovateľnosťou.

Súhra CRA s ďalšími predpismi

Úlohou CRA je „len“ doplniť existujúci rámec kybernetickej bezpečnosti EÚ pozostávajúci z právnych predpisov, ako je Akt o kybernetickej bezpečnosti, prípadne smernica NIS2. Keďže však produkty s digitálnymi prvkami môžu predstavovať aj ďalšie bezpečnostné riziká, ktoré nie vždy súvisia s kybernetickou bezpečnosťou, ale môžu byť dôsledkom narušenia bezpečnosti, v zmysle CRA by tieto riziká mali byť naďalej regulované inými príslušnými harmonizačnými právnymi predpismi EÚ³⁹, ako sú napr. GDPR a GPSR. Tieto predpisy však problematiku detských smart hodín riešia iba parciálne, konkrétne (i) GDPR stanovuje pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a (ii) GPSR reguluje všeobecnú bezpečnosť výrobkov uvedených alebo sprístupnených na trhu a slúži ako „bezpečnostná sieť“⁴⁰, pokiaľ podľa práva EÚ, ktoré upravuje bezpečnosť dotknutých výrobkov, neexistujú osobitné ustanovenia s rovnakým cieľom. V súvislosti s produktami s digitálnymi prvkami je pre zabezpečenie ich celkovej bezpečnosti podstatné, že hoci čl. 2 ods. 1 tretí pododsek písm. b) GPSR vylučuje uplatnenie oddielu 1 kapitoly III, kapitoly V a VII a kapitoly IX až XI na produkty, na ktoré sa vzťahujú osobitné požiadavky stanovené v harmonizačných právnych predpisoch EÚ, čl. 11 CRA navrhuje uplatniteľnosť týchto článkov aj na produkty s digitálnymi prvkami, pokiaľ ide o aspekty a riziká alebo kategórie rizík, na ktoré sa nevzťahuje CRA, ak sa na tieto produkty nevzťahujú osobitné bezpečnostné požiadavky

³⁷ Príloha I, časť I bod 2. písm. e) CRA

³⁸ Príloha I, časť I bod 2. písm. g) CRA

³⁹ Recitál 50 CRA a čl. 11 CRA

⁴⁰ CHIARA, Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *Int Cybersecur Law Rev.* 01. december 2022;3(2):255–72, s. 267. DOI: 10.1365/543439-022-00067-6

stanovené inými harmonizačnými právnymi predpismi EÚ. Na účely tohto príspevku je tak dôležité, že na detské smart hodinky, resp. produkty s digitálnymi prvkami všeobecne sa uplatnia, okrem iného, aj povinnosti hospodárskych subjektov (najmä výrobcov, dovozcov a distribútorov) stavené v GPSR. Podľa čl. 5 GPSR, hospodárske subjekty uvádzajú na trh alebo sprístupňujú na trhu len bezpečné výrobky, pričom pri posudzovaní sa zohľadňujú viaceré aspekty, vrátane kategórie spotrebiteľov používajúcich výrobok, najmä posúdením rizika pre zraniteľných spotrebiteľov, ako sú deti, príp. ak si to vyžaduje povaha výrobku, vhodné kyberneticko-bezpečnostné prvky potrebné na ochranu výrobku pred vonkajšími vplyvmi.⁴¹ Obdobne ako CRA, aj GPSR upravuje povinnosť posúdenia bezpečnosti produktov, analýzu rizík, príp. technickú dokumentáciu, avšak nejde o duplicitné, ale skôr komplementárne povinnosti. Prienik v regulovaných oblastiach je možné nájsť aj medzi GDPR a CRA, keďže CRA pokrýva nie len technické aspekty kybernetickej bezpečnosti, ale aj niektoré aspekty ochrany (nie len osobných) údajov, ako je minimalizácia údajov, právo na výmaz údajov, ochrana údajov pred manipuláciou a úpravou, dôvernosť a šifrovanie údajov. Vzájomné pôsobenie medzi týmito predpismi je zdôraznené v čl. 57 CRA, podľa ktorého, ak je produkt s digitálnymi prvkami v súlade s CRA, ale napriek tomu predstavuje významné kyberneticko-bezpečnostné riziko, ako aj riziko pre zdravie alebo bezpečnosť osôb alebo súlad s povinnosťami vyplývajúcimi z práva EÚ alebo vnútroštátneho práva, ktorého zámerom je ochrana základných práv (napr. práva na ochranu osobných údajov a súkromia), môžu byť voči takémuto produktu prijaté rovnaké opatrenia ako voči produktu, ktorý nie je v súlade s CRA⁴².

Prínosy a limity regulácie

Je nepochybné, že CRA má priniesť vyššiu bezpečnosť produktov na európskom trhu a to predovšetkým zavedením množstva povinností v rámci celého výrobného a životného cyklu produktov, ako aj dodávateľského reťazca. CRA má preto potenciál zvýšiť dôveru spotrebiteľov v kybernetickú bezpečnosť produktov na trhu a celkovú odolnosť voči kybernetickým hrozbám. Ochrana spotrebiteľov aj po nákupe, a to formou podpory a aktualizácií eliminuje počet zastaraných a zraniteľných zariadení v prevádzke a reflektuje špecifickú zraniteľnosť detí v kyberpriestore. Veľké množstvo a fragmentácia predpisov vzťahujúcich na tento druh produktov, vrátane prípadných vykonávacích aktov môže predstavovať významnú právnu neistotu pre povinné osoby, vrátane rizika duplicitných a prekrývajúcich sa povinností (ako aj bolo načrtnuté v predchádzajúcej časti), pričom do prijatia vykonávacích aktov viacero

⁴¹ Čl. 6 ods. 1 písm. e) a g) GPSR

⁴² CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? European Journal of Risk Regulation. jún 2025;16(2):469–84. s. 483. <http://dx.doi.org/10.2139/ssrn.5050688>

dôležitých aspektov regulácie zostane nejasných. Komplexnosť postupov posudzovania zhody v závislosti od kategorizácie produktov predstavuje zložitý systém z časti závislý od existencie harmonizačných noriem a spoločných špecifikácií, ktorý bude nevyhnutne znamenať zvýšené náklady (s negatívnym dopadom hlavne na SME) reflektujúce zložitosť povinných postupov, čo môže viesť k šedému dovozu a z toho vyplývajúcim následkom. CRA, na rozdiel od GDPR, nepriznáva práva jednotlivcom, preto títo nebudú môcť priamo uplatňovať práva voči povinným osobám na základe CRA a teda prínosy CRA pre jednotlivcov sú skôr nepriame.

Záver

Ako uvádza Chiara, „... [n]apriek tomu, že CRA je v literatúre málo viditeľný, najmä v porovnaní s aktom o umelej inteligencii, ktorý má však výrazne užší rozsah pôsobnosti, má všetko, čo potrebuje na to, aby sa stal novým "GDPR", pokiaľ ide o potenciál ovplyvniť a "revolúciu" na trhu, ktorý reguluje".⁴³ Tento článok sa osobitne zameriaval na regulačný rámec týkajúci sa primárne detských smart hodín s cieľom zistiť, aké nástroje CRA používa na eliminovanie kybernetickobezpečnostných nedostatkov týchto produktov a či dokáže efektívne eliminovať identifikované kybernetickobezpečnostné zraniteľnosti detských smart hodín. CRA disponuje významným potenciálom eliminovať identifikované kybernetickobezpečnostné zraniteľnosti detských smart hodín, avšak tento potenciál je podmienený efektívnou implementáciou a presadzovaním. Hlavnými deklarovanými cieľmi sú zvýšenie ochrany osobných údajov a súkromia, a to dopĺňaním už existujúcich právnych predpisov, ako je napríklad GDPR. Vďaka svojmu extrateritoriálnemu charakteru ovplyvní hospodárske subjekty prakticky na celom svete, ktoré budú musieť implementovať základné bezpečnostné požiadavky a ďalšie pravidlá a povinnosti vo vzťahu k svojim výrobkom. A hoci kritici CRA namietajú, okrem iného, zvýšené náklady na implementáciu, ktoré môžu viesť k spomaľovaniu uvedenia na trh, brzdeniu inovácií a straty konkurencieschopnosti, autorka verí, že posilnenie ochrany detí má v tomto prípade absolútnu prioritu. CRA, napriek svojim potenciálnym výzvam, predstavuje nevyhnutný krok k zabezpečeniu digitálneho prostredia pre najzraniteľnejších používateľov a posilňuje dôveru v digitálne produkty na jednotnom trhu EÚ.

Zoznam použitej literatúry

1. BELTRÁN, Marta: AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union. Computers &

⁴³ *Ibidem*, s. 483

- Security. 01. november 2025;158:104628., s. 1, 5.
<https://doi.org/10.1016/j.cose.2025.104628>
2. ENISA. ENISA Advisory Group: Opinion. Consumers and IoT security. September 2019. s. 5. Dostupné online: https://www.enisa.europa.eu/sites/default/files/all_files/Final%20Opinion%20ENISA%20AG%20Consumer%20IoT%20Perspective%20-09.2019.pdf
 3. Európska Komisia. Commission implementing regulation (EU) on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council. Dostupné online: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_sk
 4. Európska Komisia. Communication from the Commission on the EU Security Strategy. 24.7.2020. COM(2020) 605 final, s. 8. Dostupné online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN>
 5. Európska Komisia: Politiky EÚ v oblasti kybernetickej bezpečnosti. Dostupné online: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>
 6. Global Market Insights. Verified Market Research 2025: Europe Kids Digital Watch Market Market Size, Status & Forecast to 2032. 2025. Dostupné online: <https://www.gminsights.com/industry-analysis/kids-smartwatch-market>
 7. CHIARA, Pier Giorgio: The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *Int Cybersecur Law Rev.* 01. december 2022;3(2):255–72, s. 267, 271. DOI: 10.1365/543439-022-00067-6
 8. CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? *European Journal of Risk Regulation.* jún 2025;16(2):469–84. s. 471, 472, 475, 483, 484. <http://dx.doi.org/10.2139/ssrn.5050688>
 9. KAMARA, Irene: European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research.* 26. december 2024;37(5):1441–60, s. 1442, 1450 a nasl. <https://doi.org/10.1080/13511610.2024.2349626>
 10. MUECK, Markus – ROBERTS, Taylor - DU BOISPÉAN, Stéphane – GAIE, Christophe. Introduction to the European Cyber Resilience Act. V: Mueck M, Gaie C, editori. *European Digital Regulations* [Internet]. Cham: Springer Nature Switzerland; 2025 [cit 09. september 2025]. s. 91–110. Available at: https://doi.org/10.1007/978-3-031-80809-8_4, s. 100
 11. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady

(EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS

12. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS
13. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)
14. Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (Akt o kybernetickej bezpečnosti)
15. Nórska spotrebiteľská rada: #WatchOut. Analysis of smartwatches for children október 2017. Dostupné online: <https://storage02.forbrukerradet.no/media/2017/10/watchout-rapport-october-2017.pdf>, s. 3
16. Nórska spotrebiteľská rada: Slabé zabezpečenie GPS hodínok pre deti. 18. október 2017. Dostupné online: <https://www.forbrukerradet.no/siste-nytt/elendig-sikkerhet-i-smartklokke-for-barn/>
17. SHAFFIQUE, Mohammed Raiz: Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review. 01. september 2024;54:106009, s. 7, 10, 11. <https://doi.org/10.1016/j.clsr.2024.106009>
18. SkyQuest. Global Kids Smartwatch Market. Report ID: SQMIG20D2215. Január 2025. Dostupné online: <https://www.skyquestt.com/report/kids-smartwatch-market>
19. Smernica Európskeho parlamentu a Rady 2001/95/ES z 3. decembra 2001 o všeobecnej bezpečnosti výrobkov
20. Sonicwall. 2024 Mid-Year Cyber Threat Report. Actionable insights for evolving threats. Dostupné online: <https://www.tdsynnex.com/na/us/cybersolv/wp-content/uploads/sites/10/2024/11/SonicWall-2024-Mid-Year-Cyber-Threat-Report.pdf>
21. Sonicwall. 2025 Cyber Thread Report. The need for speed and strong allies to overcome the cybersecurity battlefield. Dostupné online: <https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report>

Kontaktné údaje

JUDr. Silvia Kratochvilová

kratochvilov7@uniba.sk

Ústav práva informačných technológií a práva duševného vlastníctva

Právnická fakulta, Univerzita Komenského v Bratislave

KYBERNETICKÁ BEZPEČNOSŤ AKO NOVÝ ROZMER SÚKROMNOPRÁVNEJ ZODPOVEDNOSTI ČLENOV ORGÁNOV OBCHODNÝCH SPOLOČNOSTÍ¹

CYBERSECURITY AS A NEW DIMENSION OF PRIVATE LAW LIABILITY FOR MEMBERS OF CORPORATE BODIES

Dominika Pintérová²

Abstrakt: V dnešnom digitálnom svete sa kybernetická bezpečnosť stáva nielen technickou, ale aj právnou otázkou, ktorá zásadným spôsobom ovplyvňuje riadenie obchodných spoločností. Príspevok analyzuje, ako rastúce riziká spojené s kybernetickými útokmi a incidentmi transformujú oblasti rozhodovania členov orgánov, ich povinnosti, ale i tradičné chápanie súkromnoprávnej zodpovednosti členov štatutárnych a dozorných orgánov. V centre pozornosti je najmä otázka, či zanedbanie povinností v rámci kybernetickej bezpečnosti môže predstavovať porušenie povinnosti konať s odbornou (náležitou) starostlivosťou podľa § 135a a 194 Obchodného zákonníka a aké dôsledky to môže mať pre členov orgánov spoločností. Cieľom bude identifikovať dôležité otvorené otázky, výzvy a odporúčania pre slovenskú prax, ktoré majú prispieť k efektívnejšiemu zvládaniu kybernetickej bezpečnosti na úrovni orgánov obchodných spoločností. Príspevok sa zaoberá aj praktickými aspektmi, ako je možnosť delegácie pôsobnosti na kvalifikovaného manažéra kybernetickej bezpečnosti, pričom sa ako kľúčové preventívne opatrenie analyzuje aj zmluvná špecifikácia týchto povinností, najmä v rámci zmluvy o výkone funkcie. Základnou hypotézou je, že na členov štatutárnych orgánov je kladený vyšší dôraz v oblasti kybernetickej bezpečnosti, pričom sa vyskytuje interdisciplinárny prístup k právnej regulácii, úprave práv a povinností ako i zodpovednosti, kde zákon o kybernetickej bezpečnosti predstavuje právny predpis *lex specialis* a Obchodný zákonník právny predpis *lex generalis*.

¹ Táto práca je financovaná z prostriedkov EÚ Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu s názvom „Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality“ (CUSEC) pod číslom 17R05-04-V01-00002.

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra obchodného práva a hospodárskeho práva

Kľúčové slová: kybernetická bezpečnosť, členovia orgánov obchodných spoločností, súkromnoprávna zodpovednosť, odborná/náležitá starostlivosť

Abstract: In today's digital world, cybersecurity is becoming not only a technical but also a legal issue that fundamentally affects the governance of business corporations. The paper analyzes how the growing risks associated with cyberattacks and incidents transform the decision-making of board members, their duties, as well as the traditional understanding of private law liability of members of statutory and supervisory bodies. The main focus is on the question of whether neglecting cybersecurity obligations may constitute a breach of the duty to act with due care under Sections 135a and 194 of the Slovak Commercial Code, and what consequences this may entail for members of company bodies. The aim is to identify key open questions, challenges, and recommendations for Slovak practice that could contribute to more effective management of cybersecurity at the level of company bodies. The paper also addresses practical aspects, such as the possibility of delegating competence to a qualified cybersecurity manager, while also analysing the contractual specification of these duties as a key preventive measure, in particular within the framework of the contract for the performance of the function. The basic hypothesis is that there is a higher emphasis on members of statutory bodies in the field of cyber security, while there is an interdisciplinary approach to legal regulation, regulation of rights and obligations as well as liability, where the Cyber Security Act is a legal regulation *lex specialis* and the Commercial Code is a legal regulation *lex generalis*.

Key words: cybersecurity, members of corporate bodies, private law liability, due care

Úvod

V súčasnej digitálnej ére sa kybernetická bezpečnosť stáva významnou výzvou nielen pre technikov, ale aj pre manažérov a členov orgánov obchodných spoločností. Rastúci počet kybernetických útokov a incidentov zásadne ovplyvňuje spôsob, akým sa spoločnosti riadia a ako členovia štatutárnych a dozorných orgánov vnímajú svoju zodpovednosť.³ Kým v minulosti bola kybernetická bezpečnosť prevažne doménou

³ LIPTON, Martin: *Risk Management and the Board of Directors*. The Harvard Law School Forum on Corporate Governance and Financial Regulation. Published 25. September 2025. Available at: <https://corpgov.law.harvard.edu/2025/09/25/risk-management-and-the-board-of-directors-10/>

IT oddelení, dnes preniká priamo do rozhodovacích procesov a právnych povinností osôb zodpovedných za riadenie spoločnosti.⁴

Príspevok obsahuje rozbor právnych povinností členov orgánov obchodných spoločností v oblasti zabezpečenia kybernetickej bezpečnosti, najmä vo vzťahu k odbornej/náležitej starostlivosti a povinnosti predchádzať vzniku škody. Tiež skúma, do akej miery sú títo členovia povinní poznávať špecifiká kybernetických rizík, implementovať primerané interné politiky a dokumentáciu, zabezpečiť školenia zamestnancov a dohliadať na výkon opatrení na ochranu pred kybernetickými incidentmi. Právna analýza sa opiera najmä o platnú slovenskú legislatívu - zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj ako „ZoKB“) a zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej aj ako „OBZ“) i ďalšie relevantné predpisy.

Príspevok sa podrobne zaoberá otázkou, ako môže zanedbanie kybernetickej bezpečnosti viesť k súkromnoprávnej zodpovednosti členov orgánov voči obchodnej spoločnosti či tretím osobám. Analyzuje možné scenáre, v ktorých môže dôjsť k porušeniu povinností i odbornej/náležitej starostlivosti, najmä v prípadoch, keď členovia orgánu nedostatočne reagujú na známe alebo predvídateľné kybernetické riziká, podcenia výber kvalifikovaného odborníka na kybernetickú bezpečnosť alebo zanedbajú zavedenie kontrolných mechanizmov. Dôležitým rozmerom príspevku je rozbor preventívnych opatrení v podobe regulácie kybernetických rizík prostredníctvom zmluvných klauzúl, ktoré môžu obchodné spoločnosti zaviesť na ochranu spoločnosti pred škodami spôsobenými kybernetickými útokmi.

Cieľom je podnietiť zamyslenie nad tým, že kybernetická bezpečnosť už nie je len technickou otázkou, ale stáva sa zásadným rozmerom právnej a manažérskej zodpovednosti, ktorý ovplyvňuje stabilitu, dôveru a dlhodobý úspech podnikov v obchodnom prostredí. Na záver autorka identifikuje dôležité otvorené otázky, výzvy a odporúčania pre slovenskú prax, ktoré majú prispieť k efektívnejšiemu zvládaniu kybernetickej bezpečnosti na úrovni orgánov obchodných spoločností.

Povinnosti štatutárnych orgánov v oblasti kybernetickej bezpečnosti

Povinnosti pri výkone funkcie členov volených orgánov vyplývajú z právnych predpisov, zmluvy o výkone funkcie člena orgánu, spoločenskej zmluvy/stanov, a rozhodnutí valného zhromaždenia. Tieto povinnosti možno rozdeliť do nasledovných kategórií:

1. *Všeobecné povinnosti stanovené Obchodným zákonníkom* (odborná starostlivosť, náležitá starostlivosť, osobný výkon funkcie, lojalita, mlčanlivosť...).

⁴ GALE, Megan – BONGIOVANNI, Ivano – SLAPNICAR, Sergeja: *Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead*. In *Computers & Security* 121(4). July 2022. p. 1 - 2. DOI:[10.1016/j.cose.2022.102840](https://doi.org/10.1016/j.cose.2022.102840)

2. *Osobitné povinnosti stanovené Obchodným zákonníkom* (zvolávanie valného zhromaždenia, povinnosť informovať spoločníkov o záležitostiach spoločnosti...).
3. *Povinnosti stanovené inými zákonmi* – zákonom o kybernetickej bezpečnosti.⁵

Povinnosti spadajúce do oblasti kybernetickej bezpečnosti sú definované predovšetkým v ZoKB, ktorý je *lex specialis* voči OBZ. Tieto povinnosti štatutárnych orgánov nie sú priamo vymedzené ako samostatná kapitola, ale vyplývajú z celkového rámca zodpovednosti prevádzkovateľov základnej služby alebo poskytovateľov digitálnej služby, za ktorých konajú štatutárne orgány. Možno ich rozdeliť do nasledovných oblastí:

1. Organizačná a riadiaca zodpovednosť

- Štatutárny orgán musí zabezpečiť, aby organizácia mala vybudovaný systém riadenia kybernetickej bezpečnosti (§ 19 ZoKB), prijať bezpečnostnú politiku a interné predpisy.
- Zodpovedá za prijatie bezpečnostných opatrení (§ 20 ZoKB), ktoré sa týkajú: riadenia rizík, bezpečnostnej politiky, riadenia prístupu, ochrany sietí, systémov a dát, kontinuity činností a obnovy po incidente.

2. Zodpovednosť za nahlasovanie a spoluprácu

- Povinnosť zabezpečiť hlásenie kybernetických bezpečnostných incidentov (§ 24 ZoKB) Národnému bezpečnostnému úradu (NBÚ) alebo príslušnému CSIRT tímu. Štatutár musí garantovať, že organizácia má určenú kontaktnú osobu a nastavené procesy pre komunikáciu s NBÚ.

3. Povinnosti v oblasti dokumentácie

- Zabezpečiť vypracovanie a aktualizáciu bezpečnostnej dokumentácie, analýzy rizík, bezpečnostného projektu, ak to povaha služby vyžaduje.

4. Zodpovednosť za školenia a povedomie

- Povinnosť zaviesť vzdelávanie a školenie zamestnancov v oblasti kybernetickej bezpečnosti. Štatutár musí dohliadať, aby sa tieto procesy reálne vykonávali.

Úloha štatutárneho orgánu v riadení kybernetických rizík by mala byť predovšetkým strategická, t j. mal by sa zaoberať skôr vývojom strategického plánu kybernetickej bezpečnosti a jeho implementáciou, než jeho operačnou realizáciou.⁶ Štatutárny orgán je tak garantom, že spoločnosť plní povinnosti podľa ZoKB – od prijatia bezpečnostných opatrení a vytvorenia systému riadenia kybernetickej bezpečnosti, cez nahlasovanie incidentov a vedenie dokumentácie, až po školenia zamestnancov. Aj keď sankcie sa ukladajú právnickej osobe, v konečnom

⁵ PINTÉROVÁ, Dominika: *K možnosti zavedenia pracovnoprávneho režimu člena orgánu kapitálovej obchodnej spoločnosti v procese rekodifikácie, 1. časť*. In *Justičná Revue*, roč. 75, č. 4, 2023, s. 505 – 506.

⁶ GALE, Megan – BONGIOVANNI, Ivano – SLAPNICAR, Sergeja: *Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead*. In *Computers & Security* 121(4). July 2022. p. 2.
DOI:[10.1016/j.cose.2022.102840](https://doi.org/10.1016/j.cose.2022.102840)

dôsledku je štatutár zodpovedný za ich implementáciu a môže niešť obchodnoprávnu alebo aj trestnoprávnu zodpovednosť (pri závažných porušeníach).⁷ Na tomto mieste je nevyhnutné uviesť, že v ZoKB sú definované aj špecifické zodpovednosti, a to zodpovednosť za riešenie bezpečnostných incidentov, zodpovednosť za oznámenie bezpečnostných incidentov, zodpovednosť za riešenie bezpečnostných zraniteľností.

Povinnosť štatutárneho orgánu konať s odbornou/náležitou starostlivosťou (osobitne v kontexte kybernetickej bezpečnosti)

Členovia štatutárnych orgánov kapitálových obchodných spoločností sú povinní vykonávať svoju pôsobnosť s **odbornou (náležitou) starostlivosťou a v súlade so záujmami spoločnosti a všetkých jej spoločníkov (akcionárov)**.⁸ Uvedené vymedzenie je ďalej pertraktované ďalšími povinnosťami, že sú

1. povinní zaobstarať si a pri rozhodovaní zohľadniť všetky dostupné informácie týkajúce sa predmetu rozhodnutia,
2. zachovávať mlčanlivosť o dôverných informáciách a skutočnostiach, ktorých prezradenie tretím osobám by mohlo spoločnosti spôsobiť škodu alebo ohroziť jej záujmy alebo záujmy jej spoločníkov (akcionárov), a
3. pri výkone svojej pôsobnosti nesmú uprednostňovať svoje záujmy, záujmy len niektorých spoločníkov (akcionárov) alebo záujmy tretích osôb pred záujmami spoločnosti.

V rámci doktríny je odborná starostlivosť chápaná ako očakávaná miera **informovanosti a odbornosti** štatutárneho orgánu v podobe objektívnych osobných kvalít, ktoré má spĺňať každá osoba pôsobiaca vo funkcii člena štatutárneho orgánu.⁹ Rovnaký záver uvádza aj doc. Duračinská „*Požiadavku odbornej starostlivosti nechápem ako požiadavku na odbornosť v zmysle požadovanej kvalifikácie, ale v zmysle profesionálneho prístupu k výkonu funkcie, to znamená zaobstarania si a zohľadnenia*

⁷ V Českej republike môže Úrad v zmysle § 58 zákona č. 264/2025 Sb. o kybernetické bezpečnosti udeliť dočasný zákaz výkonu funkcie člena štatutárneho orgánu, do doby odstránenia stanovených nedostatkov, najmenej po dobu 6 mesiacov, ak v priamej súvislosti s plnením rozhodnutia Úradu podľa § 56 ods. 1, ktorým bola poskytovateľom regulovanej služby uložená povinnosť odstrániť zistené nedostatky, opakovane alebo závažne porušil svoje povinnosti pri výkone funkcie, v dôsledku čoho bolo zmarené riadne splnenie rozhodnutia Úradu.

⁸ § 135a, § 194 ods. 5 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

⁹ Obdobne konštatuje MAMOJKA, Mojmir: § 135a ObZ [Zodpovednosť pri výkone funkcie]. In MAMOJKA, Mojmir a kol.: Obchodný zákonník – Veľký komentár. 1. zväzok. Bratislava: Eurokódex, 2016. s. 539, nasledovne „možno konštatovať, že odborná starostlivosť je očakávaná miera informovanosti a odbornosti konateľa, na základe ktorej je povinný vykonávať svoju funkciu odo dňa jej vzniku až do dňa jej zániku. V tejto súvislosti zdôrazňujeme, že informovanosť a odbornosť sa nespája s individuálnymi vlastnosťami konkrétneho konateľa, ale ide o objektívne osobné kvality, ktoré má vo všeobecnosti spĺňať každá osoba pôsobiaca v pozícii štatutárneho orgánu.“

dostupných informácií.”¹⁰ Kategória odbornej starostlivosti je teda zmiernená doktrínou „business judgement rule“, podľa ktorej má štatutárny orgán právo na podnikateľské rozhodnutie a na omyl, pokiaľ dodrží zásady odbornej starostlivosti, to znamená, že nekoná podvodne, vo vlastnom záujme, a že si zaobstaral všetky dostupné informácie a vyhodnotil riziká svojho rozhodnutia.¹¹

Kybernetická bezpečnosť sa v dôsledku nových povinností štatutárnych orgánov v kontexte ZoKB stáva ďalšou zložkou odbornej/náležitej starostlivosti.¹²

Odbornú starostlivosť v kontexte kybernetickej bezpečnosti je nevyhnutné vnímať ako prístup daného člena orgánu spoločnosti k samotnému výkonu funkcie, spočívajúci napríklad v zaobstaraní a zohľadnení dostatočného množstva informácií pre uskutočnenie konkrétneho rozhodnutia v oblasti kybernetickej bezpečnosti. To znamená, že člen orgánu nemusí byť v pravom slova zmysle odborník, resp. profesionál v sfére kybernetickej bezpečnosti. Ak by sme totiž pripustili opačný výklad, ten by v praktickej rovine znamenal, že výkon funkcie člena orgánu by bol podmienený splnením podmienky odbornosti v podobe určitého vzdelania či iných znalostí. Možno však konštatovať, že v oblasti kybernetickej bezpečnosti je štatutárny orgán povinný postupovať pri svojich rozhodnutiach a konaniach nepochybne s väčším dôrazom na odbornú/náležitú starostlivosť, pričom musí:

1. **sledovať legislatívu v oblasti kybernetickej bezpečnosti** na úrovni SR i EÚ, resp. opatrenia štátu/vlády relevantné pre daný sektor podnikania spoločnosti a následne vyhodnotiť, či spoločnosť spĺňa legislatívne požiadavky v tejto oblasti a prípadne ich implementovať a zároveň pravidelne sledovať prostredníctvom analýzy vývoj hrozieb a technológií, t. j. nestačí zaviesť raz systém ochrany, ale je nutná kontinuálna aktualizácia politiky kybernetickej bezpečnosti,
2. **zaobstaráť odborníka** – znalca,¹³ manažéra kybernetickej bezpečnosti, pokiaľ nedisponuje dostatočnou empiriou ohľadom kybernetickej bezpečnosti (tzv. vertikálna delegácia tejto oblasti riadenia spoločnosti); napríklad sa môže obrátiť na zamestnancov spoločnosti s potrebnou kvalifikáciou alebo skúsenosťami,

¹⁰ DURAČINSKÁ, Jana: *Povinnosť starostlivosti riadneho hospodára alebo povinnosť odbornej starostlivosti z hľadiska právnej komparatistiky*. In Dny práva – 2012 – Days of Law. 6. ročník mezinárodnej konferencie poľadané Právnickou fakultou Masarykovy univerzity. Sborníky příspěvků. Brno: Masarykova univerzita, 2013. s. 2. Dostupné na:

https://www.law.muni.cz/sborniky/dny_prava_2012/files/Bermudskytrojuhelnik/DuracinskaJana.pdf

¹¹ K tomu pozri ROSTÁŠ, Dušan: *8. Pravidlo podnikateľského uváženia a možnosti jeho implementácie do slovenského práva*. In MRÁZOVÁ, Žofia - HUSÁR, Ján - DOLNÝ, Jaroslav a kol.: *Volené orgány kapitálových spoločností. Vybrané otázky*. Košice: ŠafárikPress, 2021. s. 146 – 150 a s. 156 - 159.

¹² Rovnako LIPTON, Martin: *Risk Management and the Board of Directors*. The Harvard Law School Forum on Corporate Governance and Financial Regulation. Published 25. September 2025. Available at: <https://corpgov.law.harvard.edu/2025/09/25/risk-management-and-the-board-of-directors-10/>

¹³ NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Kyberbezpečnosť ako nové znalecké odvetvie*. Dostupné na: <https://www.nbu.gov.sk/kyberbezpecnost-ako-nove-znalecke-odvetvie/>

alebo na externých manažéroch kybernetickej bezpečnosti, pričom v oboch prípadoch musí uzatvoriť zmluvu, v rámci ktorej sa upravujú práva a povinnosti, zodpovednosť manažéra kybernetickej bezpečnosti.

3. **realizovať špecifické povinnosti štatutárneho orgánu, ktoré úsek kybernetickej bezpečnosti môže vyvolať** (zvolanie valného zhromaždenia, aktualizácia politiky kybernetickej bezpečnosti, vykonanie auditu a testov (internými a externými subjektmi), dokumentácia bezpečnostných incidentov, plán školení zamestnancov, atď.).

Výkon pôsobnosti štatutárneho orgánu v oblasti kybernetickej bezpečnosti – zmluvné špecifiká

Ako sme už vyššie konštatovali, kybernetická bezpečnosť sa v dôsledku nových povinností štatutárnych orgánov v kontexte ZoKB stáva ďalšou zložkou odbornej/náležitej starostlivosti, pričom priestor na bližšiu špecifikáciu týchto povinností ale aj podmienok dodržania odbornej/náležitej starostlivosti prinášajú **zmluvné klauzuly, a to najmä v zakladateľských dokumentoch a zmluve o výkone funkcie**,¹⁴ pričom inšpiráciu môžu priniesť dokumenty vydávané Ministerstvom investícií, regionálneho rozvoja a informatizácie¹⁵ alebo Národným bezpečnostným úradom.¹⁶

Právny rámec inštitútu zmluvy o výkone funkcie je *de lege lata* zakotvený v § 66 ods. 6 OBZ nasledovne: „*Vzťah medzi spoločnosťou a členom orgánu spoločnosti alebo spoločníkom pri zariaďovaní záležitostí spoločnosti sa spravuje primerane ustanoveniami o mandátnej zmluve, ak zo zmluvy o výkone funkcie uzatvorenej medzi spoločnosťou a členom orgánu spoločnosti alebo spoločníkom, ak bola zmluva o výkone funkcie uzavretá alebo zo zákona nevyplýva iné určenie práv a povinností.*“¹⁷ Keďže predmetný kontrakt nie je upravený ako samostatný pomenovaný zmluvný typ v

¹⁴ OVEČKOVÁ, Oľga – CSACH, Kristián – ŽITŇANSKÁ, Lucia: *Obchodné právo 2 (Obchodné spoločnosti a družstvo)*, Bratislava: Wolters Kluwer, 2020. s. 272 „jednostranne kogentne je vymedzený rozsah povinností člena orgánu, ktorých porušenie môže viesť k zodpovednosti za škodu, preto nie je možné zúžiť rozsah fiduciárnych povinností. Je však možné uložiť členovi orgánu ďalšie dodatočné povinnosti či obmedzenia. Uloženie dodatočných povinností bude možné aj v zmluve o výkone funkcie, teda so súhlasom daného člena orgánu.“

¹⁵ MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE: *Povinnosti správcu ISVS v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich naplňaní*. Dostupné na: https://mirri.gov.sk/wp-content/uploads/2022/02/KB-K2_3-1-Povinnosti-spravcu-ISVS_ver1.1.pdf

¹⁶ KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI: *Sekcia záväzných metodík alebo riadenie bezpečnosti*. Dostupné na: <https://cybercompetence.sk/kniznica/>

¹⁷ § 66 ods. 6 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

OBZ, uzatvára sa podľa § 66 ods. 6 OBZ a § 269 ods. 2 OBZ.¹⁸ Z nášho pohľadu vidíme v zmluve o výkone funkcie v rámci oblasti kybernetickej bezpečnosti priestor na bližšiu špecifikáciu a úpravu:

- rozsahu práv a povinností štatutárneho orgánu a jeho úlohy pri zabezpečovaní kybernetickej bezpečnosti,
- možnosti delegácie na interných/externých odborníkov – manažérov kybernetickej bezpečnosti,
- odbornej/náležitej starostlivosti v nadväznosti na kybernetickú bezpečnosť, t. j. čo musí urobiť člen štatutárneho orgánu, aby dodržal podmienky odbornej/náležitej starostlivosti, napr. pri výbere externého manažéra kybernetickej bezpečnosti,
- zmluvnej pokuty pre nedodržanie povinností v oblasti kybernetickej bezpečnosti,¹⁹
- povinnosti mlčanlivosti nad rámec § 12 ZoKB,²⁰
- ďalšie.

Príkladom špecifikácie rozsahu práv a povinností štatutárneho orgánu a jeho úlohy pri zabezpečovaní kybernetickej bezpečnosti v rámci zmluvy o výkone funkcie člena štatutárneho orgánu je táto zmluvná klauzula:

1. *Hlavnými úlohami štatutárneho orgánu v oblasti kybernetickej bezpečnosti je zabezpečiť najmä:*
 - *ochranu všetkých informačných aktív,*
 - *funkčnosť bezpečnostného výboru,*
 - *podporu plnenia úloh kybernetickej bezpečnosti presadzovaním bezpečnostnej stratégie kybernetickej bezpečnosti, politik, smerníc a ďalších interných predpisov súvisiacich s informačnou a kybernetickou bezpečnosťou,*
 - *podporu kybernetickej bezpečnosti prostredníctvom vyčlenenia dostatočného objemu finančných prostriedkov určených na zabezpečenie plnenia úloh kybernetickej bezpečnosti,*
 - *súladi so zákonom o kybernetickej bezpečnosti a súvisiacimi vykonávacími predpismi,*
 - *súladi s ďalšími právnymi predpismi obsahujúcimi element informačnej a kybernetickej bezpečnosti,*

¹⁸ K tomu pozri bližšie pozri PINTÉROVÁ, Dominika: *Časť 8.7.1 Právny vzťah medzi spoločnosťou a členmi orgánov spoločnosti v kontexte zmluvy o výkone funkcie*. In MAMOJKA, Mojmir a kol.: *Obchodné právo I (všeobecná časť, súťažné právo, právo obchodných spoločností a družstvá)*. Bratislava: C. H. Beck, 2021. s. 283 - 293.

¹⁹ Napríklad nasledovne: *Zmluvné strany sa dohodli, že v prípade, ak člen štatutárneho orgánu poruší ktorúkoľvek povinnosť uvedenú v ods. 1 tohto článku, zaväzuje sa zaplatiť zmluvnú pokutu vo výške Eur (slovom Eur).*

²⁰ § 12 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

- kontrolu dodržiavania pravidiel kybernetickej bezpečnosti.
- 2. Povinnosti z vyššie uvedených hlavných úloh môžu byť delegované na jednotlivé organizačné útvary podľa kompetencií a zodpovedností stanovenými v organizačnom poriadku.
- 3. Na zabezpečenie dohľadu nad dodržiavaním kybernetickej bezpečnosti štatutárny orgán zriadi bezpečnostný výbor.
- 4. V procese implementácie požiadaviek zákona o kybernetickej bezpečnosti a súvisiacich vykonávacích predpisov štatutárny orgán môže vymenovať manažéra kybernetickej a informačnej bezpečnosti, ktorému špecifikuje v zmluve povinnosti a právomoci súvisiace s definovaním, udržiavaním a dodržiavaním kybernetickej bezpečnosti v rámci spoločnosti.

Delegácia pôsobnosti v oblasti kybernetickej bezpečnosti na kvalifikovaného odborníka – zmluvné špecifiká

Vertikálna delegácia pôsobnosti štatutárneho orgánu v časti kybernetickej bezpečnosti na nižšie stupne riadenia je **pripustná**,²¹ dokonca je požiadavka určenia manažéra kybernetickej bezpečnosti explicitne uvedená v § 20 ods. 4 písm. a) ZoKB ako aj v § 5 písm. a) vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.²² Úlohou členov štatutárneho orgánu je však nastaviť pravidlá takej delegácie, a následne aj kontroly, pri jasne vymedzených úlohách v rámci nižších stupňov organizačnej štruktúry spoločnosti.²³ Tu je kľúčová predovšetkým **povinnosť s manažérom kybernetickej bezpečnosti uzatvoriť zmluvu**, v rámci ktorej sa upravujú práva a povinnosti, zodpovednosť manažéra kybernetickej bezpečnosti. Druh kontraktu sa diferencuje podľa toho či pôjde o interného alebo externého manažéra kybernetickej bezpečnosti.

- **Interný manažér kybernetickej bezpečnosti** (zamestnanec) má tieto povinnosti upravené v štandardnej pracovnej zmluve, resp. dodatku k tejto zmluve,

²¹ Vo všeobecnosti k vertikálnej delegácii pozri PATAKYOVÁ, Mária – DURAČINSKÁ, Jana: *III. Časť správa, riadenie a kontrola. 1. kapitola Tvorba vôle v spoločnosti. 1.1 Obchodné vedenie*. In PATAKYOVÁ, Mária - ĎURICA, Milan - HUSÁR, Ján a kol.: *Aplikované právo obchodných spoločností a družstvá – ťažiskové inštitúty*. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2021. s. 218.

²² NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: Manažér kybernetickej bezpečnosti. s. 1. Dostupné na: https://cybercompetence.sk/wp-content/uploads/dokumenty/na_stiahnutie/letak_manazer_KB_A4.pdf

²³ Manažér kybernetickej bezpečnosti má mať možnosť komunikovať a predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu. V komplikovaných a rozsiahlych organizačných štruktúrach by sa mala procesne upraviť právomoc priameho prístupu ku štatutárnemu orgánu, napríklad interným predpisom.

napríklad je nutné doplniť povinnosť zachovať mlčanlivosť (o čom a ako dlho po ukončení pracovného pomeru).

- **Externý manažér kybernetickej bezpečnosti** – inomínatna zmluva v zmysle § 269 ods. 2 OBZ, najčastejšie nazvaná *Zmluva o poskytovaní služieb v oblasti kybernetickej bezpečnosti*, v ktorej treba presne sformulovať čo a v akom rozsahu sa bude od neho požadovať a za akých podmienok.

Na tomto mieste je nevyhnutné konštatovať, že právnymi predpismi sú určené iba základné rámce, resp. minimálne požiadavky, kladené na manažéra kybernetickej bezpečnosti, preto je nevyhnutné jeho práva a povinnosti presne špecifikovať v zmluve. Za hlavné úlohy *manažéra kybernetickej bezpečnosti* možno považovať nasledovné: riadenie kybernetickej bezpečnosti v organizácii, riadenie a koordinácia bezpečnostného procesu, primeraná kvalifikácia a dostatočné podmienky na jej zvyšovanie, dostatočné zdroje k dispozícii, v prípade potreby možnosť podávať správy/hlásenia priamo štatutárnemu orgánu spoločnosti, zapojenie v počiatočnej fáze rozsiahlych projektov, ako napr. zavedenie novej aplikácie alebo IT systému.²⁴²⁵ Delegovanie pôsobnosti nemá vplyv na zodpovednosť člena štatutárneho orgánu, ktorý je v prípade delegovania pôsobnosti povinný kontrolovať plnenie zverených úloh (*culpa in eligendo*).²⁶ V tejto súvislosti poukazujeme aj na rozsudok Najvyššieho súdu Českej republiky, sp. zn. 27 Cdo 90/2019, zo dňa 30. 9. 2019, ktorý judikoval, že **ak sa štatutárny orgán rozhodne časť svojej pôsobnosti delegovať, mal by pamätať na nasledujúce dôležité povinnosti a zodpovednosti**

- a) **zodpovednosť za výber** – pri výbere tretej osoby musí postupovať starostlivo a uskutočniť výber aspoň na takej úrovni, ako by výber uskutočnila iná rozumne starostlivá osoba;
- b) **zodpovednosť za zadanie, vedenie a súčinnosť** – musí vybranej osobe zadefinovať zadanie jasne a zrozumiteľne, poskytnúť všetku potrebnú súčinnosť a dávať jej pokyny a informácie;
- c) **zodpovednosť za kontrolu** – musí byť schopný dodaný výsledok delegovanej pôsobnosti primerane kontrolovať a rozumne vyhodnocovať, a to nielen osobne, ale aj za pomoci riadne nastavených kontrolných mechanizmov.²⁷

²⁴ MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE: *Povinnosti správcu ISVS v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich naplňaní*. s. 4. Dostupné na: https://mirri.gov.sk/wp-content/uploads/2022/02/KB-K2_3-1-Povinnosti-spravcu-ISVS_ver1.1.pdf

²⁵ NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Manažér kybernetickej bezpečnosti*. s. 3. Dostupné na: https://cybercompetence.sk/wp-content/uploads/dokumenty/na_stiahnutie/letak_manazer_KB_A4.pdf

²⁶ PATAKYOVÁ, Mária – DURAČINSKÁ, Jana: *III. Časť správa, riadenie a kontrola. 1. kapitola Tvorba vôle v spoločnosti. 1.1 Obchodné vedenie*. In PATAKYOVÁ, Mária - ĎURICA, Milan - HUSÁR, Ján a kol.: *Aplikované právo obchodných spoločností a družstva – ťažiskové inštitúty*. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2021. s. 218.

²⁷ Rozsudok Najvyššieho súdu Českej republiky zo dňa 30. 9. 2019, sp. zn. 27 Cdo 90/2019.

Zodpovednosť za škodu štatutárnych orgánov v oblasti kybernetickej bezpečnosti

Predpokladom zodpovednosti je porušenie povinnosti, ktorá môže byť

a) *zmluvná* (napr. prekročenie zmluvne dohodnutých povinností v oblasti kybernetickej bezpečnosti)

b) *zákonná* (napr. povinnosti špecifikované v zákone o kybernetickej bezpečnosti *lex specialis*) zodpovednosť členov štatutárneho orgánu za porušenie povinností = zodpovednosť za škodu podľa Obchodného zákonníka. tzv. objektívna = vzniká bez ohľadu na to, či došlo k zavineniu zo strany člena orgánu - § 373 Obchodného zákonníka.

K **zákonným podmienkam pre vznik zodpovednosti člena štatutárneho orgánu za škodu** patria:

1. **Porušenie zmluvnej alebo zákonnej povinnosti, respektíve porušenie odbornej/náležitej starostlivosti.**²⁸
2. **Vznik škody.**
3. **Príčinná súvislosť medzi porušením povinnosti a vznikom škody.**

Tieto zákonné podmienky musia byť naplnené kumulatívne, inak by nedošlo ku vzniku zodpovednosti za škodu. Spoločnosť uplatňujúca nárok na náhradu škody bude voči členovi štatutárneho orgánu preukazovať vznik škody spôsobenej porušením povinnosti člena štatutárneho orgánu, príčinnú súvislosť medzi vznikom škody a porušením povinnosti člena štatutárneho orgánu, pričom porušenie povinnosti člena štatutárneho orgánu konať s odbornou/náležitou starostlivosťou a v súlade so záujmami spoločnosti je zákonom predpokladané a dôkaz opaku je na

²⁸ Demonštratívny výpočet OBZ uvádza pri jednotlivých typoch spoločností nasledovné porušenia povinností:

Pri spoločnosti s ručením obmedzeným najmä § 135a ods. 2 Obchodného zákonníka:

- poskytnutie plnenia spoločníkom v rozpore s Obchodným zákonníkom
- nadobudnutie majetku v rozpore s § 59a

Pri akciovej spoločnosti najmä § 194 ods. 6 Obchodného zákonníka:

- poskytnutie plnenia akcionárom v rozpore s Obchodným zákonníkom
- nadobudnutie majetku v rozpore s § 59a
- poskytnutie plnenia v rozpore s § 196a
- upísanie, nadobudnutie alebo prevzatie do zálohu vlastných akcií alebo akcií inej spoločnosti v rozpore s Obchodným zákonníkom
- vydanie akcií v rozpore s Obchodným zákonníkom
- nezverejnenie výročnej správy a konsolidovanej výročnej správy

Súkromnoprávnu zodpovednosť v oblasti kybernetickej bezpečnosti nachádzame napríklad v ustanovení § 19 ods. 8 zákona o kybernetickej bezpečnosti. Podľa tohto ustanovenia prevádzkovateľ základnej služby „*nezodpovedá za škodu, ktorá vznikne inému subjektu obmedzením kontinuity základnej služby pri riešení kybernetického bezpečnostného incidentu. Za škodu spôsobenú obmedzením kontinuity činnosti kybernetickým bezpečnostným incidentom plnením povinnosti spôsobom podľa predchádzajúcej vety zodpovedá úrad.*“.)

členovi štatutárneho orgánu, ktorý musí preukázať, že konal s odbornou/náležitou starostlivosťou a v dobrej viere, že konal v súlade so záujmami spoločnosti.²⁹

Člen štatutárneho orgánu podľa § 135a ods. 3 OBZ (§ 194 ods. 7 OBZ) **nezodpovedá za škodu**, ak preukáže niektorý z nižšie uvedených dôvodov, že:

1. **postupoval pri výkone svojej pôsobnosti s odbornou starostlivosťou a v dobrej viere, že koná v záujme spoločnosti.**³⁰ Samotné preukázanie odbornej spôsobilosti pri postupe člena štatutárneho orgánu ešte nepostačuje na záver, že člen štatutárneho orgánu za vzniknutú škodu nezodpovedá. Vyžaduje sa, aby bola splnená aj ďalšia požiadavka, a to postup člena štatutárneho orgánu v dobrej viere, že koná v záujme spoločnosti. Dobrá viera (*bona fide*), že konanie je v prospech obchodnej spoločnosti je psychickou kategóriou a súčasne liberačným dôvodom vylučujúcim zodpovednosťnú sankciu. Dobrú vieru je treba odlišovať od zavinenia. Na rozdiel od zavinenia, pri ktorom sa posudzuje subjektívny vzťah toho kto koná k výsledku jeho správania, predstavuje dobrá viera objektivizovaný stav nevedomosti. Dobrá viera je definovaná ako „*nezavinená nevedomosť o právnych nedostatkoch určitého právneho stavu*“.³¹ Nestačí pritom len nevedomosť člena štatutárneho orgánu, ale vyžaduje sa pozitívne vnútorne vyargumentované presvedčenie člena štatutárneho orgánu, že koná v záujme obchodnej spoločnosti. V zásade je možné konštatovať, že v dobrej viere nekonal člen štatutárneho orgánu, ktorý rozpoznal (vedel), s ohľadom na všetky relevantné skutočnosti mal rozpoznať (vedieť) alebo mohol rozpoznať (vedieť), že dochádza k porušeniu záujmov spoločnosti.
2. **vykonával uznesenie valného zhromaždenia**, to však neplatí, ak je uznesenie v rozpore so zákonom, spoločenskou zmluvou, stanovami alebo, ak ide o povinnosť podať návrh na vyhlásenie konkurzu.

Osoba v postavení člena štatutárneho orgánu sa zbaví zodpovednosti za škodu, ak preukáže, že porušenie povinnosti bolo spôsobené **okolnosťou vis maior**³², ktorú

²⁹ BARKOCI, Stanislav - BLAHA, Marián - GRAMBLIČKOVÁ, Barbora: § 135a ObZ [Zodpovednosť pri výkone funkcie]. In PATAKYOVÁ, Mária a kol.: *Obchodný zákonník. Komentár*. 1. vydanie. Bratislava: C. H. Beck, 2022. s. 671 – 679.

³⁰ Obe podmienky musia byť naplnené súčasne, ale existuje uznesenie Najvyššieho súdu Slovenskej republiky zo dňa 19. 2. 2009, sp. zn. 1 Obo 16/2008, ktoré judikovalo, že: „Zodpovednosti za škodu sa môže konateľ zbaviť preukázaním aspoň jedného z liberačných dôvodov uvedených v ods. 3.“

³¹ HURDÍK, Ján – FIALA, Josef – HRUŠÁKOVÁ, Milana: *Úvod do soukromého práva*. Brno: Masarykova univerzita, 2002, s. 94.

³² Vo všeobecnosti je vyššia moc, označovaná aj ako *force majeure*, *vis maior* alebo *Acts of God* a obvykle považovaná za okolnosť, ktorá nastala nezávisle od vôle člena štatutárneho orgánu. Takéto okolnosti môžu mať pôvod v prírodných udalostiach (napr. zemetrasenia, povodne, sopečné výbuchy, tsunami, požiar, povodeň, blesk, krupobitie, silný vietor, veterná smršť, snehová víchrica, extrémny mráz) alebo vo faktickom chovaní ľudí, za ktoré povinná strana nenesie a ani nemôže niesť

nemohla predvídať ani odvrátiť. Člen štatutárneho orgánu sa v prípade vzniku škody z kybernetického incidentu môže dovolávať vyššej moci, ak sú kumulatívne naplnené dve obligatórne podmienky, a to, že je:

1. okolnosť pri všetkej starostlivosti **nepredvídateľná** a
2. okolnosť pri všetkom úsilí **neodvratiteľná**.

Ad 1.) Nepredvídateľnosť znamená, že nebolo možné ani pri všetkej starostlivosti predvídať predmetnú okolnosť. To, že sa plnenie povinností člena štatutárneho orgánu stalo obtiažnejším ho nezbavuje zodpovednosti, nakoľko je povinný postupovať v súlade s odbornou/náležitou starostlivosťou a zásadou lojality.

Ad 2.) Druhou podmienkou je **neodvratiteľnosť**, že pri všetkom maximálne možnom úsilí nebolo možné danú okolnosť odvrátiť.

V kontexte § 135a ods. 4 OBZ, § 194 ods. 8 OBZ **sú zakázané akékoľvek dohody medzi spoločnosťou a členom štatutárneho orgánu vylučujúce alebo obmedzujúce zodpovednosť člena štatutárneho orgánu**; spoločenská zmluva ani stanovy nemôžu obmedziť alebo vylúčiť zodpovednosť konateľa/stanovy nemôžu obmedziť alebo vylúčiť zodpovednosť člena predstavenstva.³³ V prípade uzatvorenia takejto dohody, ktorou by sa vylúčila alebo obmedzila zodpovednosť člena štatutárneho orgánu by išlo o absolútne neplatný právny úkon pre jeho rozpor so zákonom.³⁴ Otázka znie, či by bolo možné sa na vylúčení alebo obmedzení zodpovednosti člena orgánu dohodnúť v zmluve o výkone funkcie. Podľa nášho názoru to možné nie je a v prípade, ak by k takejto dohode v zmluve o výkone funkcie došlo išlo by o neplatný právny úkon pre jeho rozpor so zákonom.³⁵ Obmedzenie zodpovednosti za škodu je teda zakázané (podľa 135a ods. 4., 194 ods. 8. OBZ) existuje však možnosť vzdať sa náhrady škody alebo uzatvoriť dohodu o urovaní medzi spoločnosťou a členom štatutárneho orgánu za nasledovných podmienok:

a) uplynú 3 roky

zodpovednosť (napr. vojny, štrajky, občianske nepokoje, sabotáže). Medzi ďalšie typické okolnosti vyššej moci patria revolúcie, teroristické útoky, epidémie nad/národného charakteru, výpadky energie v dôležitých veľkomestách, výpadky dodávok ropy, obchodné, menové, politické, prípadne iné opatrenia orgánov verejnej moci, atď.

³³ § 135a ods. 4, § 194 ods. 8 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

³⁴ BARKOCI, Stanislav - BLAHA, Marián - GRAMBLIČKOVÁ, Barbora: § 135a ObZ [Zodpovednosť pri výkone funkcie]. In PATAKYOVÁ, Mária a kol.: *Obchodný zákonník. Komentár*. 1. vydanie. Bratislava: C. H. Beck, 2022, s. 677.

³⁵ Rovnako MAMOJKA, Mojmir: § 135a ObZ [Zodpovednosť pri výkone funkcie]. In MAMOJKA, Mojmir a kol.: *Obchodný zákonník – Veľký komentár*. 1. zväzok. Bratislava: Eurokódex, 2016. s. 542 „spoločnosť sa nemôže s konateľom dohodnúť na vylúčení alebo obmedzení zodpovednosti pred tým, než mu táto zodpovednosť vznikne, a to prostredníctvom žiadnej obvyklej platformy - dojednanie o vylúčení alebo obmedzení zodpovednosti konateľa vo vzťahu k spoločnosti je neplatné bez ohľadu na to, či je obsiahnuté v samotnom vyhlásení spoločnosti, v inominatej zmluve uzavretej medzi spoločnosťou a konateľom, prípadne v spoločenskej zmluve alebo stanovách.“

b) súhlas valného zhromaždenia a nie je vznesený protest minoritným spoločníkom/akcionárom.

V prípade manažérov kybernetickej bezpečnosti sa neuplatňuje § 135a ods. 4 OBZ, § 194 ods. 8 OBZ a teda z hľadiska formulácie zodpovednosti a limitácie škody ich zmluvy (najmä inomínatna zmluva v zmysle § 269 ods. 2 OBZ, najčastejšie nazvaná *Zmluva o poskytovaní služieb v oblasti kybernetickej bezpečnosti*) často obsahujú určitú formu obmedzenia zodpovednosti, predovšetkým obmedzenie zodpovednosti konkrétnou sumou (napr. 10 000 Eur)³⁶ alebo inú formu obmedzenia zodpovednosti.

Záver

Výsledkom analýzy je zistenie, že kybernetická bezpečnosť sa stáva neoddeliteľnou súčasťou výkonu funkcií najmä členov štatutárnych orgánov. Je nepochybné, že je kladený vyšší dôraz v oblasti kybernetickej bezpečnosti na členov štatutárnych orgánov, pričom sa vyskytuje **interdisciplinárny prístup k právnej regulácii**, úprave práv a povinností ako i zodpovednosti, kde **zákon o kybernetickej bezpečnosti predstavuje právny predpis *lex specialis* a Obchodný zákonník právny predpis *lex generalis***. To prináša do budúcnosti otázku ohľadom presahu povinností podľa verejnoprávnych predpisov do obchodnoprávnych vzťahov, teda či **je potrebné, aby všetky subjekty súkromného práva reflektovali ZoKB alebo len tie, ktoré sú výslovne vymedzené zákonom?**

Prečo však nadobúdajú povinnosti v oblasti kybernetickej bezpečnosti takýto dôležitý rozmer? Podľa nášho názoru podcenenie môže viesť k významným ekonomickým, reputačným³⁷ aj právnym dôsledkom i vzniku škody. V obchodnom práve sa tak čoraz častejšie objavuje požiadavka regulácie kybernetických rizík prostredníctvom zmluvných klauzúl či už v zakladateľských dokumentoch, interných predpisoch, ako i zmluve o výkone funkcie.

Zmluvné strany si dojednávajú špecifické bezpečnostné štandardy ohľadom rozsahu práv a povinností štatutárneho orgánu a jeho úlohy pri zabezpečovaní kybernetickej bezpečnosti, možnosti delegácie na interných/externých odborníkov – manažérov kybernetickej bezpečnosti, odbornej/náležitej starostlivosti v nadväznosti na kybernetickú bezpečnosť, zmluvnej pokuty pre nedodržanie povinností v oblasti kybernetickej bezpečnosti, povinnosti mlčanlivosti nad rámec § 12 ZoKB, povinnosti

³⁶ Takáto formulácia obmedzenia zodpovednosti bola reálne využitá v *Zmluve o poskytovaní služieb v oblasti kybernetickej bezpečnosti* dostupnej na: <https://www.crz.gov.sk/data/att/5805764.pdf?csrt=1542131616912248691>

³⁷ LING, Shixian - LIU, Zhangxin (Frank) - XIA, Hui: *Code, Control, and Cybersecurity: How Board it Expertise Shapes Corporate Risk Management*. August 2025. p. 8. Available at SSRN: <https://ssrn.com/abstract=5394247> or <http://dx.doi.org/10.2139/ssrn.5394247>

v prípade incidentu, mechanizmy oznamovania a zodpovednosti za škodu spôsobenú kybernetickým útokom.

Zhrnutím možno konštatovať, že kybernetická bezpečnosť dnes nie je len technologickou výzvou, ale aj novým rozmerom zodpovednosti členov orgánov obchodných spoločností, ktorý vyžaduje multidisciplinárny prístup, prevenciu, pravidelnú aktualizáciu vedomostí a odvahu reagovať na meniace sa kybernetické riziká v prospech stability a dôvery v meniace sa obchodné prostredie v digitálnej ére.

Zoznam použitej literatúry

1. DURAČINSKÁ, Jana: *Povinnosť starostlivosti riadneho hospodára alebo povinnosť odbornej starostlivosti z hľadiska právnej komparatistiky*. In Dny práva – 2012 – Days of Law. 6. ročník mezinárodnej konferencie pořádané Právnickou fakultou Masarykovy univerzity. Sborníky příspěvků. Brno: Masarykova univerzita, 2013. 14 s. Dostupné na: https://www.law.muni.cz/sborniky/dny_prava_2012/files/Bermudskytrojuhelnik/DuracinskaJana.pdf
2. GALE, Megan – BONGIOVANNI, Ivano – SLAPNICAR, Sergeja: *Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead*. In Computers & Security 121(4). July 2022. 38 p. DOI: <https://doi.org/10.1016/j.cose.2022.102840>
3. HURDÍK, Ján – FIALA, Josef – HRUŠÁKOVÁ, Milana: *Úvod do soukromého práva*. Brno: Masarykova univerzita, 2002. 158 s. ISBN 80-210-2976-5.
4. KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI: *Sekcia záväzné metodiky alebo riadenie bezpečnosti*. Dostupné na: <https://cybercompetence.sk/kniznica/>
5. LING, Shixian - LIU, Zhangxin (Frank) - XIA, Hui: *Code, Control, and Cybersecurity: How Board it Expertise Shapes Corporate Risk Management*. August 2025. 43 p. Available at SSRN: <https://ssrn.com/abstract=5394247> or <http://dx.doi.org/10.2139/ssrn.5394247>
6. LIPTON, Martin: *Risk Management and the Board of Directors*, The Harvard Law School Forum on Corporate Governance and Financial Regulation. Published 25. September 2025. Available at: <https://corpgov.law.harvard.edu/2025/09/25/risk-management-and-the-board-of-directors-10/>
7. MAMOJKA, Mojmír a kol.: *Obchodný zákonník – Veľký komentár. 1. zväzok*. Bratislava: Eurokódex, 2016. 1087 s. ISBN 978-80-81550-65-2.
8. MAMOJKA, Mojmír a kol.: *Obchodné právo I (všeobecná časť, súťažné právo, právo obchodných spoločností a družstva)*. Bratislava: C. H. Beck, 2021. 832 s. ISBN 978-80 8232-007-0.

9. MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE: *Povinnosti správcu ISVS v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní*. Dostupné na: https://mirri.gov.sk/wp-content/uploads/2022/02/KB-K2_3-1-Povinnosti-spravcu-ISVS_ver1.1.pdf
10. MRÁZOVÁ, Žofia - HUSÁR, Ján - DOLNÝ, Jaroslav a kol.: *Volené orgány kapitálových spoločností. Vybrané otázky*. Košice: ŠafárikPress, 2021. 210 s. ISBN 978-80-574-0067-7.
11. NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Kyberbezpečnosť ako nové znalecké odvetvie*. Dostupné na: <https://www.nbu.gov.sk/kyberbezpecnost-ako-nove-znalecke-odvetvie/>
12. NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Manažér kybernetickej bezpečnosti*. Dostupné na: https://cybercompetence.sk/wp-content/uploads/dokumenty/na_stiahnutie/letak_manazer_KB_A4.pdf
13. OVEČKOVÁ, Oľga – CSACH, Kristián – ŽITŇANSKÁ, Lucia: *Obchodné právo 2 (Obchodné spoločnosti a družstvo)*, Bratislava: Wolters Kluwer, 2020. 428 s. ISBN 978-80-571-0291-5.
14. PATAKYOVÁ, Mária - ĎURICA, Milan - HUSÁR, Ján a kol.: *Aplikované právo obchodných spoločností a družstva – ťažiskové inštitúty*. 1. vydanie. Bratislava : Wolters Kluwer SR s. r. o., 2021. s. 864 s. ISBN 978-80-571-0363-9.
15. PATAKYOVÁ, Mária a kol.: *Obchodný zákonník. Komentár*. 1. vydanie. Bratislava: C. H. Beck, 2022. 1792 s. ISBN 978-80-8232-018-6.
16. PINTÉROVÁ, Dominika: *K možnosti zavedenia pracovnoprávneho režimu člena orgánu kapitálovej obchodnej spoločnosti v procese rekodifikácie, 1. časť*. In: Justičná Revue, roč. 75, č. 4, 2023, s. 504 – 521.
17. Rozsudok Najvyššieho súdu Českej republiky zo dňa 30. 9. 2019, sp. zn. 27 Cdo 90/2019.
18. Uznesenie Najvyššieho súdu Slovenskej republiky zo dňa 19. 2. 2009, sp. zn. 1 Obo 16/2008.
19. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov („ZoKB“).
20. Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov („OBZ“).
21. Zmluva o poskytovaní služieb v oblasti kybernetickej bezpečnosti dostupná na: <https://www.crz.gov.sk/data/att/5805764.pdf?csrt=1542131616912248691>

Kontaktné údaje

JUDr. Mgr. Dominika Pintérová, PhD.

dominika.pinterova@flaw.uniba.sk

Katedra obchodného práva a hospodárskeho práva

Univerzita Komenského

Právnická fakulta

BEZPEČNOSŤ OBCHODNÉHO TAJOMSTVA V DIGITÁLNOHOM PROSTREDÍ¹

PROTECTING TRADE SECRETS IN THE DIGITAL ENVIRONMENT

Radka Kopčová²

Abstrakt: Obchodné tajomstvá sa v súčasnosti čoraz častejšie využívajú na ochranu tajných a cenných informácií. Tieto cenné, tajné, a často kľúčové nehmotné statky, patriace k podniku, sú dnes uložené a prenášané predovšetkým v *digitálnej* forme, čo kladie na ich ochranu nové nároky v porovnaní s minulosťou. Autorka v príspevku poukazuje na problémy ochrany obchodného tajomstva v súčasnosti, ktoré so sebou priniesla éra digitalizácie informácií. Nedostatočná prevencia, nedostatočné zabezpečenie obchodného tajomstva a neopatrnosť pri manipulácii s ním, obzvlášť v digitálnej ére, môže viesť v zamietnutí právnej ochrany týchto informácií ako obchodného tajomstva zo strany súdu. Autorka analyzuje „zodpovedajúci spôsob“ zabezpečenia utajenia digitálneho obchodného tajomstva, ako hlavný zákonný predpoklad na jeho legálnu ochranu. Primeranosť opatrení na utajenie obchodného tajomstva je možné určiť na základe objektívnych kritérií, ktoré autorka bližšie vymedzuje v príspevku. Autorka zdôrazňuje, že žiaden podnik by nemal strácať nárok na ochranu obchodného tajomstva, pokiaľ nie je v jeho možnostiach zabezpečiť vysoký stupeň jeho ochrany pred neoprávneným získaním, zverejnením alebo sprístupnením v kyberpriestore. Autorka vychádza z národnej (slovenskej), európskej a medzinárodnej právnej úpravy a súvisiacej odbornej literatúry.

Kľúčové slová: obchodné tajomstvo, digitalizácia informácií, porušenie obchodného tajomstva, kybernetická krádež obchodného tajomstva, prevencia, zabezpečenie utajenia obchodného tajomstva.

Abstract: Trade secrets are increasingly used to protect confidential information. These valuable, secret, and often key intangible assets belonging to a company are now stored and transmitted primarily in digital form. This places new demands on their protection compared to the past. In the article,

¹ Tento príspevok vznikol s podporou grantu GAAA/2024/34 s názvom: „Práva majiteľů obchodních jmen a jiných označení k názvu domény na internetu“.

² Ústav súkromného práva, Právnická fakulta Paneurópskej vysokej školy v Bratislave.

the author points out the problems of protecting trade secrets today, which have been brought about by the era of digitalization of information. Insufficient prevention, insufficient security of trade secrets and carelessness in handling them, especially in the digital era, can lead to the rejection of legal protection of this information as a trade secret by the court. The author analyzes the "appropriate method" of ensuring the confidentiality of digital trade secrets as the main legal prerequisite for its legal protection. The adequacy of measures to keep trade secrets secret can be determined on the basis of objective criteria, which the author defines in more detail in the article. The author emphasizes that no company should lose its right to trade secret protection unless it is able to ensure a high level of protection against unauthorized acquisition, publication or disclosure in cyberspace. The research is based on Slovak, European and international legislation and related professional literature.

Key words: trade secrets, digitalization of information, trade secret misappropriation, cyber theft of trade secrets, preventive measures, ensuring the confidentiality of trade secrets.

Úvod

V súčasnej dobe, pre ktorú je príznačný informačný predstih, tvoria informácie cennú komoditu naprieč všetkými odvetviami. Platí to aj pre podnikateľské prostredie. V hospodárskej súťaži podnikatelia a ďalší iní sťažiteľia³ disponujú spravidla takým druhom informácií, ktoré predstavujú určitú konkurenčnú výhodu oproti iným sťažiteľom.⁴ *Obchodné tajomstvá*. Vo všeobecnosti možno obchodné tajomstvo definovať ako všetky skutočnosti (informácie), ktoré sú tajné, ktoré majú svoju ekonomickú hodnotu, pretože sú tajné, ktoré ich držiteľ uchováva v tajnosti, a robí tak tomu zodpovedajúcim spôsobom. Súčasná *digitálna* doba vystavuje

³ Sťažiteľom nemusí byť nevyhnutne len subjekt, ktorý má status podnikateľa. Pozri k tomu: KUBÍČEK, Pavel, a kol: Obchodné právo. 4. vyd. Plzeň: Aleš Čeněk, 2025, s. 74: „*Sťažiteľom je každá osoba, ktorá sa zúčastňuje na hospodárskej súťaži...*“; podľa § 41 Zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (OBZ): „*Fyzické i právnické osoby, ktoré sa zúčastňujú na hospodárskej súťaži, aj keď nie sú podnikateľmi...*“

⁴ Konkurenčná výhoda je všetko to, čím sa sťažiteľ pozitívne odlišuje od iných sťažiteľov (svojich konkurentov) a robí ho nejakým spôsobom lepším alebo v hospodárskej súťaži zaujímavejším oproti iným sťažiteľom. Podľa českej legálnej definície obchodného tajomstva je „konkurenčná významnosť“ jedným zo základných pojmových znakov obchodného tajomstva. Pozri k tomu § 504 NOZ: „*Obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastníci zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.*“ Súčasná slovenská právna úprava nevymedzuje konkurenčnú výhodu obchodného tajomstva ako jeho pojmový znak.

podnikateľov zvýšenému riziku úniku týchto hodnotných informácií, ktoré majú ostať utajené. Obchodné tajomstvá, ako cenné, tajné, a často kľúčové nehmotné statky, patriace k podniku, sú dnes uložené a prenášané predovšetkým v *elektronickej forme*, čo kladie na ich ochranu nové nároky v porovnaní s minulosťou. Krádež obchodného tajomstva kedysi znamenala skôr faktickú krádež alebo kopírovanie fyzického dokumentu alebo predmetu obsahujúceho obchodné tajomstvo. S nárastom využívania digitalizácie informácií sa formy porušenia obchodného tajomstva vo forme jeho neoprávneného získania, sprístupnenia alebo zverejnenia čoraz viac uskutočňujú prostredníctvom nezákonného prístupu k počítačovým sieťam, obsahujúce informácie chránené ako obchodné tajomstvo. Z dôvodu náročnosti dohľadania rušiteľov spôsobujú v súčasnosti takéto kybernetické krádeže obchodných tajomstiev v praxi časté problémy a spôsobujú značné škody.⁵ Podľa štatistiky z roku 2020 predstavovala *kybernetická krádež* obchodných tajomstiev v EÚ straty odhadom 60 miliárd eur.⁶ V tej súvislosti poukazujeme aj na čoraz častejšie využívanie obchodného tajomstva na ochranu tajných a cenných informácií v podnikoch a iných inštitúciách.⁷

V predložennom príspevku v prvom rade vymedzujeme obchodné tajomstvo podľa definičných rámcov európskeho a národného (slovenského) práva. Zvýrazňujeme základné funkcie a atraktivitu využívania inštitútu obchodného tajomstva v súčasnom, najmä podnikateľskom, prostredí, a to aj v porovnaní s niektorými inými obdobnými inštitútmi duševného vlastníctva (konkrétne patenty). Poukazujeme na problémy ochrany obchodného tajomstva v súčasnosti, ktoré so sebou priniesla éra digitalizácie informácií. Potrebu digitalizáciu informácií, vrátane obchodného tajomstva, so sebou prináša aj čoraz častejší trend práce z domu (home office), čo ešte viac skomplikovalo ochranu obchodných tajomstiev. Je to spôsobené tým, že v takýchto modeloch zamestnávania získavajú zamestnanci prístup k údajom svojho

⁵ APLIN, Tanya, RADAUER, Alfred, BADER, Martin, SEARLE, Nicola: The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. In: IIC - International Review of Intellectual Property and Competition Law, č. 54 (2023), s. 826–858. <https://doi.org/10.1007/s40319-023-01325-8>.

⁶ Európska Komisia: Akčný plán duševného vlastníctva na podporu obnovy a odolnosti EÚ (Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Maximálne využitie inovačného potenciálu EÚ - Akčný plán duševného vlastníctva na podporu obnovy a odolnosti EÚ) COM/2020/760 final z 24. 11. 2020 (ďalej len „akčný plán IP“).

⁷ V príspevku budeme súhrnne označovať podniky a iné organizácie, ktoré si chránia informácie ako obchodné tajomstvo ďalej len ako „podniky“, a to aj keď tieto inštitúcie nemusia byť výlučne len podnikateľským subjektom a nemusia tiež vykonávať inú zárobkovú činnosť. (Potvrďuje to dikcia odôvodnenia č. 1 smernice o obchodnom tajomstve, v ktorého prvej vete je uvedené: „*Podniky a neziskové výskumné inštitúcie (...)*“, čiže obchodné tajomstvo sa nemusí vzťahovať bezprostredne na podnik a ani na podnikateľskú alebo zárobkovú činnosť. Ide o rozdiel oproti slovenskej právnej úprave, porovnaj: § 17 ods. 1 a ods. 2 OBZ).

zamestnávateľa na diaľku v digitálnej forme, čo znižuje úroveň kontroly zdieľaných informácií zo strany zamestnávateľa.⁸

V tej súvislosti skúmame otázku bezpečnosti obchodného tajomstva v digitálnom prostredí a analyzujeme odporúčania zainteresovaných orgánov, najmä Európskej komisie a Svetovej organizácie duševného vlastníctva (WIPO). Posudzujeme *prevenciu*, ako kľúčový predpoklad na zachovanie utajenia obchodného tajomstva. Jadrom príspevku je analýza „primeranosti opatrení“ na zachovanie utajenia digitálneho obchodného tajomstva.

Vychádzame z nasledovných hypotéz:

1. Obchodné tajomstvá sa v súčasnosti čoraz častejšie využívajú na ochranu tajných a cenných informácií.
2. Obchodné tajomstvá bývajú v súčasnosti ukladané a prenášané predovšetkým v digitálnej forme, čo kladie na ich ochranu nové nároky v porovnaní s minulosťou.

Východiská: Na význam obchodného tajomstva v digitálnom prostredí poukazuje smernica o obchodnom tajomstve⁹ nasledovne: *„Podniky si bez ohľadu na svoju veľkosť cenia obchodné tajomstvo tak ako patenty a ďalšie formy práva duševného vlastníctva.“*¹⁰ Podľa WIPO: *„S rýchlym rozvojom digitálnych technológií čelia podniky jedinečným výzvam pri ochrane svojich cenných vlastníckych vedomostí a informácií. Zatiaľ čo „tradičné“ stratégie ochrany duševného vlastníctva zamerané na patenty môžu byť v tomto technologickom sektore stále platné, ochrana obchodného tajomstva sa stala jedným z kľúčových režimov ochrany digitálnych technológií.“*¹¹ V odporúčaní Komisie (EÚ) 2024/915 z 19. marca 2024 týkajúce sa opatrení na boj proti falšovaniu a na posilnenie presadzovania práv duševného vlastníctva (odporúčanie EÚ 2024/915) sa poukazuje na nárast porušenia obchodného tajomstva v digitálnom prostredí nasledovne: *„Keďže globálne hospodárstvo sa čoraz viac digitalizuje, riziko neoprávneného nadobúdania, využívania a zverejňovania nezverejneného know-how a obchodných informácií (obchodného tajomstva) prostredníctvom kybernetických útokov narástlo.“*¹² Ako uvádza A. Ubaydullaeva: *„V modernej digitálnej krajine, kde dáta a informácie poháňajú inovácie a hospodársky rast, sa ochrana obchodného*

⁸ Pozri k tomu napr.: KORYCIŇSKA-RZĄDCA, Paulina: Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets against Unauthorised Acquisition, Use and Disclosure by Its Employees? In: Białostockie Studia Prawnicze, roč. 29, č. 2 (2024), s. 163-176.

⁹ Smernica Európskeho parlamentu a Rady (EÚ) 2016/943 z 8. júna 2016 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva). Ďalej len „smernica o obchodnom tajomstve“.

¹⁰ Smernica o obchodnom tajomstve, odôvodnenie č. 1.

¹¹ World Intellectual Property Organization: WIPO Guide to Trade Secrets and Innovation. Geneva: WIPO, 2024. DOI: 10.34667/tind.49735.

¹² Odporúčanie EÚ 2024/915.

tajomstva a know-how stala prvoradou pre podniky, ktoré sa snažia udržať si konkurenčnú výhodu.", a tiež: „Keďže sa spoločnosti čoraz viac spoliehajú na proprietárne znalosti, procesy a digitálne aktíva, aby sa odlíšili, je ochrana týchto nehmotných aktív pred zneužitím a neoprávneným zverejnením kľúčová.“¹³ Podľa výskumu Gyurásza, Hamuláka a Dražovej, sa „začali objavovať prípady týkajúce sa zneužívania technológií a neúmyselného zverejnenia informácií.“¹⁴ Problém zabezpečenia bezpečnosti obchodného tajomstva v digitálnom prostredí je odôvodnený v smernici o obchodnom tajomstve nasledovne: „Inovujúce podniky sú vo vnútri Únie alebo mimo nej čoraz častejšie vystavované nekalým praktikám zameraným na zneužívanie obchodného tajomstva, ako sú krádež, neoprávnené kopírovanie, hospodárska špionáž alebo porušenie požiadaviek na dôvernosť. K zvyšovaniu rizika výskytu uvedených praktík prispieva najnovší vývoj, ako je globalizácia, častejší outsourcing, dlhšie dodávateľské reťazce, a zvýšená miera používania informačných a komunikačných technológií. Neoprávnené získanie, využitie alebo sprístupnenie obchodného tajomstva ohrozuje schopnosť oprávneného vlastníka obchodného tajomstva získať výnosy vyplývajúce z výsledkov jeho inovačného úsilia ako pôvodcu. Bez účinných a porovnateľných právnych prostriedkov ochrany obchodného tajomstva v celej únii sa znižuje motivácia zapájať sa do cezhraničnej inovačnej činnosti na vnútornom trhu a obchodné tajomstvo nedokáže naplniť svoj potenciál ako hybnej sily hospodárskeho rastu a vytvárania pracovných miest. Brzdia sa tak inovácie a tvorivosť a znižujú sa investície, a tak sa negatívne ovplyvňuje hladké fungovanie vnútorného trhu a oslabuje jeho rastový potenciál.“ Zo slovenských autorov sa skúmanou problematikou zatiaľ nikto špecifickejšie nezaoberal. Veríme, že poukázanie na problematiku bezpečnosti obchodného tajomstva v digitálnom prostredí a hľadanie ideálnych riešení na eliminovanie kybernetických krádeží obchodných tajomstiev bude prínosné pre právnu teóriu ako aj pre prax, a nastolí súvisiace otázky na ďalší výskum.

Obchodné tajomstvo a jeho digitalizácia

Pokiaľ ide o právo EÚ, pojmové vymedzenie obchodného tajomstva je obsiahnuté v ustanovení čl. 2 ods. 1 smernice o obchodnom tajomstve nasledovne:

„obchodné tajomstvo“ sú informácie, ktoré spĺňajú všetky tieto požiadavky:

¹³ UDAYDULLAEVA, Anna: Know-How and Trade Secrets in Digital Business. In: International Journal of Law and Policy, Roč. 2, č. 3 (2024). s. DOI: 10.59022/ijlp.162.

¹⁴ GYURÁSZ, Zoltán, HAMULÁK, Ondrej, DRAŽOVÁ Petra: A proactive approach to legal privilege in the light of electronic communication. In: TalTech Journal of European Studies, Roč. 15, č. 1 (2025), s. 83-105.

- a) sú tajné v tom zmysle, že nie sú ako celok alebo pri presnom usporiadaní a spojení ich častí všeobecne známe alebo bežne prístupné osobám v kruhoch, ktoré sa dotknutým druhom informácií bežne zaoberajú;
- b) majú obchodnú hodnotu, pretože sú tajné;
- c) osoba, ktorá s týmito informáciami oprávnené nakladá, podnikla za daných okolností primerané kroky, aby ich udržala v tajnosti;

Na Slovensku je základná súkromnoprávna úprava obchodného tajomstva obsiahnutá v Obchodnom zákonníku, v ktorom zákonodarca vymedzuje obchodné tajomstvo ako jeden z predmetov práv patriace k podniku.¹⁵ Podľa § 17 ods. 1 OBZ: *„Predmetom práv patriacich k podniku je aj obchodné tajomstvo. Obchodné tajomstvo tvoria všetky skutočnosti obchodnej, výrobnjej alebo technickej povahy súvisiace s podnikom, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle majiteľa obchodného tajomstva utajené a majiteľ obchodného tajomstva zodpovedajúcim spôsobom ich utajenie zabezpečuje.“*

Vo všeobecnosti možno obchodné tajomstvo definovať ako všetky skutočnosti (informácie), ktoré sú tajné, ktoré majú svoju ekonomickú (komerčnú) hodnotu, pretože sú tajné, ktoré ich držiteľ uchováva v tajnosti, a robí tak tomu zodpovedajúcim spôsobom.¹⁶ V praxi môže ísť o rôzne výrobné alebo technologické postupy, receptúry a zloženia výrobkov, obchodné stratégie, formy komunikácie so zákazníkmi, obchodnými partnermi, formy marketingu a reklamné plány, rôzne technické návody, plány, riešenia, zásady finančného riadenia podniku, zásady cenotvorby, dokonca aj algoritmy, ktoré sa využívajú v podniku, a mnohé ďalšie iné informácie, ktoré pre majiteľa¹⁷ týchto informácií predstavujú cenné údaje,

¹⁵ K podniku patria veci, práva a iné majetkové hodnoty, ktoré patria podnikateľovi a slúžia na prevádzkovanie podniku alebo vzhľadom na svoju povahu majú tomuto účelu slúžiť. Podľa vymedzeného triedenia troch elementárnych zložiek podniku býva obchodné tajomstvo podľa zaužívaného právneho názoru zaraďované k zložkám nehmotnej povahy, ktoré tvoria práva a iné majetkové hodnoty. Pozri napr.: KOUKAL, Pavel: Obchodní tajemství v novém občanském zákoníku. In: Časopis pro právní vědu a praxi, Brno, č. 21 (2013), s. 467-475; OVEČKOVÁ, Oľga. a kol.: Obchodný zákonník. Veľký komentár, II. zväzok, druhé vydanie. Bratislava: Wolters Kluwer, 2022, s. 234.

¹⁶ KOPČOVÁ, Radka: Trade secret: a significant legal institution in business and its legal regulation across selected European countries (including case law). In: Central and Eastern European Legal Studies. Atény: European Public Law Organization, č. 2 (2024), s. 241-277. ISSN 2310-2705.

¹⁷ V predloženom príspevku označujeme subjekt, ktorý oprávnené nakladá s obchodným tajomstvom, ako „majiteľ“ obchodného tajomstva. Takéto označenie je v súlade s § 17 ods. 2 OBZ, podľa ktorého *„Majiteľ obchodného tajomstva je fyzická osoba alebo právnická osoba, ktorá oprávnené nakladá s obchodným tajomstvom, ktoré sa vzťahuje na podnik prevádzkovaný touto osobou pri výkone podnikania podľa § 2 ods. 1.“* Porovnaj: V smernici o obchodnom tajomstve sa v čl. 2 ods. 2 takáto osoba označuje ako „vlastník“ obchodného tajomstva; dohoda TRIPS (čl. 39 ods. 2) obsahuje pojem „držiteľ“ nezverejnených informácií (z angl. „the person lawfully in control of the information“). Na teoreticko-

informácie alebo *know-how* (z angl. vedieť-ako), a ktoré po naplnení pojmových znakov môžu tvoriť obchodné tajomstvo. Obchodné tajomstvo v praxi často slúži aj ako náhrada alebo doplnok k patentovej ochrane.¹⁸ Na rozdiel od patentov, ktoré sú registrovanými právami, sú však obchodné tajomstvá len také silné, aké sú kontroly, ktoré sa na ich zabezpečenie použijú. V tom spočíva ich zásadný význam a zároveň najväčší rozdiel oproti patentom.

S nástupom digitálnych technológií a ich rýchleho rozvoja vo všetkých podnikoch bez ohľadu na ich veľkosť alebo zameranie sa informácie, vrátane tých, ktoré tvoria obchodné tajomstvá, už poväčšine *digitalizujú* a tiež sú *uložené a prenášané v digitálnej forme*. Preto konštatujeme, že podniky čelia novým výzvam pri ochrane svojich cenných informácií. Zatiaľ čo v minulosti sa takéto cenné a tajné informácie ukladali skôr fakticky a primerané opatrenia, ktoré vykonával majiteľ obchodného tajomstva na jeho zachovanie v tajnosti, spočívali spravidla v jeho fyzickom utajení (napríklad sa obchodné tajomstvá ukladali v trezoroch, v uzamknutých pracovných stoloch a kanceláriách)¹⁹, v digitálnej ére je zachovanie utajenia obchodného tajomstva pre podniky náročnou výzvou.

Boom cloudových úložísk, elektronickej komunikácie, pokročilej analýzy údajov a rozsiahlych jazykových modelov spôsobil v podnikoch na jednej strane jednoduché a praktické ukladanie, prenos, replikáciu, či výpočet informácií. Na druhej strane práve tieto novodobé výdobytky techniky zvyšujú riziko porušenia obchodného tajomstva vo forme jeho neoprávneného získania, sprístupnenia a zverejnenia, a to v dôsledku jednoduchosti, s akou sa digitálne údaje dajú kopírovať, zdieľať a šíriť. V minulosti preto porušenie obchodného tajomstva spočívalo najmä v jeho *faktickej (fyzickej) krádeži*, či už zo strany zamestnancov, spoločníkov alebo iných osôb, ktoré mali často prístup k týmto informáciám (napríklad faktická krádež alebo kopírovanie fyzického dokumentu alebo predmetu obsahujúceho obchodné tajomstvo). Naopak, s nárastom využívania digitalizácie informácií sa formy porušenia obchodného tajomstva vo forme jeho neoprávneného získania, sprístupnenia alebo zverejnenia čoraz viac uskutočňujú prostredníctvom nezákonného prístupu k počítačovým sieťam, obsahujúce informácie chránené ako obchodné tajomstvo. V tejto súvislosti

aplikačné problémy pokiaľ ide o nejednoznačné vymedzenie týchto pojmov poukazujeme v samostatnom príspevku.

¹⁸ Podľa prieskumu uskutočnenému vo Veľkej Británii sa však vo väčšine prípadov obchodného tajomstvá vzťahujú skôr na nepatentovateľné inovácie, ako sú napríklad marketingové alebo organizačné inovácie. Pozri: SEARLE, Nicola: The Economic and Innovation Impacts of Trade Secrets. Technical Report. UK IPO, London, 2021. [Report] <https://research.gold.ac.uk/id/eprint/30022>.

¹⁹ Takéto spôsoby ochrany obchodných tajomstiev zo strany majiteľov sa príkladmo uvádzajú v súvisiacej odbornej literatúre a tiež v komentároch k ObchZ. Pozri napr.: PATAKYOVÁ a kol. Obchodný zákonník, 1. vydanie, 2022, s. 232;

sa používa pojem *kybernetická krádež obchodných tajomstiev a kybernetická špionáž*.²⁰

V súvislosti s bezpečnosťou obchodného tajomstva v digitálnom prostredí je potrebné rozlišovať dve roviny ochrany obchodného tajomstva:

1. **Digitálny údaj, ktorý je sám o sebe obchodným tajomstvom** (v textovom, zvukovom alebo obrazovom formáte), napríklad zdrojový kód, algoritmus²¹;
2. **Digitálny objekt, v ktorom je obchodné tajomstvo uložené**, napríklad technologický postup uložený v digitálnom súbore.

Aby mohli obe formy digitálnych údajov (objektov) požívať *právnú*²² ochranu obchodného tajomstva, musia tieto informácie kumulatívne napĺňať už uvedené, zákonom vymedzené, predpoklady.²³ To znamená, tieto informácie musia byť:

1. tajné²⁴,
2. komerčne cenné, pretože sú tajné,
3. ich majiteľ ich uchováva v tajnosti, a robí tak tomu zodpovedajúcim spôsobom.

Prevenia a zabezpečenie „utajenia“ digitálneho obchodného tajomstva

V digitálnom veku predstavuje ochrana digitálneho obchodného tajomstva výzvy, najmä pokiaľ ide o zraniteľnosť voči kybernetickej krádeži, kybernetickým útokom a únikom údajov, a to nie len zo strany tretích osôb, ale aj z radu vlastných zamestnancov, obchodných partnerov, spoločníkov a ďalších osôb. Ešte viac komplikuje ochranu obchodných tajomstiev súčasný častý trend práce z domu (home office). Je to spôsobené tým, že v takýchto modeloch zamestnávania získavajú zamestnanci (prípadne aj iné osoby, ktoré sú vo vzťahu k majiteľovi obchodného tajomstva v inom ako zamestnaneckom pomere) prístup k údajom na

²⁰ Kybernetická špionáž zahŕňa úmyselné aktivity na preniknutie do počítačových systémov alebo sietí s cieľom získať informácie, ktoré sa nachádzajú v týchto systémoch alebo sieťach alebo prechádzajú cez tieto systémy alebo siete. BANKS. William C.: Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. In: Emory Law Journal, Roč. 66, č. 3 (2017).

²¹ Pozri k tomu: KOPČOVÁ, Radka: Obchodné tajomstvo ako najlepší spôsob právnej ochrany pre algoritmy v podnikaní? In: Košické dni súkromného práva V. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2024, s. 434.

²² Zvýrazňujeme slovo „právnú“, pretože podnik môže údaje (informácie), ktoré majú ostať utajené, chrániť aj iným, v praxi najmä zmluvným, spôsobom (napríklad môže v zmysle § 271 ods. 1 OBZ označiť tieto informácie ako dôverné alebo môže uzatvoriť dohodu o mlčanlivosti). Zvýrazňujeme, že samotné označenie informácie ako obchodné tajomstvo samo o sebe nepostačuje na to, aby sa tieto informácie stali obchodným tajomstvom, pokiaľ nenapĺňajú zákonom vymedzené pojmové znaky. Pozri k tomu napr.: Rozsudok Najvyššieho súdu SR z 27. januára 2015, sp. zn. 5Sžo/41/2013.

²³ ČADA, Karel: Know - how a obchodní tajemství. Praha: Úřad průmyslového vlastnictví, 2010. s. 284.

²⁴ Predpoklad „tajnosti“ je naplnený, ak sú informácie tvoriace obchodné tajomstvo známe len obmedzenému okruhu osôb.

dialku v digitálnej forme, čo znižuje úroveň kontroly zdieľaných informácií zo strany zamestnávateľa.²⁵

Základným predpokladom legálnej ochrany obchodného tajomstva je jeho „tajnosť“ (resp. „dôvernosť“), pričom podľa poslednej časti druhej vety ustanovenia § 17 ods. 1 OBZ: *„...majiteľ obchodného tajomstva zodpovedajúcim spôsobom ich utajenie zabezpečuje.“* V praxi ide o najväčšiu výzvu pre podniky, ktoré si informácie chránia (resp. snažia chrániť) ako obchodné tajomstvá, keďže v podnikoch sa v súčasnosti väčšina informácií denno-denne zdieľa, spracováva, či sa s nimi inak manipuluje. V tej súvislosti vyvstáva najdôležitejšia otázka: ako majú majitelia *digitálneho* obchodného tajomstva tieto informácie chrániť tak, aby ich ochránili pred ich neoprávneným získaním, sprístupnením alebo zverejnením; a tiež, aby mohli v súdnom (prípadne v inom)²⁶ konaní preukázať, že v individuálnom prípade bola splnená oprávnenosť na ochranu obchodného tajomstva?²⁷

V prvom rade je potrebné uviesť, že podniky by mali byť opatrné v digitalizácii obchodných tajomstiev a ich ukladaní do digitálnych súborov. Nedostatočné zabezpečenie obchodného tajomstva a neopatrnosť pri manipulácii s nimi môže totiž viesť v zamietnutí právnej ochrany týchto informácií ako obchodného tajomstva. Podľa odporúčania Komisie (EÚ) 2024/915 z 19. marca 2024 týkajúce sa opatrení na boj proti falšovaniu a na posilnenie presadzovania práv duševného vlastníctva (odporúčanie EÚ 2024/915) sa hospodárske subjekty *„vzývajú k opatrnosti pri používaní systémov umelej inteligencie a aby do systému nevkladali nezverejnené dôverné informácie, know-how alebo obchodné tajomstvá, pretože im to môže potenciálne brániť v získaní ochrany duševného vlastníctva na účely takýchto informácií v neskoršej fáze.“*²⁸ Dôraz je tak kladený najmä na *prevenciu* a zabezpečenie obchodných tajomstiev internými bezpečnostnými mechanizmami podniku, ktoré by mali zodpovedať súčasnému vývoju digitálnych technológií. Komisia v tej súvislosti zverejnila aj podrobný súbor nástrojov na zvyšovanie informovanosti pre podniky s cieľom pomôcť im predchádzať kybernetickým útokom na obchodné tajomstvá alebo reagovať na ne. Kapitola č. 5 odporúčania EÚ 2024/915 obsahuje

²⁵ Pozri k tomu napr.: KORYCIŇSKA-RZĄDCA, Paulina: Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets against Unauthorised Acquisition, Use and Disclosure by Its Employees? In: Białostockie Studia Prawnicze, roč. 29, č. 2 (2024), s. 163-176.

²⁶ Súdna ochrana proti porušeniu obchodného tajomstva býva v praxi až posledným útočiskom pre poškodeného majiteľa obchodného tajomstva a súdne spory vo veciach porušenia obchodného tajomstva sú skôr výnimočné. Nie je tomu tak preto, že by sa obchodné tajomstvá neporušovali, ale kvôli špecifickým právnym, dôkazným ako aj strategickým dôvodom spojenými s predmetom ochrany, ktorými sú tajné cenné informácie.

²⁷ Pozri: podľa § 17 ods. 1 OBZ: *„majiteľ obchodného tajomstva zodpovedajúcim spôsobom ich utajenie zabezpečuje“*

²⁸ Odôvodnenie 32 odporúčania EÚ 2024/915.

„Súbor nástrojov na predchádzanie kybernetickým krádežiam“, v ktorej sa vyzývajú jednak členské štáty a EUIPO, a jednak aj samotné hospodárske subjekty, aby zvýšili svoju ochranu pred kybernetickými útokmi.

Na tento účel sa vyzývajú:

- a) *členské štáty a EUIPO* na to, aby *podporovali a šíрили nástroje na zvyšovanie informovanosti* pre rizikové skupiny podnikov.²⁹
- b) *hospodárske subjekty* na to, aby zvýšili svoju ochranu pred kybernetickými útokmi³⁰; odborne školili svojich zamestnancov o tom, ako predchádzať kybernetickým útokom zameraným na ich obchodné tajomstvá; a aby podporovali ďalšie nástroje na zvyšovanie informovanosti sprístupnené na informačnom portáli o kybernetickej bezpečnosti s cieľom pomôcť podnikom lepšie chrániť ich duševné vlastníctvo a obchodné tajomstvá a pomôcť im účinnejšie predchádzať kybernetickým útokom.

Dôraz na prevenciu pre zmiernenie rizík neoprávneného získania, sprístupnenia a zverejnenia obchodného tajomstva v digitálnom prostredí okrem Komisie kladie aj Svetová organizácia duševného vlastníctva (WIPO), podľa ktorej je potrebné zaviesť *robustné bezpečnostné opatrenia vrátane pravidelných aktualizácií a plánov reakcie na incidenty*. Zároveň by bezpečnostné opatrenia mali byť na *primeranej úrovni*, podobne ako akékoľvek iné opatrenia na ochranu obchodného tajomstva. Môže byť potrebné *zohľadniť aj hodnotu* obchodného tajomstva oproti nákladom na ochranu obchodného tajomstva a *charakteristiku* organizácie.³¹ Na zmiernenie rizika porušenia obchodného tajomstva v digitálnom prostredí je podľa odporúčaní WIPO dôležité zaviesť *kontroly prístupu, zabezpečiť prísne zmluvné opatrenia, vzdelávanie a odbornú prípravu a absolvovať výstupné a vstupné pohovory* na prevenciu jeho porušenia.

Inak povedané, aby informácie mohli byť chránené ako obchodné tajomstvo, musí podnik prijať už *preventívne „primerané opatrenia“* na zachovanie utajenia týchto informácií a musí tak urobiť vždy s ohľadom na ich hodnotu, pričom konkrétne opatrenia na zachovanie dôvernosti budú v podrobnostiach závisieť vždy od typu obchodného tajomstva a od konkrétnych okolností použitia. Primeranosť opatrení na utajenie obchodného tajomstva je možné určiť na základe objektívnych kritérií a pri posudzovaní ich vhodnosti je potrebné brať do úvahy najmä:

²⁹ Poskytnutie nástrojov malým a stredným podnikom na lepšiu ochranu ich nehmotného majetku je upravené v kapitole č. 5 odporúčania EÚ 2024/915.

³⁰ Okrem iného pomocou nástrojov, ktoré poskytujú verejné orgány, vrátane súboru nástrojov Komisie určeného na predchádzanie kybernetickým útokom zameraným na odcudzenie obchodných tajomstiev alebo na reakciu na ne.

³¹ World Intellectual Property Organization: WIPO Guide to Trade Secrets and Innovation. Geneva: WIPO, 2024. DOI: 10.34667/tind.49735.

- hodnotu obchodného tajomstva a náklady na jeho vypracovanie, charakter informácie;
- dôležitosť obchodného tajomstva pre firmu,
- veľkosť firmy;
- obvyklé opatrenia na zachovanie utajenia v podniku;
- typ označovania informácií v podniku;
- zmluvy o mlčanlivosti a iné zmluvy o dôvernosti informácií uzavreté so zamestnancami, obchodnými partnermi a inými osobami.

Z uvedeného vyplýva minimálny štandard primeranosti opatrenia na utajenie (aj digitálnych) informácií, ktoré sú obchodným tajomstvom, a to, že:

- relevantné informácie možno zveriť len takým osobám, ktoré tieto informácie (potenciálne) potrebujú na plnenie svojej úlohy;
- relevantné informácie možno zveriť len takým osobám, ktoré sú povinné zachovávať o nich mlčanlivosť;
- tieto osoby si musia byť vedomé o povinnosti mlčanlivosti o týchto informáciách.

Ďalšie posilňujúce opatrenia by sa mali prijať v závislosti od okolností a celkovej situácie v podniku.³² Vhodnosť a primeranosť zodpovedajúcej úrovne opatrenia na utajenie obchodného tajomstva by mala vždy závisieť od *faktických možností utajenia*, ktoré má daný podnik k dispozícii, a tiež by mala závisieť aj od povahy a hodnoty informácií, ktoré sú obchodným tajomstvom. Je logické, že veľké podniky majú zvyčajne lepšie zdroje a možnosti na zabezpečenie vhodných opatrení uchovania ich obchodných tajomstiev ako malé a stredné podniky, prípadne začínajúci podnikatelia. Súhlasíme preto s názorom Csacha, že žiaden podnik by nemal strácať nárok na ochranu obchodného tajomstva, pokiaľ nie je v jeho možnostiach zabezpečiť vysoký stupeň ochrany ako je tomu vo veľkých podnikoch.³³ Stonásobne to bude platiť aj pre reálne možnosti kybernetickej ochrany obchodného tajomstva. Objektívne považujeme za zrejmé, že často nie je v silách malých a stredných podnikov brániť sa kyberútokom zo strán tretích osôb. Preto by mali aj súdy vždy posudzovať „primeranosť“ adekvátnej ochrany obchodného tajomstva vo vzťahu k možnostiam podniku.

Nepostačuje, ak majiteľ obchodného tajomstva vôľu utajiť obchodné tajomstvo má, táto vôľa sa vždy prejavuje navonok, aby bola poznateľná inými osobami (napríklad zamestnancami, obchodnými partnermi, inými spoločníkmi). Potvrdzuje to aj výklad

³² „Test primeranosti opatrenia na utajenie obchodného tajomstva“ je našou vlastnou tvorbou, inšpirovali sme sa rakúskou judikatúrou (najmä rozsudok OLG v Stuttgarte z 19. novembra 2020, sp. zn. 2 U 575/19), keďže v slovenskej ani v českej odbornej literatúre a judikatúre sme nenašli podobný „test proporcionality“, ktorý by vymedzoval hranice primeranosti zabezpečenia opatrení na utajenie obchodného tajomstva, ktoré sú zákonným predpokladom na jeho ochranu (§ 17 ods. 1 OBZ).

³³ CSACH, Kristián. In: OVEČKOVÁ, Oľga. a kol.: Obchodný zákonník. Veľký komentár, II. zväzok, druhé vydanie. Bratislava: Wolters Kluwer, 2022, s. 234.

českej judikatúry: „Podnikateľ musí túto vôľu – chrániť skutočnosti obchodnej povahy - dostatočne seznateľným spôsobom prejsť“. ³⁴

Praktickým príkladom, kedy rakúsky súd posúdil formu utajenia digitálneho obchodného tajomstva ako nedostatočnú, bol prípad, kedy majiteľ obchodného tajomstva umožnil svojim zamestnancom ukladať súbory obsahujúce obchodné tajomstvo na súkromné zariadenia na ukladanie údajov (ako sú USB nosiče) bez zabezpečenia pomocou hesla. Podľa súdu tak nebol naplnený jeden zo základných predpokladov na ochranu informácií ako obchodné tajomstvo. ³⁵

Záver

V digitálnom veku sa informácie, ktoré môžu tvoriť obchodné tajomstvo, stali cennou, ale zároveň zraniteľnou komoditou. Záverom možno konštatovať, že v súčasnosti je pre podniky kľúčové nájsť tú správnu rovnováhu medzi podporou zdieľania údajov na jednej strane (najmä digitalizácia informácií a uľahčovanie prístupu zamestnancov a iných oprávnených osôb k týmto údajom, ktoré môžu tvoriť obchodné tajomstvo) a dostatočnou ochranou obchodných tajomstiev na strane druhej. Podniky by mali byť opatrné v digitalizácii obchodných tajomstiev a ich ukladaní do digitálnych súborov. Nedostatočná prevencia, nedostatočné zabezpečenie obchodného tajomstva a neopatrnosť pri manipulácii s nimi môže totiž viesť v zamietnutí právnej ochrany týchto informácií ako obchodného tajomstva.

Aby digitálne informácie tvoriace obchodné tajomstvo boli dostatočne chránené, a aby mohli tieto informácie vôbec požívať právnu ochranu ako obchodné tajomstvo, musí podnik v prvom rade dbať na preventívne opatrenia. Tieto opatrenia v príspevku bližšie špecifikujeme, vychádzame najmä z odporúčania EÚ 2024/915 a WIPO.

Vychádzajúc zo zákonných predpokladov ochrany obchodného tajomstva a rakúskej judikatúry vyvodzujeme záver, že podniky musia prijať „primerané opatrenia“ na zachovanie utajenia týchto informácií a musia tak urobiť vždy s ohľadom na ich hodnotu, pričom konkrétne opatrenia na zachovanie dôvernosti budú v podrobnostiach závisieť vždy od typu obchodného tajomstva a od konkrétnych okolností jeho použitia. Primeranosť opatrení na utajenie obchodného tajomstva je možné určiť na základe objektívnych kritérií, ktoré bližšie prezentujeme v jadre príspevku.

Pri nezodpovedajúcom spôsobe ochrany digitálneho obchodného tajomstva zo strany jeho majiteľa je nanajvýš pravdepodobné jednak to, že tieto cenné a tajné informácie budú skôr či neskôr neoprávnene získané, zverejnené alebo inak sprístupnené zo strany tretej osoby (prípadne aj z radu vlastných zamestnancov, spoločníkov, obchodných partnerov a pod.); a jednak to, že aj pokiaľ sa bude majiteľ

³⁴ Rozsudok Najvyššieho správneho súdu ČR z 17. januára 2006, sp. zn. 21 CDO 617/2005.

³⁵ Rozsudok OLG v Stuttgarte z 19. novembra 2020, sp. zn. 2 U 575/19.

domáhať právnych prostriedkov ochrany pre porušenie obchodného tajomstva na súde, súd žalobu s najväčšou pravdepodobnosťou zamietne. Súd môže totiž v takomto prípade vyhodnotiť, že nebol splnený základný zákonný predpoklad obchodného tajomstva, konkrétne ten, že majiteľ obchodného tajomstva neujavoval (digitálne) informácie tomu zodpovedajúcim spôsobom. Ide o základný predpoklad ochrany tajných a cenných informácií, ktorý je zakotvený na národnej (§ 17 ods. 1 OBZ), európskej (čl. 2 ods. 2 smernice o obchodnom tajomstve), ako aj medzinárodnej (čl. 39 dohody TRIPS) úrovni právnej úpravy obchodného tajomstva.

Zoznam použitej literatúry

1. APLIN, Tanya, RADAUER, Alfred, BADER, Martin, SEARLE, Nicola: The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. In: IIC - International Review of Intellectual Property and Competition Law, č. 54 (2023), s. 826–858. <https://doi.org/10.1007/s40319-023-01325-8>.
2. BANKS, William C.: Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. In: Emory Law Journal, Roč. 66, č. 3 (2017).
3. CSACH, Kristián. In: OVEČKOVÁ, Oľga. a kol.: Obchodný zákonník. Veľký komentár, II. zväzok, druhé vydanie. Bratislava: Wolters Kluwer, 2022, 3704 s. ISBN 978-80-571-0437-7.
4. ČADA, Karel: Know - how a obchodní tajemství. Praha: Úřad průmyslového vlastnictví, 2010. 284 s. ISBN 978- 80-7282-087-0.
5. Európska Komisia: Akčný plán duševného vlastníctva na podporu obnovy a odolnosti EÚ (Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Maximálne využitie inovačného potenciálu EÚ - Akčný plán duševného vlastníctva na podporu obnovy a odolnosti EÚ) COM/2020/760 final z 24. 11. 2020 (ďalej len „akčný plán IP“).
6. GYURÁSZ, Zoltán, HAMULÁK, Ondrej, DRAŽOVÁ Petra: A proactive approach to legal privilege in the light of electronic communication. In: TalTech Journal of European Studies, Roč. 15, č. 1 (2025), s. 83-105.
7. KOPČOVÁ, Radka: Trade secret: a significant legal institution in business and its legal regulation across selected European countries (including case law). In: Central and Eastern European Legal Studies. Atény: European Public Law Organization, č. 2 (2024), s. 241-277. ISSN 2310-2705.
8. KORYCIŃSKA-RZĄDCA, Paulina: Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets against Unauthorised Acquisition, Use and Disclosure by Its Employees? In: Białostockie Studia Prawnicze, roč. 29, č. 2 (2024), s. 163-176.

9. KOUKAL, Pavel: Obchodní tajemství v novém občanském zákoníku. In: Časopis pro právní vědu a praxi, Brno, č. 21 (2013), s. 467-475.
10. KUBÍČEK, Pavel, ŠKRINÁR, Alexander, NEVOLNÁ, Zuzana, KOPČOVÁ, Radka, ŽURICA, Milan: Obchodné právo. 4. vyd. Plzeň: Aleš Čeněk, 2025. 450 s. ISBN: 978-80-7380-987-4.
11. PATAKYOVÁ, Mária. a kol. Obchodný zákonník. Komentár. 1. vyd. Bratislava: C. H. Beck, 2022, s. 1792. ISBN 978-80-8232-018-6.
12. SEARLE, Nicola: The Economic and Innovation Impacts of Trade Secrets. Technical Report. UK IPO, London, 2021. [Report] <https://research.gold.ac.uk/id/eprint/30022>.
13. UBAYDULLAEVA, Anna: Know-How and Trade Secrets in Digital Business. In: International Journal of Law and Policy, Roč. 2, č. 3 (2024). s. DOI: 10.59022/ijlp.162.
14. World Intellectual Property Organization: WIPO Guide to Trade Secrets and Innovation. Geneva: WIPO, 2024. DOI: 10.34667/tind.49735.
15. Smernica Európskeho parlamentu a Rady (EÚ) 2016/943 z 8. júna 2016 o ochrane nesprístupneného know-how a obchodných informácií (obchodného tajomstva).
16. Dohoda WTO o obchodných aspektoch práv duševného vlastníctva tvoriaca prílohu 1C Dohody o založení Svetovej obchodnej organizácie (Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 152/2000 Z. z.) („dohoda TRIPS“).
17. Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.
18. Zákon č. 89/2012 Sb. Občanský zákoník (nový) v znení neskorších predpisov.
19. Odporúčanie Komisie (EÚ) 2024/915 z 19. marca 2024 týkajúce sa opatrení na boj proti falšovaniu a na posilnenie presadzovania práv duševného vlastníctva.
20. Rozsudok Najvyššieho súdu SR z 27. januára 2015, sp. zn. 5Sžo/41/2013.
21. Rozsudok Najvyššieho správneho súdu ČR z 17. januára 2006, sp. zn. 21 CDO 617/2005.
22. Rozsudok OLG v Stuttgarte z 19. novembra 2020, sp. zn. 2 U 575/19.

Kontaktné údaje

JUDr. Radka Kopčová, PhD. LL.M.

radka.kopcova@gmail.com

Ústav súkromného práva, Právnická fakulta PEVŠ v Bratislave

ORCID: 0009-0000-0930-4543

ZDRAVOTNÍCTVO 2.0: KEĎ INTELIGENTNÉ HODINKY MONITORUJÚ A ZÁKON MLČÍ

HEALTHCARE 2.0: WHEN SMARTWATCHES MONITOR AND THE LAW STAYS SILENT

Soňa Sopúchová¹

Abstrakt: Predmetom príspevku je podrobná analýza právneho postavenia inteligentných hodínok a iných inteligentných nositeľných technológií, ktoré napriek rozšíreným zdravotným a monitorovacím funkciám zostávajú stále kategorizované ako spotrebná elektronika, nie ako zdravotnícke pomôcky. Táto skutočnosť vyvoláva otázky týkajúce sa primeranej úrovne ochrany zdravia a bezpečnosti používateľov, ako aj spoľahlivosti a kvality samotných zariadení. Cieľom štúdie je preto identifikovať dôsledky aktuálneho klasifikačného prístupu a analyzovať jeho dopad na mechanizmy regulačného dohľadu a na budúci vývoj legislatívneho prostredia. Metodologicky sa príspevok opiera o právnu analýzu právnych predpisov Európskej únie, pričom osobitná pozornosť sa venuje regulácii zdravotníckych pomôcok a špecifikám technológií využívajúcich algoritmy umelej inteligencie. Zistenia poukazujú na systematické nedostatky existujúcich noriem, ktoré nedostatočne reflektujú dynamický rozvoj v oblasti nositeľných technológií a vytvárajú regulačné medzery. Vedecký prínos spočíva v teoretickej reflexii hraníc medzi spotrebnými a zdravotníckymi zariadeniami, zatiaľ čo praktický prínos predstavuje formulácia odporúčaní na úpravu legislatívy s cieľom dosiahnuť vyvážený vzťah medzi inovačným potenciálom, ochranou zdravia a jasným určením právnej zodpovednosti.

Kľúčové slová: nositeľné technológie, inteligentné hodinky, regulácia zdravotníckych pomôcok, umelá inteligencia v zdravotníctve, monitorovanie zdravia

Abstract: The subject of the paper is an analysis of the legal status of smartwatches and other intelligent wearable technologies, which, despite their extensive health-related and monitoring functions, remain categorized as consumer electronics rather than medical devices. This classification raises important questions regarding the adequacy of user health and safety

¹ Univerzita Komenského Bratislava, Právnická fakulta

protection, as well as the reliability and quality of such devices. The aim of the study is therefore to identify the consequences of the current classification and to analyze its impact on regulatory oversight mechanisms and the future development of the legislative environment. Methodologically, the paper is based on a legal analysis of the European Union legislation, with particular attention paid to the regulation of medical devices and the specificities of technologies employing artificial intelligence algorithms. The findings highlight systematic shortcomings of the existing standards, which insufficiently reflect the dynamic development of wearable technologies and create regulatory gaps. The scientific contribution of this paper lies in a theoretical reflection on the boundaries between consumer and medical devices, while the practical contribution consists in formulating recommendations for legislative adjustments aimed at achieving a balanced relationship between innovation potential, health protection, and defined legal responsibility.

Key words: wearable technologies, smartwatches, medical devices regulation, artificial intelligence in healthcare, health monitoring

Úvod

Rýchly rozvoj inteligentných nositeľných technológií v posledných rokoch významne ovplyvnil spôsob, akým ľudia monitorujú svoje zdravie a celkovú pohodu. Inteligentné nositeľné technológie sa definujú ako podmnožina internetu vecí.² Typickým príkladom tohto trendu sú inteligentné hodinky, ktoré sa zmenili z jednoduchého doplnku na meranie času na multifunkčné zariadenie schopné merať životné funkcie, sledovať parametre fyzickej aktivity, monitorovať pulz či saturáciu kyslíkom a dokonca detegovať potenciálne zdravotné riziká, ako sú nepravidelné srdcové rytmy. Tieto zariadenia často využívajú umelú inteligenciu (ďalej len „AI“), ktorá im umožňuje spracúvať zdravotné údaje a poskytovať používateľom interpretáciu rôznych výsledkov. Ako príklad možno uviesť inteligentné hodinky vyvinuté americkou spoločnosťou Apple, ktoré integrujú funkciu elektrokardiogramu (ďalej len „EKG“), umožňujúcu používateľom monitorovať srdcový rytmus a detegovať anomálie, ktoré môžu naznačovať stavy, ako je fibrilácia predsiení.³ Napriek tomu, že tieto zariadenia ponúkajú funkcie blízke zdravotníckym

² Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H., Raad, A. Smart Wearables for the Detection of Occupational Physical Fatigue: A Literature Review. In: *Sensors*. Roč. 22, (2022), s. 6.

³ Spoločnosť Apple Inc. uskutočnila viacero klinických štúdií s cieľom validovať svoje zdravotné funkcie v nositeľných zariadeniach, vrátane aplikácie EKG a upozornenia na nepravidelný rytmus, pričom preukázala ich účinnosť pri detekcii fibrilácie predsiení (Apple Health Study, 2018).

pomôckam, nie sú klasifikované ako zdravotnícke pomôcky, pretože nie sú určené na medicínske účely. Toto kritérium predstavuje jeden z určujúcich znakov zdravotníckej pomôcky podľa legislatívy, ktorej podrobnejšia analýza bude predmetom ďalšieho výkladu v tomto príspevku.

Európska únia (ďalej len „EÚ“) prijala Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 o zdravotníckych pomôckach⁴ (ďalej len „Nariadenie o zdravotníckych pomôckach“ alebo „MDR“), ktoré stanovuje bezpečnostné požiadavky zabezpečujúce, aby produkty uvádzané na trh na medicínske účely boli klinicky testované, spoľahlivé a účinné. Medzi jeho najdôležitejšie ustanovenia patrí povinnosť klinického hodnotenia, ktoré článok 2 ods. 4 MDR definuje ako systematický a plánovaný proces tvorby, zhromažďovania, analýzy a posudzovania klinických údajov s cieľom overiť bezpečnosť, funkčnosť a klinický prínos zariadenia pre jeho zamýšľané použitie. Nariadenie o zdravotníckych pomôckach taktiež poskytuje právnu definíciu zdravotníckej pomôcky,⁵ ktorá je úzko spätá s jej konkrétnym medicínskym účelom.

V praxi sú však inteligentné hodinky uvádzané na trh ako spotrebiteľské produkty a nie ako zariadenia na výslovné medicínske využitie, čo ich vylučuje z právnej kategórie zdravotníckych pomôcok.⁶

Predmetom tohto príspevku je skúmanie dôvodov, prečo inteligentné hodinky nie sú právne klasifikované ako zdravotnícke pomôcky. Práca identifikuje nedostatky v súčasnej nadnárodnej legislatíve a zvažuje možné potreby reforiem. Ústrednou otázkou je, či by inteligentné hodinky a ďalšie inteligentné nositeľné technológie mali

⁴ Nariadenie (EÚ) 2017/745 Európskeho parlamentu a Rady o zdravotníckych pomôckach, ktorým sa mení smernica 2001/83/ES, nariadenie (ES) č. 178/2002 a nariadenie (ES) č. 1223/2009 a ktorým sa zrušujú smernice Rady 90/385/EHS a 93/42/EHS.

⁵ Článok 2 ods. 1 MDR: „Zdravotnícka pomôcka znamená akýkoľvek nástroj, prístroj, pomôcku, softvér, implantát, reagent, materiál alebo iný predmet, ktorý výrobca zamýšľa použiť samostatne alebo v kombinácii u ľudí na jeden alebo viac z týchto konkrétnych medicínskych účelov:

- diagnostika, prevencia, monitorovanie, predikcia, prognóza, liečba alebo zmiernenie choroby,
- diagnostika, monitorovanie, liečba, zmiernenie alebo kompenzácia poranenia alebo zdravotného postihnutia,
- skúmanie, náhrada alebo úprava anatómie alebo fyziologického či patologického procesu alebo stavu,
- poskytovanie informácií prostredníctvom in vitro skúmania vzoriek odobratých z ľudského tela vrátane darovaných orgánov, krvi a tkanív,

a ktoré nedosahuje svoj hlavný zamýšľaný účinok farmakologickými, imunologickými alebo metabolickými prostriedkami v ľudskom tele alebo na ňom, avšak jeho funkcia môže byť takýmito prostriedkami podporovaná.“

⁶ Devine, J. K., Schwartz, L. P., & Hursh, S. R. Technical, Regulatory, Economic, and Trust Issues Preventing Successful Integration of Sensors into the Mainstream Consumer Wearables Market. In: *Sensors*. Roč. 22, číslo 7 (2022), s. 3

byť považované za zdravotnícke pomôcky, keďže zohrávajú čoraz významnejšiu úlohu v monitorovaní zdravia.

Dialkové monitorovanie zdravia a nositeľné technológie

Dialkové monitorovanie je jednou z hlavných oblastí telemedicíny. Tento proces umožňuje pacientom zaznamenávať údaje o svojom zdravotnom stave v nemedicínskom prostredí, čím získavajú väčšiu mieru nezávislosti a kontroly nad vlastnou zdravotnou starostlivosťou. Získané údaje môžu byť následne zdieľané s lekármi, čo umožňuje skorú detekciu zdravotných problémov, ako aj kontinuálnu starostlivosť a rozhodovanie založené na dátach. Významnú úlohu v dialkovom monitorovaní pacientov zohráva umelá inteligencia, ktorá siaha od klasifikácie fyzickej aktivity až po sledovanie chronických ochorení a vitálnych funkcií v urgentných situáciách.⁷

Nárast používania inteligentných hodín umožnil mnohým pacientom aktívne sa zapájať do starostlivosti o seba a zasadzovať sa za zdravie iných. S rastúcim počtom týchto jednotlivcov, známych ako e-pacienti, je nevyhnutné, aby zdravotnícke inštitúcie primerane vzdelávali svojich študentov v efektívnej spolupráci s týmito pacientmi a v poskytovaní zdravotnej starostlivosti pre túto skupinu.⁸

Nositeľné technológie, ako sú inteligentné hodinky vybavené meračmi srdcovej frekvencie a funkciou EKG alebo hrudné pásy na meranie pulzu, predstavujú konkrétne príklady dialkového monitorovania zdravia.⁹ Dialkové monitorovanie a zachytávanie skorých príznakov ochorenia môže byť nesmierne prínosné pre osoby trpiace chronickými ochoreniami a pre seniorov.¹⁰

Jednou z hlavných výziev monitorovania prostredníctvom nositeľných technológií v oblasti zdravotnej starostlivosti je bezproblémová integrácia dát, ktoré tieto zariadenia zbierajú, do elektronických zdravotných záznamov¹¹ (ďalej len „EHR“). Je nevyhnutné, aby nositeľné technológie boli vybudované na infraštruktúre, ktorá

⁷ Shaik, T., Tao, X., Higgins, N., Li, L., Gururajan, R., Zhou, X., & Acharya, U. R. Remote patient monitoring using artificial intelligence: Current state, applications, and challenges. In: *WIREs DataMining and Knowledge Discovery*. Roč. 13, číslo 2 (2023), s. 1.

⁸ Hosseini, M. M., Hosseini S. T. M., Qayumi, K., Hosseinzadeh, S., Tabar S. S. S. Smartwatches in healthcare medicine: assistance and monitoring; a scoping review. In: *BMC Medical Informatics and Decision Making*. Roč. 23, č. 1 (2023), s. 2.

⁹ Zariadenia s funkciou merania EKG zaznamenávajú elektrické signály zo srdca a poskytujú zdravotníckym pracovníkom kľúčové informácie o srdcovom rytme a potenciálnych abnormalitách, ako je fibrilácia predsiení.

¹⁰ Bohr, A., Memarzadeh, K. *Artificial Intelligence in Healthcare*. London: Academic Press, 2020, s. 40.

¹¹ Canali S, Schiaffonati V, Aliverti A. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. In: *PLOS Digit Health*. 1(10), (2022), s. 7.

umožňuje zber osobných údajov jednotlivca a ich uchovávanie v stave pripravenom na použitie.¹²

Okrem technických prekážok predstavuje jednu z najväčších výziev aj právna definícia nositeľných zariadení. Nariadenie o zdravotníckych pomôckach stanovuje kritériá pre definovanie zdravotníckych pomôcok, vrátane požiadaviek na testovanie, certifikáciu a súlad s bezpečnostnými normami. Nositeľné technológie však často predstavujú „šedú zónu“, keďže sú uvádzané na trh predovšetkým ako produkty pre podporu zdravia, nie ako zdravotnícke pomôcky, napriek ich rastúcej úlohe v diaľkovom monitorovaní zdravia. Keďže hranica medzi nositeľnými zariadeniami pre wellness účely a zdravotníckymi pomôckami sa stáva čoraz ťažšie odlišiteľnou, jedno zariadenie už dokáže monitorovať viacero medicínskych rizikových faktorov.¹³

Nositeľné zariadenia možno vo všeobecnosti definovať ako mobilné elektronické zariadenia, ktoré sú nenápadne začlenené do používateľovho oblečenia alebo doplnku. Na rozdiel od konvenčných mobilných systémov môžu byť tieto zariadenia v prevádzke a prístupné bez alebo s minimálnym obmedzením používateľovej aktivity. Z tohto dôvodu sú schopné modelovať a rozpoznávať používateľovu činnosť, stav a okolité prostredie, čo predstavuje vlastnosť označovanú ako kontextová citlivosť.¹⁴ Táto a ďalšie špecifiká komplikujú ich právnu klasifikáciu, keďže sa ťažko zaraďujú do tradičných regulačných kategórií. Absencia jasných právnych definícií a klasifikácií takýchto zariadení v rámci štandardných diagnostických, liečebných či terapeutických postupov vyvoláva otázky o ich regulačnom statuse a predstavuje prekážku pre ich schvaľovanie zo strany lekárov, poskytovateľov zdravotnej starostlivosti a poisťovní, čo následne obmedzuje ich integráciu do formalizovaných systémov zdravotnej starostlivosti.

Právny rámec pre zdravotnícke pomôcky

Na úrovni EÚ predstavuje kľúčový právny nástroj regulácie zdravotníckych pomôcok Nariadenie o zdravotníckych pomôckach, ktoré opisuje zdravotnícku pomôcku ako akýkoľvek produkt, či už fyzický alebo softvérový, určený výrobcom na použitie u ľudí s jasne definovanou medicínskou funkciou. Tieto funkcie môžu zahŕňať napríklad diagnostiku, prevenciu alebo monitorovanie chorôb, liečbu alebo kompenzáciu poranení či zdravotných postihnutí, alebo skúmanie, úpravu či nahradenie fyziologických alebo anatomických procesov.

¹² Tong, R. *Wearable Technology in Medicine and Health Care*. London: Academic Press, 2018, s. 289.

¹³ Piwek, L., Ellis, S. A., Andrews, S., Joinson, A. The Rise of Consumer Health Wearables: Promises and Barriers. In: *PLoS Medicine*. 13 (2), (2016), s. 1.

¹⁴ Lukowicz, P., Kirstein, T., Tröster, G. Wearable systems for health care applications. In: *Methods of information in medicine*. Roč. 2004, č. 3 (2004), s. 232.

Vzhľadom na povahu týchto zariadení, ktoré vo veľkej miere zbierajú a analyzujú biometrické údaje v reálnom čase, vrátane srdcovej frekvencie, hladiny kyslíka v krvi či záznamov elektrokardiogramu, je dôležité, aby boli v súlade s pravidlami EÚ navrhnutými na ochranu osobných údajov jednotlivcov. Zariadenia poháňané umelou inteligenciou navyše podporujú rozvoj aplikácií tretích strán, ktoré môžu získať prístup k údajom zozbieraným týmito zariadeniami.¹⁵ Takto získané údaje by preto mali byť spracúvané zákonným, spravodlivým a transparentným spôsobom v súlade so Všeobecným nariadením o ochrane údajov (ďalej len „GDPR“)¹⁶, ktoré predstavuje regulačný rámec EÚ pre spracúvanie osobných údajov.¹⁷ GDPR stanovuje viacero kľúčových princípov a povinností, ktoré majú priamy dopad na využívanie zariadení s umelou inteligenciou v zdravotnej starostlivosti a pri monitorovaní zdravia jednotlivcov, ako sú zákonnosť, spravodlivosť a transparentnosť, obmedzenie účelu, minimalizácia údajov, bezpečnostné a ochranné opatrenia, kontrola zo strany používateľov a práva na prístup k údajom, ako aj povinnosti zodpovednosti a súladu s reguláciou.

Klasifikácia zdravotníckych pomôcok a inteligentné hodinky

Jednou z páľčivých otázok, ktoré sa týkajú tejto témy, je otázka z úvodu tohto príspevku, či možno inteligentné hodinky alebo iné nositeľné zariadenia považovať v rámci existujúceho právneho systému za zdravotnícke pomôcky.

Medzi najrelevantnejšie kritériá odvodené z Nariadenia o zdravotníckych pomôckach, ktoré môžu tvoriť rámec analýzy, patria povaha zariadenia, zamýšľaný používateľ zariadenia, konkrétny medicínsky účel zariadenia.¹⁸

a) Povaha zariadenia

Aby sa produkt kvalifikoval ako zdravotnícka pomôcka, musí spadať do jednej z kategórií uvedených v článku 2 ods. 1 Nariadenia o zdravotníckych pomôckach, ako sú nástroj, prístroj, pomôcka, softvér, implantát, reagent, materiál alebo iný predmet určený výrobcom na použitie samostatne alebo v kombinácii.

Pred posúdením, či inteligentné hodinky spĺňajú toto kritérium, je potrebné venovať sa pojmu „softvér“. Legislatíva v oblasti zdravotníckych pomôcok síce softvér explicitne nedefinuje, avšak k dispozícii sú dokumenty EÚ, ktoré túto otázku

¹⁵ Pracovná skupina pre ochranu údajov podľa článku 29: Stanovisko č. 8/2014 o najnovšom vývoji v oblasti internetu vecí.

¹⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov – GDPR).

¹⁷ Hosseini, M. M., Hosseini S. T. M., Qayumi, K., Hosseinzadeh, S., Tabar S. S. S. Smartwatches in healthcare medicine: assistance and monitoring; a scoping review. In: *BMC Medical Informatics and Decision Making*. Roč. 23, č. príspevku 248, (2023), s. 3.

¹⁸ Štvrtým kritériom je negatívna definícia týkajúca sa hlavného účinku zariadenia.

objasňujú, najmä usmernenia vydané v súvislosti s Nariadením o zdravotníckych pomôckach. Sekundárne usmernenia, ako napríklad MDCG 2021-24¹⁹, spresňujú, že softvér možno považovať za aktívnu zdravotnícku pomôcku, ak je navrhnutý na monitorovanie alebo diagnostiku zdravotných stavov.²⁰

Inteligentné nositeľné zariadenia, ako sú inteligentné hodinky, vyvolávajú zaujímavé otázky týkajúce sa toho, do ktorej kategórie podľa článku 2 ods. 1 Nariadenia o zdravotníckych pomôckach patria. Z regulačného hľadiska môžu byť klasifikované ako nástroje alebo prístroje na základe hardvérových vlastností, akými sú senzory, procesory či komunikačné moduly určené na monitorovanie a prenos fyziologických informácií. Súčasne je však výkon týchto zariadení vo veľkej miere podmienený softvérovými programami, ktoré spracúvajú zozbierané údaje a produkujú medicínsky relevantné informácie alebo výstupy (napríklad upozornenia či diagnostické odporúčania).

Na základe týchto dvoch aspektov možno konštatovať, že inteligentné hodinky spadajú do viacerých kategórií výrobkov podľa článku 2 ods. 1 Nariadenia o zdravotníckych pomôckach. Preto možno uzavrieť, že spĺňajú prvú podmienku kvalifikácie ako zdravotnícka pomôcka, ktorou je zaradenie medzi určené typy produktov.

b) Zamýšľaný používateľ zariadenia

Druhou charakteristikou je identifikácia používateľa zdravotníckej pomôcky, pre ktorého je určená, pričom podľa článku 2 ods. 1 Nariadenia o zdravotníckych pomôckach týmto používateľom môže byť výlučne človek. Všetky posudzované inteligentné nositeľné zariadenia vrátane inteligentných hodínok sú jednoznačne určené na ľudské použitie.

Usmernenie MEDDEV 2.1/6 navyše poskytuje pohľad na činnosti, ktoré patria a ktoré nepatria do pôsobnosti softvéru určeného na prospech jednotlivých pacientov. Príkladom softvéru určeného na prospech individuálnych pacientov je softvér, ktorý má byť použitý na vyhodnocovanie údajov pacienta s cieľom podporiť alebo ovplyvniť zdravotnú starostlivosť poskytovanú tomuto pacientovi. Naopak, príkladmi softvéru, ktoré sa nepovažujú za určené na prospech individuálnych pacientov, sú softvéry agregujúce populačné údaje, poskytujúce všeobecné diagnostické alebo liečebné postupy, vedeckú literatúru, medicínske atlasy, modely a šablóny, ako aj softvér pre epidemiologické štúdie či registre.²¹

Z uvedeného vyplýva, že inteligentné hodinky, ktoré sa používajú na monitorovanie a analýzu zdravotných údajov špecifických pre jednotlivca a ktoré môžu potenciálne

¹⁹ Usmernenie MDCG 2021-24 o klasifikácii zdravotníckych pomôcok.

²⁰ Usmernenie MDCG 2021-24 o klasifikácii zdravotníckych pomôcok. 2021, s. 11.

²¹ MEDDEV 2.1/6 – Usmernenia o kvalifikácii a klasifikácii samostatného softvéru používaného v zdravotnej starostlivosti v rámci regulačného rámca zdravotníckych pomôcok. 2016, s. 12.

ovplyvniť osobné rozhodnutia o zdravotnej starostlivosti, spadajú do regulačného rámca zdravotníckych pomôcok podľa písm. b). Funkcia monitorovania zdravia a bezpečnosti prostredníctvom nositeľných zariadení sa pritom najčastejšie využíva u starších osôb, detí, tehotných žien a ďalších skupín pacientov.²²

c) Konkrétny medicínsky účel zariadenia

Tretie kritérium, definované v článku 2 ods. 1 Nariadenia o zdravotníckych pomôckach, sa týka požiadavky, aby zdravotnícka pomôcka bola určená na jeden zo špecifických medicínskych účelov taxatívne vymenovaných v príslušnej legislatíve.²³ Zámer výrobcu by mal byť zrejmý z obalu zariadenia alebo z jeho návodu na použitie. V Nariadení o zdravotníckych pomôckach nie je pojem „monitorovanie“ definovaný všeobecne, ale v článku 2 ods. 1 je obmedzený na monitorovanie choroby, poranenia alebo zdravotného postihnutia. Tento rozdiel je významný, keďže nie všetky zariadenia nosené na tele sú navrhnuté na tieto účely. Napríklad bežné inteligentné hodinky, ktoré monitorujú údaje o fyzickej aktivite, ako je počet krokov či príjem kalórií, nemožno považovať za zdravotnícke monitorovanie. Na druhej strane, zariadenie schopné detegovať fibriláciu srdcových predsiení alebo monitorovať hladinu kyslíka v krvi u chronicky chorých pacientov toto kritérium spĺňa.

Ďalej, pojem medicínsky účel v Nariadení o zdravotníckych pomôckach implikuje, že zahŕňa činnosti, ktoré typicky vyžadujú medicínsku zručnosť alebo odborné skúsenosti. To vyvoláva otázku, či sa legislatíva vzťahuje primárne na zariadenia určené pre zdravotníckych pracovníkov alebo aj na nositeľné technológie vyvinuté na samo-monitorovanie zo strany laických používateľov. V tejto súvislosti je potrebné poznamenať, že definícia „používateľa“²⁴ v Nariadení o zdravotníckych pomôckach je relevantná, keďže naznačuje, že zdravotnícke pomôcky nemajú byť určené výlučne pre zdravotníckych pracovníkov, ale aj pre pacientov v domácom prostredí. Z toho vyplýva, že nositeľné zariadenia umožňujúce jednotlivcom analyzovať vlastný zdravotný stav nemožno automaticky vylúčiť z pôsobnosti zdravotníckych pomôcok

²² Lu L., Zhang J., Xie Y., Gao F., Xu S., Wu X., Ye Z. Wearable Health Devices in Health Care. In: *Narrative Systematic Review, JMIR Mhealth Uhealth*. Roč. 8, č. 11 (2020), s. 4.

²³ Medicínske účely sú súčasťou definície zdravotníckej pomôcky:

- diagnostika, prevencia, monitorovanie, predikcia, prognóza, liečba alebo zmiernenie choroby,
- diagnostika, monitorovanie, liečba, zmiernenie alebo kompenzácia poranenia alebo zdravotného postihnutia,
- skúmanie, náhrada alebo úprava anatómie alebo fyziologického či patologického procesu alebo stavu,
- poskytovanie informácií prostredníctvom *in vitro* skúmania vzoriek odobratých z ľudského tela, vrátane darcovstva krvi a tkanív, za predpokladu, že hlavný zamýšľaný účinok zariadenia sa nedosahuje farmakologickými, imunologickými alebo metabolickými prostriedkami, hoci takéto prostriedky môžu jeho funkciu podporovať.

²⁴ Článok 1 ods. 37 Nariadenia o zdravotníckych pomôckach: „Používateľom“ sa rozumie „akýkoľvek zdravotnícky pracovník alebo laik, ktorý používa zdravotnícku pomôcku.“

len preto, že ich používajú laickí užívatelia. V súčasnosti sa funkcie monitorovania zdravia v inteligentných hodinkách javia skôr ako doplnkové než ako ich primárne funkcie, pričom sú často prezentované ako nástroje na podporu zdravia, nie ako zdravotnícke pomôcky.

Problémovým aspektom v kontexte inteligentných hodínok je komponent „zamýšľaného použitia“ v definícii: akékoľvek zariadenie, ktoré by mohlo medicínske účely splniť a aj sa tak využíva, ale nie je na tento účel výslovne určené výrobcom, nespadá pod právnu definíciu zdravotníckej pomôcky a tým pádom ani pod prísnu reguláciu. Je tomu tak z dôvodu, že na to, aby bolo zariadenie zaradené medzi zdravotnícke pomôcky, musia byť splnené všetky znaky uvedené v článku 2, ods. 1 Nariadenia o zdravotníckych pomôckach. Vzhľadom na rozmanitosť, množstvo a jednoduchú dostupnosť týchto technológií pacientom-spotrebiteľom oproti skúsenejším a odborne vyškoleným zdravotníckym pracovníkom, môžu pacienti-spotrebiteľia tieto zariadenia využívať spôsobom, ktorý nie je schválený.²⁵

Súdny dvor EÚ (ďalej len „SDEÚ“) v prípade Brain Products GmbH konštatoval, že ak výrobca nenavrhol svoj produkt na medicínske účely, nemožno od neho požadovať, aby bol certifikovaný ako zdravotnícka pomôcka. Produkt je klasifikovaný ako zdravotnícka pomôcka iba vtedy, ak je výslovne určený na medicínsky účel. Predmetom sporu bolo zariadenie ActiveTwo, vyrábané spoločnosťou BioSemi a ďalšími, používané na meranie fyziologických signálov. Spoločnosť Brain Products tvrdila, že zariadenie spĺňa definíciu zdravotníckej pomôcky. Keďže nemalo označenie CE, ktoré je povinné pre uvedenie zdravotníckych pomôcok na trh, Brain Products sa snažila zakázať jeho komercializáciu. BioSemi a ďalší však argumentovali, že zariadenie ActiveTwo nebolo určené na medicínske účely, a preto nespadá do definície zdravotníckej pomôcky. Nemecký vnútroštátny súd položil SDEÚ prejudiciálnu otázku, či medicínsky účel určený výrobcom predstavuje určujúci prvok zdravotníckej pomôcky. SDEÚ potvrdil, že zamýšľaný medicínsky účel výrobcu je skutočne kľúčovým kritériom pri určovaní, či produkt spĺňa podmienky zdravotníckej pomôcky. Toto výkladové stanovisko bolo podporené nielen znením príslušných právnych predpisov, ale aj ich cieľmi, a to zabezpečiť voľný pohyb zdravotníckych pomôcok v EÚ pri zachovaní vysokej úrovne ochrany zdravia pacientov. Súd zdôraznil, že obmedzenia tejto slobody sú odôvodnené len vtedy, ak sú nevyhnutné na ochranu verejného zdravia. Okrem toho SDEÚ objasnil, že ak produkt nie je výrobcom určený na použitie aspoň na jeden z medicínskych účelov definovaných v nariadení o zdravotníckych pomôckach, nemôže podliehať certifikačným požiadavkám. Súd to ilustroval konštatovaním, že rôzne športové zariadenia, ktoré dokážu merať fungovanie určitých ľudských orgánov bez akejkoľvek

²⁵ Iqbal J. D., Biller-Andorno, N. The regulatory gap in digital health and alternative pathways to bridge it. In: *Health Policy and Technology*. Roč. 11, č. 3 (2022), s. 4.

medicínskej aplikácie, nemožno automaticky klasifikovať ako zdravotnícke pomôcky. Inak by neopodstatnene podliehali certifikačným postupom napriek absencii medicínskeho cieľa.

Zásadnou regulačnou výzvou teda zostáva to, že výrobcovia musia nositeľné zariadenia výslovne navrhovať a uvádzať na trh ako zdravotnícke pomôcky, aby splnili regulačné požiadavky. V súčasnosti sa funkcie monitorovania zdravia v inteligentných hodinkách zdajú byť doplnkové, a nie primárne, pričom často sú prezentované skôr ako nástroje pre wellness než ako zdravotnícke pomôcky. To vyvoláva otázku, či je súčasná definícia zdravotníckej pomôcky dostatočne flexibilná na to, aby reflektovala nové trendy v oblasti nositeľných zdravotných technológií. Možno bude potrebné prehodnotiť regulačné kritériá, aby sa zabezpečilo, že potenciálne zdravotné prínosy týchto technológií budú v právnom rámci primerane uznané.

Záver

V posledných rokoch možno pozorovať exponenciálny nárast inteligentných nositeľných zariadení, najmä inteligentných hodínok, ktoré zaznamenávajú a spracúvajú zdravotné údaje alebo poskytujú používateľom praktické informácie o ich zdravotných parametroch. Komerčné zariadenia poháňané umelou inteligenciou, ako sú inteligentné hodinky, už nie sú iba jednoduchými fitness náramkami. Dnes ich funkcionality presahuje základné prvky, ako je počítanie krokov či sledovanie polohy prostredníctvom GPS. Naopak, ide o technologicky vyspelé nástroje, ktoré obsahujú širokú škálu funkcií navrhnutých na monitorovanie zdravia a fyzickej aktivity používateľov. Avšak, pochopenie rozdielu medzi wellness údajmi a zdravotnými údajmi, ako aj obmedzení údajov zhromaždených prostredníctvom nositeľných technológií, môže byť pre bežných používateľov bez medicínskeho vzdelania náročné.²⁶

Presnejšia právna definícia by odstránila nejasnosti týkajúce sa klasifikácie inteligentných nositeľných zariadení. Konkrétne, súčasné Nariadenie o zdravotníckych pomôckach by mohlo byť novelizované s cieľom poskytnúť jasnejšiu a explicitnú definíciu nositeľných zariadení, ktoré sú určené na monitorovanie zdravia. To by znamenalo, že všetky zariadenia ponúkajúce významné možnosti zdravotného monitorovania, vrátane dátovo orientovaných technológií, by mohli podliehať prísny štandardom, ako aj režimom bezpečnosti, presnosti a certifikácie.

²⁶ Scheid, J. L., Reed, J. L., West, S. L. Commentary: Is Wearable Fitness Technology a Medically Approved Device? Yes and No. In: *International Journal of Environmental Research and Public Health*. 20 (13), (2023), s. 2.

Ďalším navrhovaným konceptom je viacstupňový certifikačný systém, ktorý by klasifikoval nositeľné zariadenia podľa ich funkcionality a medicínskeho prínosu, napríklad:

1. Úroveň: zariadenia poskytujúce všeobecné informácie o zdraví a kondícii
2. Úroveň: zariadenia schopné monitorovať základné zdravotné ukazovatele (napr. monitorovanie srdcového rytmu)
3. Úroveň: zariadenia s prediktívnou diagnostikou, ktoré by už mali byť považované za zdravotnícke pomôcky

Takýto stupňovitý prístup umožňuje flexibilitu, vďaka ktorej môžu byť technologicky vysoko vyspelé zariadenia, ako sú inteligentné hodinky s medicínskym potenciálom, vystavené primeranej úrovni regulácie, pričom sa zároveň nebrzdí inovácia v oblasti spotrebiteľských produktov.

Uvedené všeobecné certifikačné stupne by sme mohli doplniť o analytické kritéria, ktoré umožnia lepšie posúdenie inteligentných nositeľných technológií z hľadiska ich regulačného zaťaženia vzhľadom na inovatívnosť, ktorou disponujú. Tieto kritériá totiž zohľadnia reálne osobitosti týchto zariadení, ako aj praktickú interakciu používateľa so zariadením:

1. Miera autonómie zariadenia
Otázka: Vyhodnocujú inteligentné nositeľné zariadenia dáta samé alebo slúžia len ako pasívny zberač údajov?
Príklad: Inteligentné hodiny, ktoré dokážu vyhodnotiť nepravidelný srdcový rytmus a poslať varovanie, predstavujú vyšší regulačný záujem než zariadenie, ktoré len zaznamenáva tep.
2. Dopad výstupov na rozhodovanie o zdraví
Otázka: Slúžia výstupy inteligentného nositeľného zariadenia ako podklad pre klinické rozhodovanie alebo len ako informačný doplnok?
Príklad: Ak pacient na základe výstrahy zo svojich inteligentných hodínok upraví liečbu, mal by mať výrobca zodpovednosť za presnosť takýchto výstupov.
3. Miera personalizácie a učenia systému
Otázka: Prispôsobuje sa inteligentné nositeľné zariadenie konkrétnemu používateľovi? Učí sa zo správania alebo zdravotnej histórie?
Príklad: Adaptívne algoritmy, ktoré menia správanie na základe predchádzajúcich výsledkov, by mali podliehať vyššiemu regulačnému dohľadu.
4. Predpokladané správanie používateľa
Otázka: Je pravdepodobné, že používateľ bude inteligentné nositeľné zariadenie vnímať ako diagnostický nástroj?

Príklad: Ak dizajn a marketing inteligentných hodín navodzujú dojem, že ide o diagnostický nástroj (napr. „odhalí srdcové arytmie“), mali by sa prísnejšie regulované – bez ohľadu na zámer výrobcu.

Ak legislatíva nedokáže flexibilne reagovať na rýchlo sa vyvíjajúce technológie, vzniká tzv. regulačné vákuum, v ktorom môže dôjsť k nejasnosti právnej zodpovednosti pri zlyhaní technológie, k nedostatočnej ochrane pacientov pri nesprávnej interpretácii dát, k brzdeniu inovácií, ak výrobca nevie, do ktorej kategórie bude jeho produkt zaradiť a k rôznym ďalším rizikám. Zároveň vzniká trhová asymetria, kde niektorí výrobcovia investujú do certifikácie, zatiaľ čo iní uvádzajú podobné produkty na trh ako „lifestyle“ zariadenia bez zodpovedajúcej právnej zodpovednosti. Jednou z možných ciest na premostenie regulačného deficitu sú tiež prechodné režimy certifikácie, ktoré umožnia vývojárom postupne overovať funkcie zariadení podľa ich reálneho využitia a rizikovosti. Takýto postup by mohol predstavovať flexibilný nástroj na posúdenie nových technológií pred ich plnohodnotným zaradením do kategórie zdravotníckych pomôcok.

Tento príspevok skúma špecifický aspekt inteligentných nositeľných zariadení, ktorý umožňuje monitorovanie vybraných zdravotných ukazovateľov v domácom prostredí alebo v neklinických podmienkach a poskytovanie relevantných zdravotných informácií. Hoci inteligentné hodinky ponúkajú sľubný pokrok v oblasti diaľkového monitorovania zdravia, významné právne a technické bariéry pretrvávajú. Výsledky poukazujú na to, že súčasný právny rámec v EÚ zatiaľ nereflektuje rastúcu úlohu nositeľných zariadení poháňaných umelou inteligenciou v zdravotnej starostlivosti. Zastarané definície a regulácie obmedzujú ich potenciál a spomaľujú ich využívanie v medicínskej praxi. Aby bolo možné tieto technológie bezpečne a efektívne využívať, legislatíva sa bude musieť zmeniť tak, aby reflektovala nové kategórie technológií a ich dopad na zdravotnú starostlivosť.

Zoznam použitej literatúry

1. BOHR, Adam, MEMARZADEH, Kaveh. Artificial Intelligence in Healthcare. London: Academic Press, 2020, 355 s. ISBN: 978-0-12-818438-7. Dostupné na: <https://www.sciencedirect.com/book/9780128184387/artificial-intelligence-in-healthcare?via=ihub=>
2. BOUDERHEM, Rabia. Privacy and Regulatory Issues in Wearable Health Technology. In: *Engineering Proceedings*. Roč. 58, č. 1 (2023). Dostupné na: <https://www.mdpi.com/2673-4591/58/1/87>
3. CANALI Stefano, SCHIAFFONATI Viola, ALIVERTI Andrea. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. In: PLOS Digit Health. Roč. 1(10) (2022).

Dostupné

na:

<https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000104>

4. DEVINE, Jaime K., SCHWARTZ, Lindsay P., & HURSH, Steven R. Technical, Regulatory, Economic, and Trust Issues Preventing Successful Integration of Sensors into the Mainstream Consumer Wearables Market. In: Sensors. Roč. 22, č. 7, (2022). Dostupné na: <https://pubmed.ncbi.nlm.nih.gov/35408345/>
5. EUROPEAN PARLIAMENR AND COUNCIL. Regulation of the European Parliament and the Council (EU) no. 2017/745 on medical devices, amending Directive 2001/83/EC, Regulation (EC) no. 17.8/2002 and Regulation (EC) No. 1223/2009 and on the repeal of Council Directives 90/385/EEC and 93/42/EEC.
6. EUROPEAN PARLIAMENR AND COUNCIL. Regulation of the European Parliament and of the Council (EU) no. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
7. EUROPEAN PARLIAMENR AND COUNCIL. Regulation of the European Parliament and the Council (EU) no. 2025/327 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.
8. EUROPEAN COMMISION. MEDDEV 2.1/6 – Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. 2016.
9. HOSSEINI, Mohsen Masoumian, HOSSEINI Seyedeh Toktam Masoumian, QAYUMI, Karim, HOSSEINZADEH, Shahriar, TABAR Seyedeh Saba Sajadi. Smartwatches in healthcare medicine: assistance and monitoring; a scoping review. In: BMC Medical Informatics and Decision Making. Roč. 23(1) (2023). Dostupné na: https://pmc.ncbi.nlm.nih.gov/articles/PMC10625201/pdf/12911_2023_Article_2350.pdf
10. IQBAL Jeffrey David, BILLER-ANDORMO, Nikola. The regulatory gap in digital health and alternative pathways to bridge it. In: Health Policy and Technology. Roč. 11, č. 3, 100663, 2022, ISSN 2211-8837, <https://doi.org/10.1016/j.hlpt.2022.100663>.
11. LU Lin, ZHANG Jiayao, XIE Yi, GAO Fei, XU Song, WU Xinghuo., YE Zhewei. Wearable Health Devices in Health Care. In: Narrative Systematic Review, JMIR Mhealth Uhealth. Roč. 8, č. 11 (2020). Dostupné na: <https://mhealth.jmir.org/2020/11/e18907/PDF>
12. LUKOWICZ, Paul, KIRSTEIN, Tristan, TRÖSTER, G. Wearable systems for health care applications. In: Methods of information in medicine. 43. 232-8, (2004). Dostupné na:

https://www.researchgate.net/publication/8480044_Wearable_systems_for_health_care_applications

13. MOSHAWRAB, Mohammad, ADDA, Mehdi, BOUZOUANE, Abdenour, IBRAHIM, Hussein, RAAD, Ali. Smart Wearables for the Detection of Occupational Physical Fatigue: A Literature Review. In: Sensors. Roč. 22, 7472. (2022). Dostupné na: <https://www.mdpi.com/1424-8220/22/19/7472#B82-sensors-22-07472>
14. MEDICAL COORDINATION GROUP. MDCG 2021-24 Guidance on classification of medical devices. 2021.
15. PIWEK, Lukasz, ELLIS, David. A., ANDREWS, Sally, JOINSON, Adam. The Rise of Consumer Health Wearables: Promises and Barriers. In: PLoS Medicine. Roč. 13, č. 2, (2016). Dostupné na: <https://doi.org/10.1371/journal.pmed.1001953>
16. SHAIK, Thansveer, TAO, Xiaohui, HIGGINS, Niall, LI, Lin, GURURAJAN, Raj, ZHOU, Xujuan, & ACHARYA, Rajendra. Remote patient monitoring using artificial intelligence: Current state, applications, and challenges. In: WIREs DataMining and Knowledge Discovery. Roč. 13, č. 2 (2023). Dostupné na: <https://doi.org/10.1002/widm.1485>
17. SCHEID, Jennifer L., REED, Jennifer L., WEST, Sarah L. Commentary: Is Wearable Fitness Technology a Medically Approved Device? Yes and No. In: International Journal of Environmental Research and Public Health. Roč. 20 (13), (2023), Dostupné na: <https://www.mdpi.com/1660-4601/20/13/6230>
18. TONG, Raymond Kai-Yu Wearable Technology in Medicine and Health Care. London: Academic Press, 2018, ISBN 978-0-12-811810-8. Dostupné na: <https://www.sciencedirect.com/book/9780128118108/wearable-technology-in-medicine-and-health-care>

Kontaktné údaje

doc. JUDr. Soňa Sopúchová, PhD.
sona.sopuchova@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta

VÝVOJ A NAJNOVŠIE TRENDY PRI APLIKÁCIÍ AKTU DSA V POMEROCH KOLABORATÍVNEHO HOSPODÁRSTVA S OHĽADOM NA ZODPOVEDNOSŤ PLATFORMIEM¹

DEVELOPMENT AND LATEST TRENDS IN THE APPLICATION OF THE DSA IN THE CONTEXT OF THE COLLABORATIVE ECONOMY WITH REGARD TO PLATFORM RESPONSIBILITY

Lukáš Macko²

Abstrakt: Príspevok analyzuje uplatňovanie Aktu o digitálnych službách (DSA) v oblasti kolaboratívneho hospodárstva so zameraním na zodpovednosť online platformiem a nové regulačné mechanizmy. Vychádza z kombinácie právnej analýzy, hodnotenia judikatúry Súdneho dvora EÚ a dostupných empirických údajov o povedomí spotrebiteľov. Osobitná pozornosť sa venuje inštitútu dôveryhodných nahlasovateľov, ktorý predstavuje zásadnú novinku oproti smernici o elektronickom obchode. Príspevok zdôrazňuje jeho možné prínosy, ale aj riziká spojené s nedostatočnou transparentnosťou, rozdielnymi výkladmi členských štátov a potenciálnym zásahom do slobody prejavu. Dôležitou súčasťou je aj analýza rozsudku *Zalando/Komisia*, ktorý spresňuje kritériá na určovanie veľmi veľkých online platformiem a posilňuje požiadavky na transparentnosť vykazovania aktívnych príjemcov služby. Empirické zistenia ukazujú nízku úroveň verejného povedomia o právach vyplývajúcich z DSA, čo znižuje jeho praktickú účinnosť. Výsledky naznačujú, že napriek ambicióznemu cieľu posilniť bezpečné a transparentné digitálne prostredie zostáva aplikácia DSA sprevádzaná interpretačnými problémami, nerovnomernou implementáciou a potrebou ďalšieho metodického usmernenia.

Kľúčové slová: zodpovednosť, nariadenie DSA, spotrebiteľ, dôveryhodný nahlasovateľ

Abstract: The paper examines the application of the Digital Services Act (DSA) within the collaborative economy, focusing on the liability of online platforms and the introduction of new regulatory mechanisms. It draws on a combination

¹ Tento príspevok je publikovaný v rámci projektu ALTAML č. 09l05-03-V02-00049

² Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave

of legal analysis, an assessment of the case law of the Court of Justice of the EU, and available empirical data on consumer awareness. Particular attention is paid to the institute of trusted flaggers, which represents a significant novelty compared to the former E-Commerce Directive. The paper highlights both their potential benefits and the risks associated with insufficient transparency, divergent interpretations among Member States, and possible interference with freedom of expression. An important part of the analysis is the *Zalando/Commission* judgment, which clarifies the criteria for designating very large online platforms and strengthens the transparency requirements related to reporting the number of active recipients of the service. Empirical findings reveal a low level of public awareness of the rights arising from the DSA, which reduces its practical effectiveness. The results suggest that despite the DSA's ambitious goal of enhancing a safe and transparent digital environment, its application remains accompanied by interpretative challenges, uneven implementation, and the need for further methodological guidance.

Key words: liability, DSA regulation, consumer , trusted flagger

Úvod

Kolaboratívne hospodárstvo je neoddeliteľne prepojené s právom informačných a komunikačných technológií, predstavujúc súbor právnych noriem upravujúcich samostatné vzájomne nezávislé a vysoko špecializované právne oblasti. Tieto oblasti sa dynamicky vyvíjajú v dôsledku rýchleho technologického pokroku a praktickej implementácie nových inovácií.

Odvetvie kolaboratívneho hospodárstva patrí k najnovším segmentom európskej ekonomiky a jeho vznik je spojený so štvrtou priemyselnou revolúciou, často označovanou aj ako digitálna revolúcia. Podľa Európskej komisie je cieľom kolaboratívneho hospodárstva prispieť k vytvoreniu stabilného a jednotného digitálneho trhu (JDT), ktorý zahŕňa aj úpravu zodpovednostných vzťahov vyplývajúcich z využívania digitálnych platforiem spotrebiteľmi.

Akt DSA je navrhnutý tak, aby zabezpečil riadne fungovanie JDT, najmä prostredníctvom regulácie cezhraničných online sprostredkovateľských služieb. Medzi hlavné ciele Aktu DSA³ patrí: zachovanie bezpečného online prostredia, zlepšenie podmienok pre inovatívne cezhraničné digitálne služby, posilnenie postavenia používateľov a ochrana ich základných práv online, ako aj zavedenie

³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES

efektívneho dohľadu nad digitálnymi službami a podporu spolupráce medzi príslušnými orgánmi.

Možno povedať, že zavádza nový regulačný prístup zameraný na systémové riziká spojené s fungovaním veľkých online platforiem. V súvislosti s tým sa v tomto článku identifikujú viaceré otázky a trendy aplikácie Aktu DSA s osobitným zameraním na úlohu dôveryhodných oznamovateľov. Ďalej sa analyzuje všeobecné povedomie spotrebiteľov o tomto regulačnom rámci, ako aj súčasné trendy vyplývajúce z judikatúry Súdného dvora Európskej únie, predovšetkým vo veci Zalando vs. Komisia.⁴

Dôveryhodní nahlasovatelia a ich vplyv

Akt DSA okrem mnohých novín priniesol so svojou účinnosťou okrem iného aj inštitút dôveryhodných nahlasovateľov, ktorý je oproti pôvodnej úprave obsiahnutej v Smernici o elektronickom obchode⁵ nový. Nemožno však povedať, že inštitút dôveryhodných nahlasovateľov by v kultúre online sveta bol neznámym. Už v minulosti spoločnosti ako Meta a iné poskytovali možnosť nahlasovať nezákonný obsah prostredníctvom funkcionality s označením fact-checking. Možno však povedať, že na rozdiel od dobrovoľnosti, na ktorej bolo založené moderovanie obsahu nezávislými tretími osobami nazývanej fact-checking, inštitút dobrovoľného nahlasovateľa má daný priamo právny základ nachádzajúci sa v čl. 22 Aktu DSA. Zákonodarca na úrovni EÚ pristúpil ku kreovaniu tohto inštitútu z dôvodu rýchlejšej a efektívnejšej ochrany používateľov platforiem naprieč členskými štátmi. Už zo samotného odôvodnenia 61 Aktu DSA vyplýva, že sa mu kladie vysoká úroveň odbornosti a zabezpečenia plynulého vybavovania sťažností týkajúcich sa nezákonného obsahu.⁶

Vymedzenie inštitútu dôveryhodného nahlasovateľa možno vyabstrahovať z vyššie spomenutého čl. 22 Aktu DSA. Podľa tohto článku aj s ohliadnutím na odôvodnenie 61 Aktu DSA možno jednoznačne povedať, že postavenie a priznanie štatútu dôveryhodného nahlasovateľa určitému subjektu podlieha viacerým kritériám. Po prvé, vo vzťahu ku koordinátorovi digitálnych služieb, ktorým je napríklad na území Slovenskej republiky Rada pre mediálne služby musí smerovať žiadosť, ktorú koordinátor musí posúdiť v súvislosti so splnením kvalifikačných štandardov kladených na status dôveryhodného nahlasovateľa podľa čl. 22 ods. 2 Aktu DSA. Ako sme už spomenuli, na území Slovenskej republiky je koordinácia postupu v úplnej

⁴ Rozsudok SDEÚ vo veci Zalando/Komisia zo dňa 03.09.2025, sp.zn.: T-348/23

⁵ Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode

⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES

gescii Rady pre mediálne služby, ktorá má na svojej stránke uverejnený postup podávania žiadosti ako aj samotné formulárové tlačivo.⁷

Po krátkom úvode však možno treba do veci vniesť aj trochu kritického pohľadu. Aj keď sa zdá aplikácia a fungovanie tohto inštitútu ako bezproblémové, nie je tomu tak. Možno to vidieť na pomerne malom počte doposiaľ registrovaných dôveryhodných nahlasovateľov naprieč všetkými členskými štátmi, ktorých je aj napriek účinnosti Aktu DSA už tretí rok pomerne málo a to 42⁸ čo sa javí s ohľadom na veľkosť digitálneho trhu ako nedostatočné nevynímajúc fakt, že na území Slovenskej republiky doposiaľ nemáme registrovaný žiadny takýto subjekt. Otázkou zostáva prečo tomu tak je, môže za to zložitý byrokratický proces alebo len nedostatok celospoločenskej vedomosti? Asi by bolo dobré zdôrazniť, že inštitút dôveryhodných nahlasovateľov v žiadnom prípade nenahrádza možnosť podávania individuálnych sťažností používateľov na odstránenie nezákonného obsahu, Akt DSA však ráta s tým, že sťažnosti nahlasovateľov budú kvalifikované a budú sa týkať len oprávnených podnetov a preto im priznáva aj prioritnú povahu pri ich vybavovaní. Viaceré riziká spojené s inštitútom dôveryhodných nahlasovateľov možno charakterizovať do troch základných oblastí. Prvou je otázka transparentnosti a zneužívania nahlásení čo môže viesť na konci dňa k moderovaniu obsahu na platformách, ktorý nezákonným aj nie je.

Po druhé, ak sa zastavíme pri otázke transparentnosti, možno povedať, že určité subjekty, ktoré by získali štatút dôveryhodného nahlasovateľa môžu zastupovať určité názorové hľadiská. Vzhľadom na to, že zo samotného odôvodnenia 61 Aktu DSA a článkov 20 až 22 vyplýva priorita vybavovania sťažností podaných dôveryhodnými nahlasovateľmi, môže sa ľahko stať, že ich kompetencie budú zneužívané. V odbornej verejnosti sa tento jav nazýva rubberstamping. Túto situáciu možno charakterizovať ako stav, keď platforma obmedzuje obsah bez akéhokoľvek hlbšieho posúdenia z dôvodu, že bol nahlásený práve dôveryhodným nahlasovateľom, u ktorého sa ráta, že pôjde o oprávnené nahlásenie. Z uvedeného možno vyabstrahovať, že opakované nahlasovanie bez právneho a skutkového dôvodu by mohlo viesť k nadmernému obmedzovaniu slobody prejavu a práva na informácie, čo by nebolo v súlade so samotnou Chartou. V Európskej únii je sloboda prejavu chránená článkom 11 Charty základných práv, ktorý v súlade s článkom 52 ods. 3 Charty základných práv možno vykladať na základe judikatúry Európskeho súdu pre ľudské práva týkajúcej sa článku 10 Európskeho dohovoru o ľudských právach (EDLP), keďže tieto články sa týkajú

⁷ Odkaz na stránku Rady pre mediálne služby, kde možno dohľadať postupy k podaniu žiadosti.: <https://rpms.sk/ziadost-o-statut-doveryhodneho-nahlasovateľa>

⁸ Zoznam doposiaľ registrovaných zodpovedných nahlasovateľov v členských štátoch EÚ.: <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>

toho istého práva. Sloboda prejavu zahŕňa právo vyjadriť sa na internete (napr. Melike proti Turecku, 35786/19 (2021), ESLP) a právo na informácie.⁹

Odstránenie obsahu môže tak zasahovať do tohto práva, buď obmedzením prejavu používateľa internetu, alebo práva na informácie používateľa internetu, ktorý už nemá prístup k tomuto obsahu. Zasahovanie do týchto práv je povolené, ak spĺňa požiadavky článku 52 ods. 1 Charty základných práv EÚ, t. j. ak sleduje legitímny cieľ, je stanovené zákonom a je nevyhnutné v demokratickej spoločnosti. Takéto zásahy sú zvyčajne predmetom súdneho preskúmania, pri ktorom sa posudzuje, či sú splnené uvedené požiadavky čo sa však neuplatňuje v prípade dôveryhodných nahlasovateľov. Takéto posúdenie totiž nevykonáva súdny orgán, ale subjekt, ktorý podáva oznámenie, a nakoniec platforma, ktorá moderuje obsah. Hoci konečné vyvažovanie skutočne vykonáva platforma, je možné, že tlak vyplývajúci z takýchto žiadostí privilegovaných subjektov vedie k odstráneniu obsahu. To môže viesť k scenáru, v ktorom hoci platforma dobrovoľne rozhodne o odstránení obsahu, tlak vyvíjaný na základe žiadosti o odstránenie, ktorá vedie k odstráneniu, môže zasahovať do slobody prejavu používateľa internetu.

Napätie v súvislosti so základnými právami existuje v prípade súkromných subjektov, ktoré pôsobia ako dôveryhodní nahlasovatelia, ako aj v prípade vládnych subjektov, ktoré pôsobia ako dôveryhodní nahlasovatelia. Súkromné subjekty nie sú priamo viazané normami základných práv ale majú zodpovednosť, implicitne v judikatúre členských štátov EÚ a explicitne v Akte DSA, napr. v článku 14 ods. 4, dodržiavať normy základných práv pri poskytovaní svojich služieb. Pre štátne subjekty môže konanie ako dôveryhodný nahlasovateľ vytvoriť relevantnejšie napätie v oblasti základných práv. Štátne subjekty nesú osobitnú zodpovednosť, pokiaľ ide o slobodu prejavu používateľov internetu, a to vo väčšej miere ako platformy. Štátne subjekty, ktoré vydávajú neformálne žiadosti o odstránenie, môžu zasahovať do slobody prejavu pretože ich oznámenia majú pravdepodobne väčšiu váhu vzhľadom na potenciálne regulačné sankcie, ktoré môžu nasledovať v prípade nedodržania.¹⁰

Okrem obáv o slobodu prejavu môžu v prípadoch, keď štátne subjekty fungujú ako dôveryhodní nahlasovatelia, existovať aj obavy o dodržiavanie zásad právneho štátu, vzhľadom na ich povinnosť konať v súlade so zákonom. Moderovanie obsahu sa zakladá buď na zákone, alebo na smerniciach komunity platforiem. Úloha dôveryhodného nahlasovateľa poskytuje štátnym subjektom privilegovaný kanál na podávanie oznámení na základe smerníc komunity, čo vytvára napätie v oblasti právneho štátu, de facto by štátne subjekty mohli presadzovať súkromné smernice, nie zákon. V rámci právneho štátu potrebujú štátne subjekty právny základ na

⁹ Husovec M. Principles of the Digital Services Act. Oxford: Oxford University Press; 2024

¹⁰ Husovec, M.: The DSA's Scope Briefly Explained, Husovec, Martin, The DSA's Scope Briefly Explained, 2023

moderovanie obsahu, aj keď to znamená len povzbudenie platforiem, aby presadzovali svoje vlastné smernice komunity.

Vo vzťahu k transparentnosti procesu nahlasovania sťažnosti možno uviesť najmä to, že neprehľadným sa stáva najmä mechanizmus dohôd medzi platformami a samotnými dôveryhodnými nahlasovateľmi. Aj keď článok 22 ods. 3 Aktu DSA ráta s podávaním správ o činnosti nahlasovateľov v snahe predísť vnútorným dohodám medzi nahlasovateľmi a platformami, ktoré by mohli spôsobiť obmedzenie voľného trhu, javí sa ako problematické zabezpečiť riadne fungovanie tohto odseku. Problematickým je totiž preukázanie skutočnosti či naozaj platforma a určitý nahlasovateľ môžu vytvárať potencionálne riziko pre ostatné platformy v súvislosti s nahlasovaním obsahu. Problematickým je najmä skutočnosť ako preukázať vnútorný vzťah medzi týmito subjektmi v prípade dokazovania na súde.

Aj keď síce samotný Akt DSA poskytuje riešenie v prípade nadmerných sťažností, riziko nadmerného odstraňovania obsahu vyplýva z toho, že dôveryhodní nahlasovatelia zastupujú špecifické záujmy, čo vedie k agresívnym postupom nahlasovania, ktoré nevyvážajú slobodu prejavu so záujmami, ktoré zastupujú. Toto riziko môže existovať pri interpretácii výberových kritérií pre dôveryhodných nahlasovateľov podľa článku 22 Aktu DSA.¹¹

Výberové kritériá článku 22 ods. 2 DSA sú viacerými spôsobmi interpretovateľné a môžu byť ovplyvnené národnými preferenciami, keďže dôveryhodní nahlasovatelia sú nakoniec certifikovaní národnými autoritami. V prostredí EÚ, kde dochádza k úpadku právneho štátu a postoje k slobode prejavu sa v jednotlivých regiónoch líšia, je možné, že vybrané organizácie by mohli predstavovať riziko pre slobodu prejavu. Takéto organizácie by mohli potenciálne podávať nadmerný počet oznámení online platformám, čo by viedlo k nadmernému odstraňovaniu obsahu. Výberové kritériá stanovené v článku 22 preto neposkytujú účinnú ochranu pred týmto javom. Ďalším problémom, ktorý sa v súvislosti s aplikáciou čl. 22 Aktu DSA javí je, že Akt DSA nešpecifikuje prostriedky, ktoré musia dôveryhodní nahlasovatelia používať na detekciu obsahu. Kým niektorí dôveryhodní nahlasovatelia sa spoliehajú na vlastné vyšetrovanie, čo predstavuje skôr remeselný, prípadový prístup k moderovaniu obsahu, iní sa môžu snažiť používať algoritmické prostriedky na prístup k moderovaniu obsahu alebo hľadať prostriedky na detekciu nezákonného obsahu. Problém v nahlasovaní nezákonného obsahu spočíva v tom, že aj keď by určitý nahlasovateľ podával opakovane sťažnosti na detekciu nezákonného obsahu, čo by platformu nútilo k nadmernému moderovaniu, je potrebné povedať, že aj v prípade ak by sa preukázalo zneužitie alebo nedostatočné posúdenie, za určitých okolností nahlasovatelia nemusia uvedené prípady uvádzať v ročných výkazoch tak ako to

¹¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES

vyžaduje od nich čl. 22 Aktu DSA. Ak sa totiž pozrieme na dikciu čl. 16 Aktu DSA, ten vyžaduje, aby oznámenia boli podávané na základe *nezákonného obsahu*, ktorý je v článku 3 písm. h) DSA definovaný ako „*akákoľvek informácia, ktorá nie je v súlade s právom Únie alebo právom ktoréhokoľvek členského štátu, ktoré je v súlade s právom Únie*“.

Napriek dodatočnej úrovni zodpovednosti existujú medzery v uplatňovaní nahlasovania prostredníctvom čl. 16, ktoré predstavujú riziko pre právny štát, a to nielen pre štátne subjekty, ale aj pre všetkých dôveryhodných nahlasovateľov. Aj keď článok 16 špecifikuje, že oznámenia môžu byť podávané iba v prípade nezákonného obsahu, menovaní dôveryhodní nahlasovatelia môžu na základe podmienok používania služby de facto označovať obsah, nie len v rámci článku 16.

Ak je oznámenie podané mimo článku 16, nie je potrebné podávať transparentné správy o takýchto oznámeniach podľa článku 22 ods. 3. Naopak, neočakáva sa, že online platformy budú týmto oznámeniam poskytovať rovnakú prioritu a rýchlosť. Odôvodnenie 62 však naznačuje, že online platformy by mali poskytovať podobné (prioritné) zaobchádzanie s oznámeniami podanými subjektmi, ktorým nebol udelený status dôveryhodného nahlasovateľa, aby „mohli prijať rýchle a spoľahlivé opatrenia proti obsahu, ktorý je nezlučiteľný s ich podmienkami používania“.

Ďalším bodom v rámci rámca dôveryhodných nahlasovateľov podľa Aktu DSA, ktorý predstavuje výzvu pre právny štát, je nadnárodný charakter internetu. Obsah, ktorý je v jednom členskom štáte nezákonný, môže byť v inom členskom štáte zákonný, ale dôveryhodní nahlasovatelia bojujúci proti nezákonnému obsahu získavajú svoj status pre celú EÚ. To môže viesť k odstráneniu obsahu, ktorý je potenciálne zákonný v danom členskom štáte, ale nezákonný v inom. Príkladmo možno uviesť, že obsah súvisiaci s LGBT+ v reklamách je nezákonný v Maďarsku (zákon LXXIX z roku 2021), ale nie v iných členských štátoch EÚ (Európska komisia proti Maďarsku, C-769/22 (2022), SDEÚ). Maďarský dôveryhodný nahlasovateľ by mohol tento obsah nahlasovať mimo Maďarska, čo by viedlo k jeho odstráneniu z dôvodu nedostatočnej ostražitosti online platformy, aj keď v danom členskom štáte chýba právny základ. Rozhodnutie o tom, či je právny základ pre podané oznámenie platný v inom členskom štáte, je ponechané na uvážení dôveryhodného nahlasovateľa a na uvážení platformy, ktorá nakoniec rozhoduje o tom, či bude obsah obmedzený, čo opätovne bude viesť k obmedzeniu slobody prejavu.

Vedomosť spotrebiteľov o Akte DSA

Zo štúdií, ktoré boli na vzorke spotrebiteľov urobené v posledných mesiacoch, najmä vo vzťahu k ich vedomosti o Akte DSA vyplýva, že aj napriek takmer trojročnej účinnosti je Akt DSA pomerne stále v laickej verejnosti neznámy. Problematickým sa javí najmä fakt, že bežní používatelia internetu si často neuvedomujú, že Akt DSA sa

dotýka aj ich práv – napríklad pokiaľ ide o možnosť nahlasovať nelegálny obsah, byť informovaní o dôvodoch odstránenia príspevku či získať väčšiu ochranu pred škodlivými praktikami digitálnych platforiem. Názor, ktorý vo verejnosti prevláda hovorí jasne za to, že spotrebitelia sa väčšinou domnievajú, že Akt DSA je určený veľkým technologickým platformám a bežného spotrebiteľa sa nijako nedotýka.

Na základe štúdie vykonanej organizáciou CEDMO s názvom Poznatelnosť a postoje populácie k DSA má prehľad o tomto dôležitom právnom predpise iba približne pätina respondentov – priemerne 20 % v deviatich skúmaných európskych krajinách.¹² Z hľadiska socio-demografických faktorov sa ukazuje, že muži (25 %) majú o DSA väčšie povedomie než ženy (16 %). Vyššiu informovanosť deklarujú aj mladí ľudia do 34 rokov (25 %), obyvatelia väčších miest (23 %), osoby s vysokoškolským vzdelaním (25 %) či respondenti, ktorí používajú sociálne siete denne (20 %) alebo aspoň raz týždenne (23 %).

Pri pohľade na socio-demografické ukazovatele sa výsledky podobajú na tie z otázky týkajúcej sa povedomia o existencii Aktu DSA. Muži (21 %) sa častejšie považujú za informovaných než ženy (14 %). Lepšie sa orientujú aj mladší ľudia do 34 rokov (25 %), obyvatelia väčších miest (18 %) a tí, ktorí používajú sociálne siete denne (19 %). Tieto trendy sú do istej miery očakávané pretože práve tieto skupiny patria medzi digitálne zdatnejšie, trávajú viac času online a aktívnejšie sledujú technologické či spoločenské témy.

Pri skúmaní obsahu, ktorí užívatelia vnímajú za najviac škodlivý panuje zhoda, že ide najmä o detskú pornografiu, za tým nasleduje obsah podporujúci terorizmus a iné, pričom najsilnejšie presvedčenie panuje v Nemecku a Estónsku.

Pozoruhodným je však posudzovanie nezákonného obsahu vo vzťahu k nenávistným prejavom. Aj vo vyspelých krajinách ako Fínsko tento typ obsahu považuje za nezákonný len zhruba 40 percent respondentov. Pod priemerom sú aj Česko (52 %) a Estónsko (50 %).

Za najmenej nebezpečné online hrozby považujú ľudia porušovanie autorských práv (41 %) a predaj zakázaného či falšovaného tovaru (48 %). Najnižšia miera obáv sa objavuje vo Fínsku (23 %) a Česku (31 %). Kým pri autorských právach môže ísť o dôsledok dlhodobiejšieho zľahčovania pirátstva, ktoré mnohí nevnímajú ako priamu hrozbu pre jednotlivca, pri falšovanom tovare pretrváva presvedčenie, že škodu

¹² Spracované podľa CEDMO Tracking V4+5 – 1. vlna očami Ipsosu: Poznatelnosť a postoje populácie k DSA, 21.08.2025, dostupné na <https://cedmohub.eu/sk/cedmo-tracking-v45-1-vlna-ocami-ipsosu-poznatelnost-a-postoje-populacie-k-dsa/>

utrpia najmä veľké značky, nie konkrétni ľudia. V Česku k tomu prispieva aj kultúrna tolerancia k pirátstvu, ktorá sa sformovala už v 90. rokoch.¹³

Súdny spor Zalando/Komisia

V súvislosti s uplatňovaním čl. 33 ods. 1, 2 a 3 Aktu DSA sa od jeho prijatia a nadobudnutia účinnosti u viacerých poskytovateľov služieb prejavuje neistota, či spadajú pod kategóriu veľmi veľkých online platforiem (VLOP). Komisia sa pri príprave na uplatňovanie Aktu DSA, najmä v súvislosti so zverejňovaním informácií o priemernom mesačnom počte používateľov platformy, zameriava na otázku určovania počtu aktívnych príjemcov služby v EÚ, čo je kľúčové pre zaradenie medzi VLOP. Táto problematika sa týka predovšetkým čl. 24 ods. 2 a odôvodnenia 77 Aktu DSA.

Situáciu ilustruje aj súdny spor medzi spoločnosťou Zalando SE ako žalobkyňou a Európskou komisiou ako žalovanou, vedený pod číslom T-348/23. Z obsahu žaloby zo dňa 27. júna 2023 vyplývalo, že mechanizmus určovania veľkosti VLOP je nedostatočne definovaný. Žalobkyňa namietala, že na ňu sa nevzťahuje Akt DSA, pretože nepôsobí ako sprostredkovateľská služba, a teda ani ako hostingová služba či online platforma podľa jeho definície. Ďalej tvrdila, že nedosahuje hranicu 45 miliónov používateľov, pričom otázkou ostáva jej „hybridný“ charakter – či ide o platformu sprístupňujúcu obsah tretím osobám. Ďalšími námietkami boli údajná nejasnosť čl. 33 ods. 1 v spojení s čl. 24 ods. 2 Aktu DSA a príliš nepresné požiadavky na výpočet prahovej hodnoty, čo podľa viacerých subjektov porušuje zásadu právnej istoty práva Únie.

Spor bol rozhodnutý SDEÚ dňa 3. septembra 2025, keď súd žalobu v plnom rozsahu zamietol. Rozsudok potvrdzuje široký výklad pojmu „aktívny príjemca“ a posilňuje regulačný rámec EÚ, pričom môže slúžiť ako precedens pre iné veľké e-commerce platformy kombinujúce vlastný predaj a predaj tretích strán.

Súd konštatoval, že aj platformy, ktoré kombinujú vlastný predaj a predaj tretích strán a vykonávajú určitú kontrolu nad obsahom, môžu byť považované za online platformy, pričom „aktívnym príjemcom“ je každá osoba vystavená obsahu, nie iba tá, ktorá uskutoční nákup. Rozsudok zároveň zdôraznil, že zásady právnej istoty a proporcionality nie sú porušené, ak sa norma flexibilne aplikuje na široké spektrum služieb.

Je potrebné povedať, že niektorí poskytovatelia online platforiem zohľadňujú aktívnych príjemcov len na svojich internetových stránkach, ale nie na svojich

¹³ Spracované podľa CEDMO Tracking V4+5 – 1. vlna očami Ipsosu: Poznatelnost' a postojе populácie k DSA, 21.08.2025, dostupné na <https://cedmohub.eu/sk/cedmo-tracking-v45-1-vlna-ocami-ipsosu-poznatelnost-a-postoje-populacie-k-dsa/>

zodpovedajúcich aplikáciách. Okrem toho tvrdí, že poskytovatelia online platforiem, na ktorých je dostupný tak ich obsah, ako aj obsah predávajúcich, ktorí sú tretími stranami, zohľadňujú len „príjemcov obsahu tretích strán“, a to aj vtedy, keď títo poskytovatelia prezentujú svoj vlastný obsah na tom istom rozhraní.

S týmto názorom sa treba vysporiadať tak, že konanie, ktoré je vyššie opísané a teda aj konanie spoločnosti Zalando, bolo v rozpore aj s nariadením 2022/2065. Treba uviesť, že na jednej strane sa v odôvodnení 77 nariadenia 2022/2065 uvádza, že príjemca služby „*by sa mal podľa možnosti započítať len raz*“, že toto nariadenie „nevyžaduje, aby poskytovatelia online platforiem osobitne sledovali jednotlivcov online“ a že ak sú poskytovatelia „schopní“ „bez ďalšieho spracovania osobných údajov a sledovania nezohľadňovať automatizovaných používateľov, ako sú boty alebo extrakcia dát, môžu tak urobiť“.

Nemožno však z toho vyvodit', že títo poskytovatelia môžu na účely výpočtu užívateľov nezohľadniť niektorých aktívnych príjemcov z dôvodu, že niektorí odmietli používanie súborov cookies a že nie je potrebné započítať boty. Z odôvodnenia 77 nariadenia 2022/2065 naopak vyplýva, že od poskytovateľov online platforiem sa môže vyžadovať, aby započítali boty, ak ich nie sú schopní vylúčiť bez ďalšieho spracovania osobných údajov alebo sledovania, ako aj to, aby započítali viackrát toho istého aktívneho príjemcu, hoci je cieľom „podľa možnosti“ započítať aktívnych príjemcov len raz. Títo poskytovatelia tak môžu byť za určitých okolností vedení k nadhodnoteniu užívateľov svojej online platformy v súlade s uvedeným nariadením. Naproti tomu im toto nariadenie neumožňuje podhodnocovať uvedený počet. Ako vyplýva z judikatúry pripomenutej v bode 78, vyššie uvedeným poskytovateľom prináleží najmä vybrať spoľahlivú metódu, ktorá môže zabezpečiť dodržanie požiadavky nepodhodnocovať dotknutý počet.

Skutočnosť, na ktorú poukazuje žalobkyňa, že článok 33 ods. 1 nariadenia 2022/2065 uvádza aktívnych užívateľov, a nie priemerný mesačný počet dotknutej online platformy, nemôže spochybniť tento záver. Toto ustanovenie, ako sa vykladá s prihliadnutím na odôvodnenie 77 tohto nariadenia, totiž nevedie k započítaniu všetkých týchto užívateľov, hoci by mohlo viesť k nadhodnoteniu počtu aktívnych príjemcov dotknutej online platformy. Na druhej strane, ako bolo pripomenuté v bode 60 vyššie, na to, aby bol príjemca služby kvalifikovaný ako aktívny príjemca online platformy v zmysle článku 3 písm. p) nariadenia 2022/2065, musí byť len v kontakte s touto platformou, najmä tým, že je vystavený informáciám uloženým touto platformou a šíreným prostredníctvom jej online rozhrania.

Z uvedeného vyplýva, že poskytovateľ online platformy nemôže na účely výpočtu užívateľov vylúčiť príjemcov služby, ktorí napriek tomu, že boli vystavení informáciám uloženým na tejto platforme, nie sú na nej prihlásení, neuzavreli v nej žiadne transakcie, určitý čas zostali nečinní, odmietli používanie súborov cookies alebo sa pripojili na platformu prostredníctvom aplikácie. V druhom rade žalobkyňa

tvrdí, že poskytovatelia online platforiem sa obávajú, že viackrát započítajú toho istého aktívneho príjemcu, ak sa spoľahnú len na počet konzultácií svojich online platforiem. Dodáva, že počet týchto duplikátov hodnotia odlišným spôsobom. Takéto okolnosti však nemôžu preukázať porušenie zásady právnej istoty z dôvodu nepresnosti pojmu „aktívny príjemca online platformy“ v nariadení 2022/2065.

Posledným problematickým faktorom je započítavanie na účely výpočtu užívateľov a to len príjemcov služby, ktorí na nich zostávajú dostatočne dlho. Spresňuje, že stanovená minimálna dĺžka sa v závislosti od dotknutého poskytovateľa pohybuje od 3 do 45 sekúnd a že výber tejto dĺžky trvania môže mať významný vplyv na výpočet užívateľov ich online platforiem. V tejto súvislosti je nepochybne nesporné, že užívateľ online platformy sa môže líšiť v závislosti od toho, či je stanovená minimálna dĺžka trvania 3 sekundy alebo 45 sekúnd, počas ktorej musia príjemcovia služby zostať na tejto platforme na to, aby boli započítaní ako aktívni príjemcovia.

V odôvodnení 77 nariadenia 2022/2065 sa však uvádza, že výpočet užívateľov, a teda počtu osôb vystavených informáciám uloženým online platformou, môže závisieť od „povahy služby a spôsobu interakcie príjemcov služby s ňou“. Okolnosť, že toto nariadenie nestanovuje abstraktne a pre všetky online platformy minimálnu dĺžku trvania, ktorú musia poskytovatelia týchto platforiem stanoviť na účely výpočtu užívateľov, teda nestačí na preukázanie toho, že neumožňuje konkrétne určiť užívateľov online platformy vzhľadom na charakteristiky vlastné tejto platforme.

Záver

Možno zdôrazniť, že prijatie Aktu DSA bolo dôležitým krokom potrebným na udržanie regulácie nezákonného obsahu na internete, ktorý nahradil pomerne zastaraný model založený ešte Smernicou E-commerce. Je však potrebné konštatovať, že aj napriek skoro trom rokmi od jeho účinnosti, stále zostali nezodpovedané viaceré otázky. Ako sme už v príspevku spomenuli, od počiatku sprevádzali nariadenie viaceré problémy najmä s výkladom a pomerne široko definovanými ustanoveniami, ktoré častokrát spôsobovali nedostatočnosť výkladu. Možno to reflektovať najmä na otázke určenia veľkosti platforiem, ktoré aj napriek viacerým Usmerneniam Komisie skončili súdnym sporom, ktorý bol skončený len nedávno. Ďalej možno povedať, že problematickým aj otázka zodpovedných nahlasovateľov, pri ktorých doposiaľ nie je jasný pomerne mechanizmus ich kreovania ako aj ďalšie otázky v súvislosti s ich činnosťou pri nahlasovaní nelegálneho obsahu. V neposlednom rade je potrebné povedať, že aj napriek pomerne dlhšiemu časovému obdobiu účinnosti Aktu DSA možno bádať nevedomosť širokej verejnosti o tomto právnom akte čo len umocňuje obavu pri zabezpečení plynulého moderovania a nezákonného obsahu

Zoznam použitej literatúry

1. Aade, L. The regulation of social media commerce under the DSA: A consumer protection perspective: *Computer Law & Security Review*, 2025, <https://doi.org/10.1016/j.clsr.2025.106181>.
2. Aade, L. The regulation of social media commerce under the DSA: A consumer protection perspective: *Computer Law & Security Review*, 2025, <https://doi.org/10.1016/j.clsr.2025.106181>.
3. Annabell T, Kelder T, van de Kerkhof J, Goanta C. Influencer as Individual and Trader: Exploring the Boundaries of Discrimination in Influencer Marketing from a Multidisciplinary Perspective. *J. Media and Cult. Stud.* 2025:1–16. <https://doi.org/10.1080/10304312.2025.2518967>.
4. C. Goanta, Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising, <https://verfassungsblog.de/dsa-now-what/>, 2022
5. Cauffman C. New EU Rules on Business-to-Consumer and Platform-to-Business Relationships. *Maastricht J. Eur. Comp. Law* 2019;26:469–88. <https://doi.org/10.1177/1023263X19865835>.
6. Eurostat (2024), IMF World Economic Outlook (2024).
7. F Krause, IOS Privacy: Instagram and Facebook can track anything you do on any website in their in-app browser. <https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser>, 2022 (accessed 4 September 2024).
8. Husovec M. *Principles of the Digital Services Act*. Oxford: Oxford University Press; 2024
9. HUSOVEC, M.: The DSA's Scope Briefly Explained, Husovec, Martin, The DSA's Scope Briefly Explained, 20.02.2023, cit. 04.04.2023 s. 3 , <http://dx.doi.org/10.2139/ssrn.4365029>
10. J. P. Quintais, N. Appelman, R. Fathaigh, Using Terms and Conditions to Apply Fundamental Rights to Content Moderation, *Ger. Law J.* 24(5) (2023) 881-911. <https://doi.org/10.1017/glj.2023.53>; J. van de Kerkhof, Article 22 Digital Services Act: Building Trust with Trusted Flaggers, *Internet Policy Rev.* (2025). <https://doi.org/10.14763/2025.1.1828>.
11. Kim D. Under What Conditions Will Social Commerce Business Models Survive? *Electron. Commer. Res. Appl.* 2013;12(2):69–77. <https://doi.org/10.1016/j.elerap.2012.12.002>.
12. MACKO, L. *Zodpovednosť za využitie digitálneho obsahu na internete*. Praha. C. H. Beck, 2024, 136 s.
13. Martínez-Lopez, F. To Have or Have Not: Buy Buttons on Social Platforms. *J. Bus. Res.* 2019. <https://doi.org/10.1016/j.jbusres.2019.07.029>.

14. Meta, Shopping on Facebook. <https://www.facebook.com/business/news/shopping-on-facebook>, 2015 (accessed 4 September 2024); V Luckerson, 'Here's Why 'Buy Buttons' Are Invading the Internet'. <https://time.com/4075560/buy-button-facebook-youtube-pinterest/>, 2015.
15. MYŠKA, M. Výjimky a omezení autorského práva v prostředí digitálních sítí. Praha: Wolters Kluwer ČR, 2020, s. 26, původný zdroj JIRSA, J. Uživatelská práva v informační společnosti (online) . Praha , 2012, s. 80
16. Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/2394 z 12. decembra 2017 o spolupráci medzi vnútroštátnymi orgánmi zodpovednými za presadzovanie právnych predpisov v oblasti ochrany spotrebiteľa a o zrušení nariadenia (ES) č. 2006/2004 [2017] Ú. v. EÚ L 345 (nariadenie o spolupráci v oblasti ochrany spotrebiteľa).
17. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES
18. Rozsudok SDEÚ vo veci Zalando/Komisia zo dňa 03.09.2025, sp.zn.: T-348/23
19. Smernica Európskeho parlamentu a Rady (EÚ) 2019/790 zo 17.04. 2019 o autorskom práve a právach súvisiacich s autorským právom na digitálnom jednotnom trhu a o zmene smerníc 96/9/ES a 2001/29/ES
20. Smernica Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004
21. Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami
22. Smernica Európskeho parlamentu a Rady č. 2001/29/ES zo dňa 22.05.2001 o zosúladení niektorých o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti

Kontaktné údaje

JUDr. Lukáš Macko, PhD.

lukas.macko@flaw.uniba.sk

Ústav práva informačných technológií a práva duševného vlastníctva

FROM CONTENT MODERATION TO USER RIGHTS: NEW PERSPECTIVES ON DIGITAL REGULATION ¹

Jana Zigo²

Abstract: Digital platforms process millions of interactions every day. From daily communication between users to business activities, political mobilisation, and the formation of public opinion. However, alongside significant benefits, they also bring risks in the form of illegal or harmful content that requires regulation. One of the tools that platforms use to address these undesirable situations is content moderation. Content moderation is primarily based on automated systems. While these have enabled rapid interventions, they have also raised legitimate concerns about disproportionate interference and thus also the intervention on freedom of expression, for example, and the risk of „automated censorship“. The adoption of the Digital Services Act (DSA) marked an important shift from unilateral decisions by platforms towards greater transparency and recognition of users' procedural rights. The paper discusses Articles 17, 20 and 21 of the DSA as the core provisions strengthening users' procedural rights. The aim is to outline how these mechanisms enhance the transparency and accountability of platforms and to what extent they provide effective remedies to users. This paper also highlights the practical challenges and limits of their application.

Key words: Digital Services Act, Content moderation, User rights, Platforms

Introduction

Digital platforms have become central actors in today's digital ecosystem, mediating communication, business interactions, and even shaping political and cultural discourse.³ They wield considerable power, as they resolve what content will be restricted and what will be removed, which in some cases can also significantly

¹ This article was supported by the Recovery Plan K9: Transformational and Innovation Consortia - More Effective Governance and Strengthening of Science, Research and Innovation Funding - Government office of the Slovak Republic.

² Comenius University in Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property.

³ GAWER, Annabelle Gawer. EPRS STUDY. Online platforms: Economic and societal effects [online]. 2021. p. 2 Available from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU\(2021\)656336_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf).

interfere with the right to freedom of expression.⁴ Content moderation has therefore become a key process through which platforms influence not only the availability but also the visibility of individual content.⁵ Additionally, they establish the rules for what is acceptable on their services through their own terms and conditions, and can restrict access to content or user accounts. However, these mechanisms can run counter to the fundamental right to freedom of expression and create an imbalance between platforms and individuals.⁶ This imbalance is further amplified by the extensive use of automated systems in content moderation. According to the DSA Transparency Report, approximately 93% of enforcement actions on Facebook and 98% on Instagram were performed automatically.⁷ While automation enables interventions at scale, it also introduces risks of erroneous or disproportionate measures, raising concerns about “automated censorship” and the lack of adequate user safeguards. The adoption of the Digital Services Act (DSA) directly addresses these challenges. More than twenty years after the E-Commerce Directive, it introduces a comprehensive framework for intermediation services, with special attention to very large online platforms and search engines (VLOPs and VLOSEs).⁸ What makes the DSA distinctive is its focus on users’ procedural rights: Article 17 obliges platforms to provide clear and specific statements of reasons, Article 20 establishes internal complaint-handling mechanisms, and Article 21 creates an option for out-of-court dispute resolution by independent bodies. Together, these provisions represent a significant attempt to rebalance the relationship between

⁴ PEHLIVAN, Ceyhun Necati, and Peter CHURCH. The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability. *Global Privacy Law Review* [online]. 2023, 4(Issue 1), 53–59. p. 57 ISSN 2666-3570. Available from: doi:10.54648/gplr2023005.

⁵ SARTOR, Giovanni, and Andrea LOREGGIA. EP STUDY. The impact of algorithms for online content filtering or moderation "Upload filters" [online]. 2020. p. 17 Available from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU\(2020\)657101_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf).

⁶ LEERSSEN, Paddy. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review* [online]. 2023 . pp. 9-10 Available from: doi:10.1016/j.clsr.2023.105790.

⁷ RYBNÍKÁR, Jakub, and Katarína DREVENÁ. DSA TRANSPARENCY REPORTS BRIEFING. [online]. 2024. p. 7 Available from: https://rpms.sk/sites/default/files/202402/CMS_DSA_TransparencyReports_briefing.pdf.

⁸ BURI, Ilaria, and Joris VAN HOBOKEN. The Digital Services Act (DSA) proposal: a critical overview". Digital Services Act (DSA) Observatory [online]. 2021 p. 4 Available from: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

platforms and users by combining transparency, accountability, and accessible redress mechanisms.⁹

User Rights in the Digital Space: A New Framework of Safeguards and Remedies under the DSA

As mentioned in the introduction to this paper, the DSA represents a fundamental shift in the regulation of the digital space. Its aim is not only to create a safer online environment by combating illegal content, but also to strengthen users' procedural rights and ensure fair redress mechanisms. In other words, the DSA connects two levels, where, on the one hand, it emphasises the protection of society from harmful content and, on the other hand, the protection of the individual from arbitrary interventions by platforms.¹⁰ This approach reflects the principle of *ubi ius, ibi remedium*, which states that where there is a right, there must also be a remedy to protect it.¹¹ A key tool in this regard is the so-called *notice-and-action mechanism*, which introduces a simple reporting of illegal content and the obligation of platforms to respond quickly and effectively.¹² The system also includes the priority handling of reports by so-called *trusted flaggers*, which creates space for the faster removal of content that poses a serious risk. Additionally, the DSA enhances the right to information and transparency. Platforms must provide users with a clear and concrete justification for each intervention through a statement of reasons.¹³ The user thus receives not only information about the reason for the intervention, but also a basis for applying further remedies. In the context of this paper, it is essential to note that the new framework introduces a multi-tiered system of redress, ranging from an internal complaint handling mechanism to the possibility of reaching independent bodies for out-of-court dispute resolution arising from the platform's moderation activities, and ultimately to judicial protection.¹⁴ This system is designed to ensure that the user always has an available and suitable tool with which to defend against the platform's decision. A separate group consists of measures aimed at

⁹ BUSCH, Christoph, and Vanessa MAK. Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation. *SSRN Electronic Journal* [online]. 2021. p. 13 Available from: doi:10.2139/ssrn.3933675.

¹⁰ DAŇKO, Martin, and Petra ŽÁRSKA. Impact Of The Digital Services Act On Intellectual Property. In: Bratislavské právnické fórum 2023 : autonómia subjektov v 21. storočí / Laura Fotopulosová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. p.201.

¹¹ KUCZERAWY, Aleksandra. Remediating Overremoval. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 167-180.

¹² Article 16 of the DSA.

¹³ Article 17 of the DSA.

¹⁴ Article 20 and 21 of the DSA.

increasing the transparency of platforms. Platforms are obliged to regularly publish reports on content moderation or records within the DSA Transparency Database.¹⁵ These measures enable not only users but also regulatory authorities and the academic community to monitor the extent to which platforms fulfil their obligations.

As we mentioned in introduction of this section, one of the key tools for enhancing transparency in the DSA is the obligation for platforms to provide a *statement of reasons* whenever they take a decision restricting content or a user's account.¹⁶ This mechanism is based on the fact that the previous practice of large platforms was often non-transparent because users did not know on what basis specific measures were taken, and in some cases even whether they were applied at all.¹⁷ Article 17 of the DSA, therefore, extends the obligation to inform about any decision related to content moderation.¹⁸ The obligation applies not only to the removal of content, but also to other interventions, such restriction of access to content or reduction of its visibility, suspension or termination of the provision of the service, blocking or termination of the user's account, restriction or termination of the possibility of monetising content.¹⁹ The statement must be specific, clear and understandable. The DSA outlines the minimum requirements that it must meet.²⁰ The statement is provided to all affected recipients of the service, if the provider has their contact details, without delay after the measure is applied. An exception is situations where the platform refuses to act after the user has been notified, in which case the obligation to justify the decision does not arise.²¹ From the point of view of the system of remedies, the obligation to provide statement of reasons is of fundamental importance. The information contained in the statement of reasons is essential for further proceedings, whether when assessing the dispute within the internal

¹⁵ TESSA, Benedetta et al. Improving Regulatory Oversight in Online Content Moderation. arXiv.org [online]. 2025. pp. 1-2 Available from: <https://arxiv.org/abs/2506.04145>.

¹⁶ Article 17 of the DSA.

¹⁷ CLUNE, Conor, and Emma MCDAID. Content moderation on social media: constructing accountability in the digital space. *Accounting, Auditing & Accountability Journal* [online]. 2023 pp. 17-19 Available from: doi:10.1108/aaaj-11-2022-6119.

¹⁸ Supranote 14.

¹⁹ Article 17(1)(a-d) of the DSA.

²⁰ According to Article 17(3) of the DSA, the reasoning for the decision must include, in particular, at least information on the measure taken and its scope and duration, the factual circumstances and reasons for the decision (including whether it was based on a notification under Article 16 or on a voluntary investigation), details of the use of automated means, the legal or contractual basis for the decision and, finally, clear information on the available remedies (internal complaint, ODS, judicial protection).

²¹ ORTOLANI, Pietro. If You Build It, They Will Come. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 157.

mechanisms of the platforms, or when making decisions by ODS under Article 21 of the DSA. As already mentioned, the DSA adheres to the fundamental principle of the right to an effective remedy. Everyone whose rights have been restricted by the platform's intervention must be able to defend themselves, based on precise and comprehensible reasons provided by the platform. Article 17, therefore, plays a central role in ensuring fairness and predictability in the online space, as without a clear justification, any redress mechanism would lose its meaning and effectiveness.²² According to the DSA Transparency Database, more than 11 billion statements of reasons have been published to date by platforms in connection with their decisions under Article 17 DSA. The most frequently reported violations concern other breaches of providers' terms and conditions, followed by illegal or harmful speech and scams or fraud. The most common types of restrictions include disabling access to content, removal of content, and other specific forms of limitation. Currently, around 220 platforms are active in the system, with statistics further showing that approximately 50% of all decisions are made fully automatically.²³ While Article 17 of the DSA focuses on the obligation of platforms to provide users with clear and specific justifications for interventions in content or accounts, Article 20 represents a further step in protecting users' rights. Article 20 of the DSA introduces an obligation for online platform providers to establish an internal complaint-handling system that enables users to challenge content moderation decisions that adversely affect them, free of charge and electronically.²⁴ This mechanism must be accessible for at least six months from the date the platform adopts the measure and is available not only to the users but also to third parties who have reported the content. The subject of a complaint may include various decisions, such as the removal or blocking of content, the reduction of its visibility, the suspension or termination of service provision, the blocking or termination of an account, or the limitation of content monetisation.²⁵ The mechanism applies not only to content that has been deemed illegal, but also to content that has been deemed incompatible with the platform's terms and conditions.²⁶ It can also be used in situations where the platform refuses to act on a notification and leaves the content online. The system must be easily accessible, user-friendly and allow for the submission of sufficiently precise and reasonably substantiated complaints. Platforms are obligated to handle complaints in a timely, non-discriminatory,

²² *Ibid.*

²³ See more: Home - DSA Transparency Database [online]. Available from: <https://transparency.dsa.ec.europa.eu/>.

²⁴ Article 20 of the DSA.

²⁵ Article 20(1) DSA.

²⁶ Supranote 9..

professional, and impartial manner, without arbitrary action.²⁷ If the complaint is sufficiently substantiated, they must immediately reverse their original decision. At the same time, decisions cannot be taken solely based on automated means, but must be under human supervision.²⁸ After handling a complaint, the platform is obliged to inform the user without undue delay of the reasons for its decision and provide them with clear and comprehensible instructions on further redress options. This includes, in particular, a reference to out-of-court dispute resolution under Article 21 of the DSA and to other available means of protection, including judicial protection.²⁹ Article 20 thus provides a counterbalance to the notice and action mechanism included in Article 16. The key benefit is that platforms are obliged to reinstate content that, after review, is found to be legal or compliant with the terms of service. However, it also allows those whose notifications have been rejected to challenge this situation. This means that the mechanism is available to both parties to the dispute.³⁰

The internal complaint handling system, as outlined in Article 20, is supplemented by Article 21 of the DSA, which provides users with an additional level of protection through independent out-of-court dispute resolution. While Article 20 still leaves the decision-making power in the hands of the platform, Article 21 allows disputes to be examined by a certified body, ensuring independence and expertise.³¹ This step represents a fundamental strengthening of users' procedural rights, as it opens up access to adequate and affordable redress outside the platform.

As mentioned in the previous sections of this paper, Article 21 of the DSA introduces a new type of mechanism that can be considered one of the most significant innovations in online regulation. It is an out-of-court dispute resolution (ODS) system designed to provide users with a opportunity to defend against decisions made by platforms regarding content moderation or account management.³² The main aim is to balance the asymmetry between technology giants and individuals, as remedies for users have been limited so far.³³ A user who is not satisfied with a decision made by a platform within its internal system has the opportunity to turn to an independent ODS. These ODS can review a wide range of decisions, which are defined in Article

²⁷ HARRISON, Ruairí, Jonny SHIPP, and Aebha CURTIS. Settling DSA-related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act. *SSRN Electronic Journal* [online]. 2024. p. 9 Available from: doi:10.2139/ssrn.4787648.

²⁸ Article 20(6) of the DSA.

²⁹ Article 20(4) of the DSA.

³⁰ Supranote 24.

³¹ Supranote 9.

³² *Ibid.*

³³ HARRISON, Ruairí, Jonny SHIPP, and Aebha CURTIS. Settling DSA-related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act. *SSRN Electronic Journal* [online]. 2024. p. 24 Available from: doi:10.2139/ssrn.4787648.

20(1) of the DSA.³⁴ These are situations that can directly affect not only the economic interests of users but also their fundamental rights, particularly freedom of expression or the right to access information. The proceedings before the ODS must be accessible, affordable and straightforward for users.³⁵ The platforms typically bear the costs of the proceedings, while users may only be required to pay a minimum fee, which is refunded if the case is successful.³⁶ This model removes barriers to access to justice and can also create pressure on platforms to avoid systematic errors in their decision-making processes. If incorrect interventions were to occur on a larger scale, the platform would have to repeatedly finance processes before independent bodies, which represents both an economic and reputational cost. In this context, however, it can be stated that this fee structure has faced considerable criticism in practice, as it raises concerns about an excessive number of unjustified complaints.³⁷ A fundamental condition for the functioning of the ODS is its independence and professional competence.³⁸ The national coordinator of digital services grants the certification of these bodies for a period of five years. Certified bodies must demonstrate not only organisational and financial independence from platforms, but also expertise in selected areas, such as addressing illegal content or the rules governing the use of individual types of platforms.³⁹ ODS are obliged to conduct electronic procedures and comply with clearly defined procedural deadlines (standard 90 days, with a maximum of 180 days in more complex cases).⁴⁰ However, it should be emphasised that ODS decisions are not legally binding. They are intended to act as a kind of "*second opinion*" and quasi-another instance that follows up on the internal mechanisms of individual platforms, since it can be assumed that the platform cannot be completely independent within these internal procedures.⁴¹ Within this procedure, platforms are obliged to act in good faith, however, due to the non-binding nature of decisions, they may decide not to accept the ODS

³⁴ Article 21(1) of the DSA.

³⁵ Article 21(3)(e) of the DSA.

³⁶ For example, on the fee models of existing ODS centres, *see more*: HOLZNAGEL, Daniel. Art. 21 DSA Has Come to Life. *Verfassungsblog* [online]. 2024 Available from: <https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification>.

³⁷ RUSCHEMEIER, Hannah et al. Brave New World. Out-Of-Court Dispute Settlement Bodies and the Struggle to Adjudicate Platforms in Europe. *Verfassungsblog* [online]. 2024 Available from: <https://verfassungsblog.de/ods-dsa-user-rights-content-moderatin-out-of-court-dispute-settlement/>.

³⁸ Article 21(3)(a) of the DSA.

³⁹ Article 21(3)(b) of the DSA.

⁴⁰ Article 21(1)(d)(e) and Article 21(4) of the DSA.

⁴¹ HUSOVEC, Martin. Certification of Out-of-court Dispute Settlement Bodies under the Digital Services Act. *SSRN Electronic Journal* [online]. 2023. p. 2. Available from: [doi:10.2139/ssrn.4501726](https://doi.org/10.2139/ssrn.4501726).

recommendation in a specific case.⁴² This element raises questions about the credibility of the system and the motivation of users to use it. On the other hand, systematic disregard for decisions could be considered a breach of obligations under the DSA, and especially for very large online platforms, respecting ODS decisions is also important in terms of the obligation to reduce systemic risks.⁴³ Transparency is also an important element. ODS must publish their procedural rules, decision statistics and ensure that their practice is predictable.⁴⁴ Several ODS bodies have already been certified⁴⁵, which are profiled according to various criteria, such as language coverage, types of disputes, or specialisation on specific platforms. However, as this is an entirely new mechanism, decision-making practice is still being formed, and there is not enough data available to assess its real effectiveness.⁴⁶

Implementation Challenges and Limitations

Although the DSA has brought significant reinforcement of users' rights and new protection mechanisms, its practical implementation also raises several question marks. Alongside the undeniable benefits, some potential limits and challenges may affect their effectiveness. Article 17 of the DSA deserves special attention, as it enhances the transparency of platforms' decision-making. However, its practical implementation also reveals several problematic aspects. The platform's obligation to provide statements of reasons, for example, for each partial reduction in content visibility, could lead to an overload of notifications for users. On the other hand, there is a risk that platforms, out of fear of excessive costs or administrative burden, will

⁴² *Ibid.*

⁴³ Article 35 of the DSA.

⁴⁴ Article 21(4) of the DSA. Although the existing ODS have already published all the necessary information and rules of procedure, they have not yet provided access to the decisions or to reports on their activities. This raises questions about the transparency and consistency of their practice. According to the DSA, they are obliged to submit reports to the digital coordinator once a year; however, it is unclear whether these reports will also be made available to users. Making at least some of the decisions available would be crucial for strengthening trust and consistency in decision-making practice.

⁴⁵ List of Out-of-court dispute settlement bodies under the Digital Services Act (DSA). [online]. Available from: <https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement>.

⁴⁶ ODS bodies have already handled thousands of disputes. However, as no decisions or detailed statistics have been published, a comprehensive overview of their practice is missing. Partial data can be inferred from platform reports. According to Meta's Transparency Report (Jan–Jul 2025), ODS issued 491 decisions for Facebook, upholding 196 and overturning 295, with the platform implementing only 32%. For Instagram, 241 decisions were made, of which 46 upheld and 195 overturned the original decision, with an implementation rate of just 23%. Due to the lack of available data, it remains unclear why platforms chose not to follow these decisions. *See more:* (EU) 2022/2065 Digital Services Act Transparency Report for Facebook and Instagram [online]. 2025 Available from: <https://transparency.meta.com/reports/regulatory-transparency-reports/>.

stop using some beneficial measures, such as reducing the reach of problematic but not explicitly illegal content.⁴⁷ Another possible weakness is the unilateral setting of the obligation. The platform is only obliged to justify its actions if it takes action against the content or account. However, if it decides not to take action, for example, by not removing the content after receiving a notification, it is not obliged to provide this justification for the information. This asymmetric approach can create imbalances and appear unfair, as the user whose report has been rejected does not receive any explanation for the rejection.⁴⁸ Despite these limitations, the statement of reason under Article 17 should provide a clearer understanding of the action the platform has taken and the reasons behind it. This information can also serve as a basis for further dispute resolution strategies by the users concerned.⁴⁹

The limits of the obligation to provide reasons under Article 17 are also linked to the challenges associated with the internal complaint-handling mechanism under Article 20. Operating a sophisticated internal mechanism is financially and organizationally demanding, which can be particularly problematic for smaller platforms.⁵⁰ At the same time, there is a risk that platforms may be overwhelmed by a large number of complaints.⁵¹ Another limit is the absence of more detailed procedural standardisation. While the DSA requires the system to be user-friendly and accessible, it leaves platforms with considerable freedom in their specific settings. It is precisely the lack of uniform rules that can lead to the effectiveness and predictability of the mechanism varying significantly between individual platforms.⁵² Despite these limits, Article 20 of the DSA represents a significant step forward in protecting users' rights, as it provides them with a direct and relatively quick remedy

⁴⁷ KELLER, Daphne. The European Union's New DSA and the Rest of the World. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 233.

⁴⁸ Supranote 19.

⁴⁹ *Ibid.*

⁵⁰ Supranote 9.

⁵¹ Data from Meta's reports show that the internal complaint mechanism is being used intensively in practice. In the case of Facebook account termination, more than 3.8 million complaints were recorded in the EU, with approximately 861,000 accounts being reinstated, which is around 22.6% of cases. Similar figures are seen for other types of restrictions, such as service suspensions or monetisation restrictions, where the original decisions were reversed in a smaller but still significant proportion of cases. Another interesting fact is that the median time to resolve a complaint was under one hour, which points to the speed of processing, but also to the enormous strain on the platforms' capacities. See more: (EU) 2022/2065 Digital Services Act Transparency Report for Facebook and Instagram [online]. 2025 Available from: <https://transparency.meta.com/reports/regulatory-transparency-reports/>.

⁵² Supranote 19.

that can contribute to fairer content decision-making and enhance the transparency of the online environment.⁵³

In relation to the out-of-court dispute resolution mechanism under Article 21 of the DSA, it is essential to state that the main advantage is that it provides a faster and more accessible way for users to review platform decisions. So users do not have to engage in lengthy and costly legal proceedings. The very existence of an independent body that an ordinary user can turn to represents a shift in access to justice in the digital environment.⁵⁴ Moreover, since the platforms essentially bear the costs of disputes, indirect pressure is created to improve the quality of their internal decision-making processes. Combined with the relatively short decision-making periods, this mechanism has the potential to become a functional counterweight to the power of large platforms.⁵⁵

Given that the Article 21 DSA mechanism has only been operational in practice for a very short time, the available empirical data is limited. Nevertheless, the first publicly available sources already indicate its real impact. One of the ODS - the Appeals Centre Europe (ACE), published its first transparency report on 1 October 2025, stating that it had received almost 10,000 complaints between November 2024 and August 2025, of which more than 3,300 fell within its competence. The platforms most frequently subject to dispute included Facebook, Instagram, TikTok and YouTube. By the end of August, ACE had decided more than 1,500 cases, overturning the platform's original decision in more than three-quarters of them, mainly in cases of unjustified removal of content, misclassification of sensitive content or unjustified account suspension. These data suggest that platforms often make mistakes in automated moderation and that independent review can effectively correct these failures. The report also highlights uneven cooperation between platforms and ODSs, including cases where platforms have refused to provide the contested content, leading ACE to issue so-called "default decisions" in favour of the user.⁵⁶ On the other hand, the non-binding nature of the decisions may be a significant weakness of the entire system. Although platforms are expected to act in good faith, there is nothing to prevent them from rejecting a specific decision. If this were to happen more widely, the mechanism could lose credibility and discourage users. There are also other risks in the background, in the form of pressure on platforms to

⁵³ HUSOVEC Martin. Will the DSA Work?. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 233.

⁵⁴ Supranote 19.

⁵⁵ *Ibid.*

⁵⁶ See more: Appeals Centre Europe Transparency Report. [online]. 2025 Available from: <https://www.appealscentre.eu/wp-content/uploads/2025/09/Appeals-Centre-Europe-Transparency-Report.pdf>

minimise the number of disputes, which can lead not only to more responsible moderation, but also to insufficient intervention against content that should be removed, or to too immediate restoration of content without in-depth analysis, just to avoid reputational or financial loss.⁵⁷ The independence and expertise of ODS also remain an open question. Formal independence does not yet guarantee actual impartiality, as practice can introduce conflicts of interest, ties to former platform employees, or other forms of pressure.⁵⁸ There is also a sufficient volume of decisions that would allow the creation of predictable standards and strengthen legal certainty for users. Ultimately, the key will be to what extent the transparency of decision-making practice and the professional competence of ODS bodies can be ensured. Article 21 is a significant step in making justice accessible within the digital environment. However, its success relies on strict oversight by regulators and the trust of users and platforms alike.⁵⁹

Conclusion

The DSA undoubtedly represents a significant step forward in strengthening users' procedural rights. The mechanisms enshrined in Articles 17, 20 and 21 create a framework that aims to bring greater transparency, fairness and accountability to platforms. However, in practice, it remains questionable to what extent these rules will actually be effective, as early experience has already shown not only their benefits but also the limits and risks of formal compliance. Early practice suggests that procedural safeguards alone may not be sufficient to address deeper structural asymmetries between users and large platforms. In conclusion, the key challenge lies not in the legal framework, but in consistent enforcement and in the willingness of platforms to respect not only the significance of the law but also its purpose. From this perspective, the DSA can be seen as a positive and necessary step, which, however, still needs to be tested in practice. If the redress mechanisms are to be genuinely effective, they must operate not merely as formal processes, but as functional tools capable of correcting erroneous or disproportionate platform decisions. In that case, the DSA can fulfil its ambition of establishing a balance between the power of large platforms and the rights of individuals.

⁵⁷ GRADONI, Lorenzo, and Pietro ORTOLANI. Vying for the Scales. Content Moderation Made in Europe after One Year of DSA. *Verfassungsblog* [online]. 2025 Available from: <https://verfassungsblog.de/vying-for-the-scales-dsa-ace/>.

⁵⁸ *Ibid.*

⁵⁹ Supranote 33.

Bibliography

1. BURI, Ilaria, and Joris VAN HOBOKEN. The Digital Services Act (DSA) proposal: a critical overview". Digital Services Act (DSA) Observatory [online]. 2021 [viewed 21 September 2025]. Available from: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.
2. BUSCH, Christoph, and Vanessa MAK. Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation. SSRN Electronic Journal [online]. 2021 [viewed 16 September 2025]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.3933675.
3. CLUNE, Conor, and Emma MCDAID. Content moderation on social media: constructing accountability in the digital space. Accounting, Auditing & Accountability Journal [online]. 2023 pp. 17-19 [viewed 10 September 2025]. ISSN 0951-3574. Available from: doi:10.1108/aaaj-11-2022-6119.
4. DAŇKO, Martin, and Petra ŽÁRSKA,. Impact Of The Digital Services Act On Intellectual Property. Bratislavské právnické fórum 2023 : autonómia subjektov v 21. storočí / Laura Fotopulosová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 209 s. ISBN 98-80-7160-705-2.
5. GAWER, Annabelle Gawer. EPRS STUDY. Online platforms: Economic and societal effects [online]. 2021. [viewed 30 August 2025]. Available from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU\(2021\)656336_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf).
6. GRADONI, Lorenzo, and Pietro ORTOLANI. Vying for the Scales. Content Moderation Made in Europe after One Year of DSA. Verfassungsblog [online]. 2025 [viewed 10 September 2025]. Available from: <https://verfassungsblog.de/vying-for-the-scales-dsa-ace/>.
7. HARRISON, Ruairí, Jonny SHIPP, and Aebha CURTIS. Settling DSA-related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act. SSRN Electronic Journal [online]. 2024. [viewed 11 September 2025]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4787648.
8. HUSOVEC, Martin. Certification of Out-of-court Dispute Settlement Bodies under the Digital Services Act. SSRN Electronic Journal [online]. 2023 [viewed 22 September 2025]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4501726.
9. HUSOVEC Martin. Will the DSA Work?. In: VAN HOBOKEN, Joris et al. Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications. Berlin: Verfassungsbooks, 2023. ISBN 978-3-757517-96-0. pp. 19-35.

10. HOLZNAGEL, Daniel. Art. 21 DSA Has Come to Life. *Verfassungsblog* [online]. 2024 [accessed 11 September 2025]. Available from: <https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification>.
11. KELLER, Daphne. The European Union's New DSA and the Rest of the World. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 233. ISBN 978-3-757517-96-0.
12. KUCZERAWY, Aleksandra. Remedying Overremoval. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. p. 167-180. ISBN 978-3-757517-96-0.
13. LEERSEN, Paddy. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review* [online]. 2023, 48, 105790 [viewed 10 September 2025]. ISSN 0267-3649. Available from: doi:10.1016/j.clsr.2023.105790.
14. ORTOLANI, Pietro. If You Build It, They Will Come. In: VAN HOBOKEN, Joris et al. *Putting the Digital Services Act into Practice Enforcement, Access to Justice, and Global Implications*. Berlin: Verfassungsbooks, 2023. ISBN 978-3-757517-96-0.
15. PEHLIVAN, Ceyhun Necati, and Peter CHURCH. The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability. *Global Privacy Law Review* [online]. 2023, 4(Issue 1), 53–59 [viewed 12 September 2025]. ISSN 2666-3570. Available from: doi:10.54648/gplr2023005.
16. RYBNÍKÁR, Jakub, and Katarína DREVENÁ. DSA TRANSPARENCY REPORTS BRIEFING [online]. 2024 [viewed 20 September 2025]. Available from: https://rpms.sk/sites/default/files/2024-02/CMS_DSA_TransparencyReports_briefing.pdf.
17. RUSCHEMEIER, Hannah et al. Brave New World. Out-Of-Court Dispute Settlement Bodies and the Struggle to Adjudicate Platforms in Europe. *Verfassungsblog* [online]. 2024 [viewed 15 September 2025]. Available from: <https://verfassungsblog.de/ods-dsa-user-rights-content-moderatin-out-of-court-dispute-settlement/>.
18. SARTOR, Giovanni, and Andrea LOREGGIA. EP STUDY. The impact of algorithms for online content filtering or moderation "Upload filters" [online]. 2020. p. 17 [viewed 1 September 2025]. Available from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU\(2020\)657101_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf).
19. TESSA, Benedetta et al. Improving Regulatory Oversight in Online Content Moderation. *arXiv.org* [online]. 2025 [viewed 18 September 2025]. Available from: <https://arxiv.org/abs/2506.04145>.

20. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) In EUR-Lex. Available from: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.
21. List of Out-of-court dispute settlement bodies under the Digital Services Act (DSA). [online]. Available from: <https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement>.
22. (EU) 2022/2065 Digital Services Act Transparency Report for Facebook and Instagram [online]. 2025 Available from: <https://transparency.meta.com/reports/regulatory-transparency-reports/>.
23. Home - DSA Transparency Database [online]. [viewed 28 September 2025]. Available from: <https://transparency.dsa.ec.europa.eu/>.

Contact details

Mgr. Jana Zigo, PhD., LL.M.

cihanovaz@uniba.sk

Comenius University in Bratislava, Faculty of Law

Institute of Information Technology Law and Intellectual Property

PREDMETY DUŠEVNÉHO VLASTNÍCTVA AKO PREDMET ZÁLOŽNÉHO PRÁVA - FINANCOVANIE ZABEZPEČENÉ DUŠEVNÝM VLASTNÍCTVOM¹

INTELLECTUAL PROPERTY AS A COLLATERAL – IP BACKED FINANCING

Albert Priehoda²

Abstrakt: Článok analyzuje duševné vlastníctvo ako súčasť nehmotného majetku podnikov, jeho využitie pri financovaní podniku formou záložného práva a prepojenie s kybernetickou bezpečnosťou. Metodicky vychádza z analýzy právneho rámca, sekundárnych dát Úradu priemyselného vlastníctva SR a pološtruktúrovaných rozhovorov so zástupcami slovenských bánk. Empirické zistenia potvrdzujú konzervatívny prístup slovenského bankového sektora. Duševné vlastníctvo je akceptované iba ako doplnkový kolaterál, spravidla bez vplyvu na výšku úveru, cenotvorbu a posúdenie rizika. Bariérami sú najmä neistota ocenenia a volatilita hodnoty, vymožitelnosť a speňažiteľnosť, nízka likvidita, chýbajúce poistné produkty, medzery v evidencii nehmotných aktív a absencia relevantného trhu. Článok zároveň poukazuje na jednotlivé kategórie ochrany duševného vlastníctva a ich špecifické limity z pohľadu použiteľnosti duševného vlastníctva ako zálohu. Zároveň ukazuje, že úroveň kybernetickej bezpečnosti (vrátane požiadaviek NIS2) je významným faktorom due diligence, ktorá ovplyvňuje udržanie hodnoty duševného vlastníctva a jeho akceptáciu ako zálohu. Príspevok odporúča podporiť štandardy oceňovania, rozvoj sekundárnych trhov s právami duševného vlastníctva, zlepšiť evidenciu a integrovať hodnotenie kybernetickej bezpečnosti do úverových procesov.

Kľúčové slová: duševné vlastníctvo, nehmotný majetok, financovanie kryté právami duševného vlastníctva, ochrana duševného vlastníctva, kybernetická bezpečnosť, NIS2.

Abstract: The article analyses intellectual property as part of a company's intangible assets, its use in corporate financing as collateral, and its connection

¹ Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17Ro5-04-Vo1-00002 (Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality).

² Univerzita Komenského v Bratislave, Právnická fakulta, Ústav ekonomických vied.

with cybersecurity. Methodologically, it draws on an analysis of the legal framework, secondary data from the Industrial Property Office of the Slovak Republic, and semi-structured interviews with representatives of Slovak banks. Empirical findings confirm the conservative approach of the Slovak banking sector. Intellectual property is accepted only as supplementary collateral, usually without any effect on loan amount, pricing, or risk assessment. The main barriers include valuation uncertainty and volatility, issues related to enforceability and monetization, low liquidity, the absence of insurance products, gaps in intangible asset records, and the lack of a relevant market. The study also points to the individual categories of intellectual property protection and their specific limitations in terms of the usability of intellectual property as collateral. It further shows that the level of cybersecurity (including NIS2 requirements) is a significant due diligence factor influencing both the preservation of intellectual property value and its acceptance as collateral. The paper recommends supporting valuation standards, developing secondary markets for intellectual property rights, improving record-keeping, and integrating cybersecurity assessments into lending processes.

Key words: intellectual property, intangible assets, IP backed financing, intellectual property protection, cybersecurity, NIS2

Úvod

V súčasnej znalostne orientovanej ekonomike sa význam duševného vlastníctva a nehmotného majetku neustále zvyšuje. Zatiaľ čo kedysi tvorili základ hodnoty podnikov najmä hmotné aktíva, dnes sa čoraz viac ukazuje, že rozhodujúcu úlohu majú inovácie, know-how, ochranné známky či softvérové riešenia. Tieto formy nehmotného majetku prinášajú podnikom konkurenčnú výhodu, no zároveň otvárajú množstvo právnych, ekonomických a bezpečnostných otázok. Osobitne dôležitým sa stáva ich právne postavenie, spôsob ocenenia a možnosti využitia v podnikovej praxi, napríklad aj ako predmetu záložného práva pri získavaní kapitálu. Rovnako významná je aj ochrana týchto aktív pred neoprávneným zásahom, či už v podobe porušovania práv alebo kybernetických hrozieb. Text sa preto zameriava na tri kľúčové oblasti, ktorými sú duševné vlastníctvo ako súčasť nehmotného majetku, financovanie činnosti podniku kryté nehmotným majetkom podniku a akceptáciou nehmotného majetku bankami ako predmetu záložného práva, a napokon na otázku ochrany nehmotného majetku a duševného vlastníctva, vrátane úzkeho prepojenia s kybernetickou bezpečnosťou.

Duševné vlastníctvo ako súčasť nehmotného majetku

Nehmotný majetok predstavuje kategóriu aktív, ktoré nemajú fyzickú podstatu, no prinášajú podnikom významné ekonomické úžitky. Zahŕňa rôzne formy práv, nákladov či hodnotových položiek, ako sú softvér, goodwill, licencie, povolenia, franšízy a aktivované náklady na vývoj. V modernej ekonomike má nehmotný majetok čoraz väčší význam, keďže rastie podiel znalostne orientovaných odvetví, kde rozhodujúcu úlohu zohrávajú práve nehmotné zdroje podniku. Ide najmä o práva a iné majetkové hodnoty nadobudnuté za odplatu alebo vytvorené vlastnou činnosťou podniku, ktoré sú spôsobilé byť predmetom právneho vzťahu. Typickými príkladmi sú patenty, licencie, ochranné známky, softvérové produkty, know-how, výsledky výskumu a vývoja. V účtovníctve sa vyказuje v súlade s platnou právnou úpravou ako dlhodobý nehmotný majetok a podlieha systematickému odpisovaniu počas doby svojej použiteľnosti. V zmysle právneho poriadku Slovenskej republiky sa práva duševného vlastníctva dajú členiť na tri hlavné oblasti:

- autorské právo a práva s ním súvisiace,
- priemyselné vlastníctvo,
- práva príbuzné právam duševného vlastníctva.

Legislatíva definuje jednotlivé druhy predmetov duševného vlastníctva a umožňuje ich právnu ochranu. Umožňuje identifikáciu legálneho vlastníka predmetov duševného vlastníctva, definuje spôsob a podmienky za ktorých vzniká právna ochrana (registráciou alebo automaticky), definuje aký je jej rozsah a dĺžka trvania právnej ochrany, aké práva majú vlastníci a aké majú prostriedky na domáhanie sa svojich práv. Právna ochrana umožňuje uplatnenie si nárokov majiteľov práv k predmetom duševného vlastníctva vyplývajúcich z ich držby súdnou cestou, vrátane náhrady vzniknutej škody alebo trestnoprávneho postihu narušiteľa práv.

Akceptácia predmetov duševného vlastníctva ako predmetu záložného práva bankami na Slovensku

Záložné právo je jedným zo základných zabezpečovacích inštitútov, ktorý slúži na ochranu veriteľa v prípade, že dlžník nesplní svoj záväzok. Jeho podstata spočíva v tom, že veriteľ má právo uspokojiť svoju pohľadávku z hodnoty zálohu. Tradične sa záložné právo viaže na hmotný majetok, najmä na nehnuteľnosti, stroje, vozidlá alebo zásoby. Vývoj ekonomického prostredia však prináša potrebu uplatňovať ho aj na nehmotný majetok podniku, vrátane práv duševného vlastníctva. V praxi sa preto začínajú využívať modely, ktoré umožňujú založenie softvéru, patentov alebo ochranných známok.

Podľa údajov Úradu priemyselného vlastníctva SR bolo k marcu 2023 registroch a evidovaných 746 záložných práv na predmety duševného vlastníctva. V 724 prípadoch išlo o ochrannú známku. Vlastníci založených predmetov duševného

vlastníctva boli najmä zo Slovenskej republiky, potom z Českej republiky a Cypru. Dominovali odvetvia ako spravodajský a mediálny priemysel, potravinársky priemysel a obranný priemysel.³

Individuálne rozhovory, ktoré sme realizovali so zamestnancami jednotlivých bankových inštitúcií, nám poskytli pohľad na postoj slovenských bánk k použitiu nehmotného majetku a duševného vlastníctva ako predmetu záložného práva pri financovaní podnikov (IP backed financing). Identifikovali sme hlavné bariéry pre kolateralizáciu práv duševného vlastníctva z pohľadu bánk, ktorými sú vysoké riziko vyplývajúce najmä z problémov so stanovením hodnoty predmetov duševného vlastníctva, zmena hodnoty predmetu záložného práva a možnosť jej poklesu v čase, vymožitelnosť záložného práva k právam duševného vlastníctva, časové obmedzenie registrácie práv duševného vlastníctva (zánik predmetu práva automaticky vedie k zániku záložného práva), nízka schopnosť a malé skúsenosti veriteľa so speňažením zálohu na uspokojenie pohľadávky banky, nízka likvidita nehmotného majetku v podobe duševného vlastníctva, absencia poistných produktov zameraných na duševné vlastníctvo, nemožnosť prevzatia zálohu bankou v prípade úpadku podniku, prednosť daňových a mzdových povinností pred právami záložného veriteľa, existujúce regulačné obmedzenia a neexistencia relevantného trhu s predmetmi duševného vlastníctva. Všeobecne je možné povedať, že z pohľadu financujúcich bánk je s duševným vlastníctvom ako s predmetom záložného práva spojené vyššie riziko.

Medzi obmedzenia použitia nehmotného majetku ako predmetu záložného práva sa v určitých prípadoch zaraďuje aj nejasné legislatívne vymedzenie nehmotného majetku v Obchodnom zákonníku a ďalších právnych predpisoch. Ďalším limitom je aj skutočnosť, že sa vedie evidencia iba niektorých predmetov duševného vlastníctva, pričom napríklad softvér, vývojové náklady, ocenené práva, goodwill, know-how, alebo receptúry v žiadnych registroch evidované nie sú. Daňové predpisy uznávajú za nehmotný majetok iba majetok s obstarávacou cenou nad 2 400 eur a s dobou použiteľnosti presahujúcou jeden rok, pričom musí ísť o majetok nadobudnutý. To zároveň obmedzuje možnosť zaradiť do majetku podniku hodnotu vlastných vytvorených nehmotných statkov.

Podľa nášho výskumu jedna z najväčších bánk na Slovensku akceptuje vybrané práva duševného vlastníctva ako záloh pri získavaní kapitálu a financovaní podnikateľských aktivít podnikov, vždy však len ako doplnkový, nikdy nie ako jediný kolaterál. Dôležitou podmienkou je samotná možnosť zriadenia záložného práva. Táto banka evidovala v čase zberu dát minimálne 18 prípadov financovania, v ktorých bolo

³ HAVIER, Ján - PRIEHODA, Albert: Slovakia's journey. In: Unlocking IP-backed financing series: Country perspectives / The journey of the Visegrad Group. Ženeva: World Intellectual Property Organization, 2025. ISSN: 3005-9747. s. 52 - 53.

zriadené záložné právo k viacerým právam duševného vlastníctva v jej prospech. Z nich bolo aktívnych päť, pričom nesplatená istina predstavovala 16,8 milióna EUR. V týchto prípadoch však práva duševného vlastníctva nemali vplyv na konečnú výšku financovania, úrokovú sadzbu, riziko ani iné parametre financovania.

Výnimočne a z veľmi špecifických dôvodov bolo v prospech banky zriadené záložné právo k podniku dlžníka, ktoré zahŕňalo aj ochranné známky. V súlade s § 151f ods. 1 druhou vetou Občianskeho zákonníka bolo teda záložné právo zriadené aj na ochranné známky. V tomto prípade financovanie presiahlo 90 miliónov EUR.

V súlade s vnútornými pravidlami oceňovania banky a externými predpismi možno nominálnu hodnotu takéhoto zálohu určiť iba na základe znaleckého posudku. Pre vnútorné účely banky sa však takzvaná vážená hodnota takéhoto kolaterálu vždy rovná o %, bez ohľadu na výsledok znaleckého posudku. Banka používa tento typ zabezpečenia iba ako doplnkový. Hlavným dôvodom je potreba vedieť speňažiť všetok majetok dlžníka pri výkone iného zabezpečenia tak, aby nadobúdateľ mohol čo najplynulejšie pokračovať v podnikaní dlžníka, respektíve aby sa vytvorila čo najlepšia východisková pozícia na vymáhanie nesplatenej pôžičky. Tento prístup by sa mohol zmeniť, ak by existoval relevantný trh, na ktorom by sa takéto záložné práva mohli obchodovať. Vtedy by bolo možné spoliehať sa na predpoklad, že kolaterál možno v prípade potreby speňažiť za vopred odhadnutelnú cenu.

Ďalšia banka uvedená v Tabuľke č. 1, ktorá sa zapojila do prieskumu a poskytla informácie anonymne, využíva práva duševného vlastníctva ako záloh len veľmi sporadicky a výhradne pri korporátnom (nie retailovom) financovaní. Počet takýchto záloh je veľmi nízky, v jednotkách ročne, v niektorých rokoch vôbec žiadny. Nikdy však nejde o samostatné záložné právo, vždy iba v kombinácii s iným hmotným kolaterálom. Kolaterál v podobe práv duševného vlastníctva nemá žiadny významný vplyv na výšku ani podmienky financovania. Doterajšia skúsenosť je iba so záložnými právami k ochranným známkam. V prípade, že práva duševného vlastníctva patria obchodnej spoločnosti, banka uprednostňuje záložné právo k podielom (spoločnosť s celým majetkom vrátane práv duševného vlastníctva ako celok). Banka však nemá interné procesy na speňaženie tohto typu zabezpečenia. Hodnota takéhoto kolaterálu je preto automaticky stanovená na nulu. Likvidita takéhoto zálohu je z pohľadu banky taktiež sporná, keďže banka nemá skúsenosti s jeho vymáhaním a speňažením.

Záložný veriteľ	Počet záložných práv	%
Všeobecná úverová banka	24	4%
Tatra banka	29	5%
Poštová banka	74	12%
Iné banky	79	13%
Slovenská sporiteľňa	105	17%

ČSOB	300	49%
Celkom	611	100%

Tabuľka 1.

Zabezpečovacie práva podľa záložného veriteľa. Zdroj: Úrad priemyselného vlastníctva Slovenskej republiky, marec 2023. Vlastná prezentácia.

Ďalšia z bánk uvedených v Tabuľke č. 1. vyjadrila podobné stanovisko ako predchádzajúce banky, čím potvrdzuje existujúci systém akceptovania financovania krytého právami duševného vlastníctva. Duševné vlastníctvo je touto bankou akceptované len ako záloh popri iných aktívach, pričom môže pomôcť napríklad navýšiť objem financovania, zlepšiť jeho podmienky alebo ovplyvniť celkovú štruktúru financovania. Samostatne bez doplnkových hmotných aktív však banka duševné vlastníctvo neprijíma.

Je zrejmé, že banky pôsobiace v Slovenskej republike zaujímajú konzervatívny prístup k financovaniu krytému právami duševného vlastníctva, čo potvrdili výsledky prieskumu aj individuálne odpovede najväčších bánk na slovenskom trhu. Treba zdôrazniť, že banky pôsobiace na Slovensku majú silne konzervatívnu orientáciu v oblasti rizík, čo vo veľkej miere ovplyvňuje aj ich ochotu akceptovať záložné práva na nehmotný majetok v podobe duševného vlastníctva.

Ochrana predmetov duševného vlastníctva

Ochrana predmetov duševného vlastníctva môže byť realizovaná prostredníctvom viacerých metód a nástrojov. Právne metódy zahŕňajú registráciu práv podaním prihlášok na Úrad priemyselného vlastníctva SR alebo na medzinárodné úrady (napr. patent, úžitkový vzor, dizajn či ochranná známka), využívanie licenčných zmlúv, ktoré umožňujú kontrolované používanie práv inými subjektmi, utajovanie, uzatváranie zmlúv o mlčanlivosti (NDA - non-disclosure agreement) na ochranu know-how a obchodného tajomstva pri spolupráci viacerých subjektov, ako aj právne kroky proti porušeniu vo forme súdnych žalôb, predbežných opatrení alebo arbitráže. Medzi právne metódy môžeme zaradiť aj vyžadovanie dodržiavania legislatívny v oblasti kybernetickej bezpečnosti, ktoré však vyúsťuje do technických a organizačných metód ochrany.

Európska smernica NIS2 (2022/2555) zavádza pre podniky povinnosti v oblasti kybernetickej bezpečnosti, ktoré zahŕňajú zavedenie interných politík, technických opatrení a povinnosť hlásiť incidenty.⁴

⁴ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie

Pre podniky, ktoré využívajú duševné vlastníctvo ako záloh, je kľúčové, aby boli tieto povinnosti dodržiavané. Je to najmä z dôvodu samotnej ochrany predmetov duševného vlastníctva pred kyberútokmi.

Podľa Andraška, jedným z dôvodov prijatia právnej úpravy kybernetickej bezpečnosti je snaha zabrániť ekonomickým škodám, ktoré môžu byť následkom kybernetického bezpečnostného incidentu.⁵

Ale aj ak by doposiaľ v podniku k takejto situácii nedošlo, implementácia a dodržiavanie politik kybernetickej bezpečnosti môže byť predmetom due diligence podniku pri posudzovaní a stanovovaní hodnoty predmetov duševného vlastníctva, a ich akceptovania zo strany záložného veriteľa ako predmetu záložného práva.

Technické a organizačné metódy ochrany sa zameriavajú na digitálne zabezpečenie, ako je šifrovanie, ochrana softvéru proti kopírovaniu a digitálne práva (DRM – Digital Rights Management, technológie a mechanizmy, ktoré majú kontrolovať, ako sa digitálny obsah používa, kopíruje a distribuuje), ďalej na označovanie výrobkov a log pomocou označenia ® alebo ™ pri ochrannej známke, vodotlačí či hologramov. Významné je aj utajovanie receptúr, algoritmov a výrobných postupov ako obchodného tajomstva a zavedenie interných politik, ktoré obmedzujú prístup k citlivým informáciám len pre oprávnené osoby.

Každý technologický prístup k ochrane duševného vlastníctva vyžaduje kompromis medzi bezpečnosťou nehmotného majetku a jeho dostupnosťou, nákladmi a rovnosťou. Technologické bariéry môžu v niektorých prípadoch fungovať ako varovný signál pred neoprávneným použitím, žiadna forma technologickej ochrany však nie je 100-percentná.⁶

Ekonomické nástroje predstavujú napríklad poistenie práv duševného vlastníctva, ktoré kryje škody pri sporoch alebo porušení práv, finančné oceňovanie duševného vlastníctva prostredníctvom znaleckých posudkov na preukázanie hodnoty pri rokovaní alebo sporoch, a napokon aj licencovanie a franchising ako aktívne využívanie duševného vlastníctva ako zdroja príjmu, čo zároveň umožňuje kontrolovať jeho použitie. Významné sú aj inovácie, ktoré umožňujú podnikom stále udržiavať náskok od konkurencie.

Due diligence v rámci ekonomických nástrojov je proces, počas ktorého si investor alebo financujúci subjekt overuje tvrdenia, ktoré vlastníak predmetov duševného

(EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2). s. 101-132.

⁵ ANDRAŠKO, Jozef - MESARČÍK, Matúš - SOKOL, Pavol: Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. ISBN: 978-80-7160-632-1. s. 59.

⁶ Intellectual property rights in an age of electronics and information [online]. Washington DC: Congress, Office of Technology Assessment, U.S. Government printing office, 1986. [cit.2025-08-25]. s. 116-126. Dostupné na:

<https://repository.digital.georgetown.edu/handle/10822/708334>.

vlastníctva uviedol počas kvalifikačnej etapy získavania financovania, pretože tieto tvrdenia sú základom toho, čo financujúci subjekt v prvom rade prijalo k financovaniu.⁷

Pri posudzovaní hodnoty nehmotného majetku ako predmetu záložného práva prostredníctvom due diligence sa môže preverovať aj úroveň jeho kybernetickej ochrany. Kybernetická bezpečnosť je priamo naviazaná na uchovanie hodnoty nehmotného majetku (napr. ochrana databázy zákazníkov pred jej zverejnením).

V niektorých podnikoch majú manažéri pocit, že ochrana predmetov duševného vlastníctva prostredníctvom patentovej právnej ochrany nie je dostatočná a v prípade malých podnikov by nebola vnímaná ako racionálna. S podaním patentovej prihlášky je taktiež spojené odhalenie vynálezu. Manažéri nadobúdali pocit, že komplexnosť v kombinácii s rýchlym inovačným cyklom, utajením a efektívnym zdieľaním znalostí im ponúkala oveľa lepšiu úroveň ochrany ako patenty.⁸

Reputačné a trhové metódy ochrany súvisia najmä s budovaním značky, keďže čím je značka silnejšia, tým je pre konkurenciu ťažšie neoprávnene ju využívať. Patrí sem tiež monitoring trhu a internetu so zameraním sa na odhaľovanie falzifikátov, pirátskych kópií či zneužívania značky na sociálnych sieťach, a spolupráca s colnými a kontrolnými orgánmi prostredníctvom registrácie ochrannej známky v colnom registri na boj proti falšovanému tovaru.

Medzi preventívne metódy patrí vzdelávanie zamestnancov o dôležitosti ochrany duševného vlastníctva, včasná registrácia práv pred zverejnením nápadu alebo výrobku a vypracovanie stratégie, ktorá zabezpečí ochranu na hlavných trhoch, kde podnikateľ už pôsobí, alebo plánuje pôsobiť.

Kategória ochrany	Konkrétne nástroje
Právne metódy	Registrácia (patent, dizajn, známka), licenčné zmluvy, NDA, legislatíva v oblasti kybernetickej bezpečnosti (napr. NIS2), uplatnenie si práv na súde
Technické a organizačné metódy	Šifrovanie, DRM, označovanie ®/™, vodotlače, interné politiky, blockchain technológie ochrany
Ekonomické nástroje	Poistenie IP, due diligence (posudzovanie vrátane úrovne kybernetickej ochrany),

⁷ REMENTILLA, Lilla: Intellectual property-backed financing. In: Intellectual property management for start-ups. Management for professionals. Cham: Springer, 2023. ISBN: 978-3-031-16992-2. s. 181.

⁸ KULMALA, Riikka - KETTUNEN, Juha: Intellectual property protection and process modeling in small knowledge intensive enterprises. In: Information communication technology law, protection and access rights: global approaches and issues. Hershey: Information Science Reference, 2010. 560 s. ISBN: 9781615209767. s. 151-168.

	oceňovanie znalcom, licencovanie, franchising, predajné modely, náskok pred konkurenciou, inovácie
Reputačné a trhové metódy	Budovanie značky, monitoring trhu, spolupráca s colnými orgánmi
Preventívne metódy	Vzdelávanie zamestnancov, stratégie informovania verejnosti, včasná registrácia, medzinárodná stratégia ochrany

Tabuľka 2.

Nástroje ochrany duševného vlastníctva. Vlastné spracovanie.

Kulmala a Kettunen poukazujú na ďalšie nástroje ochrany, využívané mnohými vlastníckmi práv, a to informovanie o právach spojených s duševnom vlastníctvom a presviedčanie o dodržiavaní týchto práv. Takéto budovanie vzťahov s verejnosťou, so snahou ovplyvniť ju, sa môže realizovať prostredníctvom troch základných stratégií. Prvou môže byť informovanie verejnosti o tom, že kopírovanie je nelegálne a bude potrestané. Druhou je snaha presvedčiť verejnosť, že ma podiel na zabezpečení spravodlivého odmeňovania umelcov a vlastníkov ostatných práv duševného vlastníctva. Treťou stratégiou je vzdelávanie verejnosti a apelovanie na dodržiavanie zákona.⁹

Duševné vlastníctvo a kybernetická bezpečnosť

Duševné vlastníctvo predstavuje kľúčový prvok znalostnej ekonomiky a je často najcennejším aktívom moderných podnikov. Z tohto dôvodu sa ochrana duševného vlastníctva stáva prioritou nielen v právnej, ale aj v technickej a organizačnej rovine. V súčasnosti, keď väčšina tvorivých diel, inovatívnych riešení a obchodného know-how existuje v digitálnej podobe, sa kybernetická bezpečnosť javí ako nevyhnutná podmienka efektívnej ochrany týchto aktív podniku.

Kybernetická bezpečnosť predstavuje multidisciplinárnu oblasť, ktorá sa zameriava na ochranu počítačov, komunikačných sietí, informačných systémov, dát a digitálnych služieb pred neoprávneným prístupom, zneužitím alebo poškodením. Jej cieľom je vytvoriť bezpečné prostredie pre fungovanie moderných informačných a

⁹ KULMALA, Riikka - KETTUNEN, Juha: Intellectual property protection and process modeling in small knowledge intensive enterprises. In: Information communication technology law, protection and access rights: global approaches and issues. Hershey: Information Science Reference, 2010. ISBN: 9781615209767. s. 151-168.

komunikačných technológií, ktoré sú základom fungovania verejnej správy, podnikateľských subjektov aj jednotlivcov.

Z hľadiska obsahu charakterizuje Sokol¹⁰ kybernetickú bezpečnosť ako súbor opatrení, technológií a organizačných postupov, ktorých úlohou je zabezpečiť tri základné princípy používané zo strany:

- **dôvernosť dát** – zabezpečenie, aby k informáciám mali prístup iba oprávnené osoby,
- **integritu informácií** – záruku, že dáta neboli neoprávnene pozmenené,
- **dostupnosť systémov** – garanciu, že služby a systémy budú funkčné v čase, keď sú potrebné.

Vzhľadom na ich pôvodné definovanie v anglickom jazyku ako princíp dôvernosti (confidentiality), celistvosti (integrity) a dostupnosti (availability), označujú sa aj ako „triáda CIA“.¹¹

Kybernetická bezpečnosť je v tejto súvislosti kľúčová najmä z dôvodu prevencie krádeže inovácií a know-how. Útoky zamerané na získanie zdrojových kódov, výskumných dát alebo technickej dokumentácie môžu viesť k strate konkurenčnej výhody, pričom škody spôsobené únikom informácií často presahujú rámec jednej organizácie a negatívne ovplyvňujú aj celé odvetvia. Ďalším významným aspektom je prevencia hospodárskej špionáže, ktorá sa čoraz častejšie realizuje prostredníctvom sofistikovaných kybernetických útokov. Nelegitímne získanie obchodných tajomstiev alebo patentovo chránených technológií môže mať za následok nielen priame finančné straty, ale aj dlhodobé poškodenie reputácie a dôveryhodnosti podniku. Kybernetická bezpečnosť je zároveň úzko spätá s dodržiavaním legislatívnych rámcov a medzinárodných dohovorov v oblasti ochrany duševného vlastníctva. K účinným bezpečnostným opatreniam patria najmä šifrovanie dát, riadenie prístupových práv a monitorovanie sieťovej prevádzky, ktoré organizáciám umožňujú včas identifikovať hrozby a zabrániť úniku citlivých informácií.

V oblasti **autorského práva a súvisiacich práv** je významná najmä zraniteľnosť literárnych, umeleckých a vedeckých diel, ktoré sa pri online distribúcii stávajú predmetom nelegálneho kopírovania a pirátskeho šírenia. Významnú úlohu taktiež zohráva ochrana počítačových programov a databáz, ktoré sú častým cieľom útokov zameraných na malware či krádež dát. Digitálne prostredie vytvára nové riziká aj pre práva výkonných umelcov, výrobcov zvukových a audiovizuálnych záznamov a

¹⁰ ANDRAŠKO, Jozef - MESARČÍK, Matúš - SOKOL, Pavol: Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. ISBN: 978-80-7160-632-1. S. 14.

¹¹ NICHOLS, Lester: Cybersecurity architect's handbook: An end-to-end guide to implementing and maintaining robust security architecture. Birmingham: Packt Publishing, 2024. ISBN: 978-1-80323-584-4. s. 10-13.

vysielateľov, kde sa bezpečnostné opatrenia zameriavajú na ochranu pred neautorizovaným zdieľaním, nelegálnym šírením či neoprávneným prístupom k vysielacím platformám.

Priemyselné vlastníctvo je špecifické tým, že obsahuje vysoko hodnotné technické riešenia a inovácie. Patenty a s nimi súvisiace dodatkové ochranné osvedčenia sa často stávajú cieľom kyberšpionáže, predovšetkým v odvetviach farmaceutického a chemického priemyslu. Úžitkové vzory sú síce menej komplexné, avšak z hľadiska rizika neoprávneného kopírovania, či úniku dokumentácie, sú rovnako zraniteľné. Únik týchto dát alebo ich zneužitie môže dramaticky znížiť hodnotu nehmotného majetku a duševného vlastníctva podniku a tým aj schopnosť fungovať ako predmet záložného práva. Priemyselné dizajny a ochranné známky čelia riziku digitálneho falšovania a zneužitia v online prostredí, čo môže mať priamy negatívny dopad na dôveryhodnosť a reputáciu značiek. Osobitnú kategóriu predstavujú topografie polovodičových výrobkov a označenia pôvodu výrobkov, ktoré sú náchylné na sofistikované hackerské útoky a digitálne manipulácie. Rovnako aj ochrana odrôd rastlín si vyžaduje vysokú úroveň zabezpečenia, keďže genetické databázy predstavujú citlivý zdroj informácií s výraznou ekonomickou hodnotou.

V kategórii **súvisiacich práv** sú relevantné najmä subjekty, ktorých hodnota je úzko spätá s dôveryhodnosťou a dobrou povestou. Obchodné meno môže byť zneužitie pri phishingových útokoch, goodwill firmy je ohrozený narušením webovej prezentácie alebo únikom dát a obchodné tajomstvo je priamo závislé od efektívnych opatrení kybernetickej bezpečnosti. V modernom podnikateľskom prostredí sa zároveň objavujú formy nekalej súťaže, ktoré využívajú digitálne nástroje, od falošných recenzií až po manipulácie vyhľadávacích algoritmov. Osobitnú pozornosť si vyžadujú aj doménové mená, logá a slogany, ktoré môžu byť predmetom útokov typu domain hijacking, pričom ich ochrana je neoddeliteľne spätá so zabezpečením DNS infraštruktúry podniku (domain name system – DNS), systémom sieťových služieb a serverov, ktoré zabezpečujú preklad doménových mien na IP adresy a tým umožňujú fungovanie podnikových aplikácií, webov a interných služieb.

Z uvedeného vyplýva, že kybernetická bezpečnosť prestáva byť len technickou otázkou informačných technológií, ale predstavuje základný pilier udržania hodnoty a integrity nehmotného majetku a duševného vlastníctva vo všetkých jeho formách.

Záver

Spoločným menovateľom troch skúmaných oblastí je otázka hodnoty a bezpečnosti nehmotného majetku. Záložné právo poskytuje právny rámec, duševné vlastníctvo je zdrojom hodnoty a kybernetická bezpečnosť je garanciou jej uchovania. Tieto tri prvky tvoria jednotný systém, ktorý je dôležité analyzovať spoločne.

Duševné vlastníctvo sa stáva kľúčovým aktívom modernej ekonomiky. Jeho využitie ako predmetu záložného práva prináša nové výzvy, ktoré súvisia s jeho ocenením, zápisom do registra, akceptáciou veriteľmi a ochranou pred kybernetickými hrozbami. Ak sa tieto problémy podarí vyriešiť, otvorí sa priestor pre nové formy financovania a posilní sa konkurencieschopnosť podnikov.

Budúci vývoj by sa mohol orientovať na prepojenie jednotlivých kategórií ochrany, najmä na prepojenie právnych rámcov s technologickými riešeniami. Ďalšie výzvy môže priniesť aj právna úprava záložného práva v súvislosti s požiadavkami na kybernetickú bezpečnosť.

Na základe uvedeného možno konštatovať, že kybernetická bezpečnosť je integrálnou súčasťou stratégie ochrany duševného vlastníctva. Bez adekvátnej implementácie opatrení kybernetickej bezpečnosti hrozí, že výsledky kreatívnej a výskumnej činnosti stratia hodnotu, budú zneužitá alebo znehodnotená. Kybernetická bezpečnosť je kľúčovým predpokladom pre ochranu hodnoty duševného vlastníctva. Väčšina duševných práv je dnes uchovávaná v digitálnej forme, ako softvér, databázy, technická dokumentácia alebo know-how podnikov. Strata alebo únik týchto dát môže dramaticky znížiť hodnotu duševného vlastníctva a tým aj schopnosť fungovať ako predmet záložného práva.

Zoznam použitej literatúry

1. ANDRAŠKO, Jozef - MESARČÍK, Matúš - SOKOL, Pavol: Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. 186 s. ISBN: 978-80-7160-632-1.
2. HAVIER, Ján - PRIEHODA, Albert: Slovakia's journey. In: Unlocking IP-backed financing series: Country perspectives / The journey of the Visegrad Group. Ženeva: World Intellectual Property Organization, 2025. 62 s. ISSN: 3005-9747.
3. Intellectual property rights in an age of electronics and information [online]. Washington DC: Congress, Office of Technology Assessment, U.S. Government printing office, 1986. [cit.2025-08-25]. s. 116-126. Dostupné na: <https://repository.digital.georgetown.edu/handle/10822/708334>.
4. KULMALA, Riikka - KETTUNEN, Juha: Intellectual property protection and process modeling in small knowledge intensive enterprises. In: Information communication technology law, protection and access rights: global approaches and issues. Hershey: Information Science Reference, 2010. 560 s. ISBN: 978-161520-976-7.
5. NICHOLS, Lester: Cybersecurity architect's handbook: An end-to-end guide to implementing and maintaining robust security architecture. Birmingham: Packt Publishing, 2024. 496 s. ISBN: 978-1-80323-584-4.

6. REMENTILLA, Lilla: Intellectual property-backed financing. In: Intellectual property management for start-ups. Management for professionals. Cham: Springer, 2023. 521 s. ISBN: 978-303116-992-2.
7. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).
8. Zákon č. 185/2015 Z. z. Autorský zákon, v znení neskorších predpisov.
9. Zákon č. 595/2003 Z. z. o dani z príjmov, v znení neskorších predpisov.
10. Zákon č. 444/2002 Z. z. o dizajnoch, v znení neskorších predpisov.
11. Zákon 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
12. Zákon č. 513/1991 Zb. Obchodný zákonník, v znení neskorších predpisov.
13. Zákon č. 40/1964 Zb. Občiansky zákonník, v znení neskorších predpisov.
14. Zákon č. 146/2000 Z. z. o ochrane topografií polovodičových výrobkov, v znení neskorších predpisov.
15. Zákon č. 506/2009 Z. z. o ochranných známkach, v znení neskorších predpisov.
16. Zákon č. 469/2003 Z. z. o označeniach pôvodu výrobkov a zemepisných označeniach výrobkov, v znení neskorších predpisov.
17. Zákon č. 435/2001 Z. z. o patentoch, dodatkových ochranných osvedčeniach a o zmene a doplnení niektorých zákonov (Patentový zákon), v znení neskorších predpisov.
18. Zákon č. 202/2009 Z. z. o právnej ochrane odrôd rastlín, v znení neskorších predpisov.
19. Zákon č. 486/2013 Z. z. o presadzovaní práv duševného vlastníctva colnými orgánmi.
20. Zákon č. 431/2002 Z. z. o účtovníctve, v znení neskorších predpisov.
21. Zákon č. 517/2007 Z. z. o úžitkových vzoroch, v znení neskorších predpisov.
22. Zákon č. 527/1990 Zb. o vynálezoch, priemyselných vzoroch a zlepšovacích návrhoch, v znení neskorších predpisov.

Kontaktné údaje

Ing. Albert Priehoda, PhD.

albert.priehoda@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

Ústav ekonomických vied

SECURING DEMOCRACY: THE ROLE OF EU CYBERSECURITY LAW IN PROMOTING DEMOCRATIC SUSTAINABILITY¹

Matúš Mesarčík²

Abstract : The article analyses how European Union cybersecurity law supports the sustainability of democracy. Its objective is to examine the NIS2 Directive and the EU Cybersecurity Act as legal instruments that contribute to sustainability of democracy, with emphasis on forward-looking governance, democratic political culture, and protection of the environment. The study deploys a normative and doctrinal methodology, focusing on the scope and provisions of both instruments in the context of democratic theory and European policy frameworks. The findings show that the NIS2 Directive integrates long-term planning into organizational governance by requiring board-level accountability, risk management, and structured incident reporting. The Cybersecurity Act ensures continuity at Union level through a permanent mandate for ENISA and the creation of an EU-wide certification framework, fostering trust in digital systems. Together, these frameworks indirectly strengthen democratic culture through transparency and accountability and safeguard environmental infrastructures against cyber threats. The contribution lies in connecting cybersecurity regulation to democratic sustainability in both theory and practice.

Keywords: democracy, sustainability, cybersecurity law, security

Introduction

Nowadays, democracy is a challenging concept. On one hand, many subjects attempt to challenge democratic institutions and the concept as such. On the other hand, democratic deficit of the EU is often discussed and debated among academics.³

¹Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 17R05-04-V01-00002 (Competence Center for the Regulation of Cybersecurity, Privacy Protection and Cybercrime).

²Comenius University Bratislava, Faculty of Law, Institute of IT and IP Law.

³BLAUBERGER, Martin – NAURIN, Daniel – SEDELMEIER, Ulrich – WUNSCH, Natasha: The multi-level politics of countering democratic backsliding: state of the art and new research directions. In: Journal of European Public Policy, Vol. 32, No. 2 (2024), p. 323–340.

Democracy is one of the core values recognized by the founding treaties of the EU. „The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.”⁴ A deeper, substantive interpretation of the value of democracy within the European Union framework necessarily extends beyond mere reliance on majority rule. It encompasses the essential preconditions that enable a democratic system to function effectively, such as institutional integrity, respect for fundamental rights, and adherence to the rule of law.⁵

Sustainability, in the context of democracy, refers to a long-term and forward-looking orientation of democratic governance. Additionally, it means that democratic institutions and policies should not only address present needs but also safeguard the ability of future generations to meet theirs.

The connection between cybersecurity law and democratic sustainability is an underexplored field. Although research on cybersecurity, disinformation, and digital authoritarianism is expanding, few studies address how legal frameworks like the NIS 2 Directive and the EU Cybersecurity Act support democratic resilience.

Scholars traditionally frame cybersecurity as part of national resilience strategies, but without addressing democracy as a normative goal. Recently, Croissant and Lott⁶ introduce the concept of "democratic resilience," distinguishing between structural capacity and performance in crisis response. Their framework suggests that cybersecurity protections can serve as institutional safeguards against democratic erosion. Merkel adds that resilience requires not only technical capacity but also civic

<https://doi.org/10.1080/13501763.2024.2418957> or SCHERZ, Antonia: How should the EU respond to democratic backsliding? A normative assessment of expulsion and suspension of voting rights from the perspective of multilateral democracy. In: *Journal of European Public Policy*, (2025), p. 1–26. <https://doi.org/10.1080/13501763.2024.2444326>.

⁴ Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007. OJ C 202, 7.6.2016, pp. 1–388.

⁵ BOUZORAA, Nadia: The value of democracy in EU law and its enforcement: A legal analysis. In: *European Papers*, Vol. 8, No. 2 (2023), p. 809–851. ISSN 2499-8249. <https://doi.org/10.15166/2499-8249/690>.

⁶ CROISSANT, Aurel – LOTT, Lars: Democratic resilience in the twenty-first century. Search for an analytical framework and explorative analysis. Gothenburg: University of Gothenburg, Varieties of Democracy Institute, Working Paper No. 149, August 2024. Available at SSRN: <https://ssrn.com/abstract=4932497>.

engagement and trust-building.⁷ Pohle and Thiel⁸ argue that trust in digital systems is foundational for democratic legitimacy, and thus cybersecurity law plays a constitutive role in enabling public trust. Similarly, De Gregorio⁹ highlights that the resilience of information ecosystems, including the regulation of digital service providers, underpins democratic discourse.

Despite valuable insights across disciplines, there remains a gap in connecting EU cybersecurity law explicitly with democratic theory and sustainability frameworks. No comprehensive legal analysis yet examines how cybersecurity regulation contributes to the long-term viability of democratic institutions, processes, and rights.

This paper addresses that gap by offering a normative and doctrinal analysis of how the NIS 2 directive and the Cybersecurity Act can be interpreted as legal instruments supporting democratic sustainability.

This paper proceeds as follows.

After this introduction, the sustainability of democracy is analyzed through the lens of EU and Council of Europe policy approaches and democratic theory. Subsequently, the scope of NIS 2 Directive and Cybersecurity Act is defined and evaluated on how these norms apply in terms of sustainability of democracy. Conclusions are offered at the end of the paper.

Sustainability of democracy

Sustainability as the element of democracy has gained a recent prominence. The Council of Europe has explicitly identified "*sustainability and long-term orientation*" as one of the principles of good democratic governance.¹⁰ This principle recognizes that truly democratic decision-making must consider impacts beyond the next election cycle. According to the Council of Europe's guidelines: "*Efforts should prioritize the sustainability of decisions made by government...considering their impact on future generations... Current policy and decision-making processes incorporate principles of resilience, sustainability, and intergenerational equity, ... extending beyond*

⁷ MERKEL, Wolfgang: What is democratic resilience and how can we strengthen it? Toda Peace Institute, Policy Brief, 2023.

⁸ POHLE, Julia – THIEL, Thorsten: Digital sovereignty. In: Internet Policy Review [online], Vol. 9, No. 4 (2020). Available at: <https://policyreview.info/concepts/digital-sovereignty> [Accessed: 18 Sep. 2025].

⁹ DE GREGORIO, Giovanni: Digital constitutionalism in Europe. Cambridge: Cambridge University Press, 2022. ISBN 9781009291656.

¹⁰ Council of Europe: 12 Principles of Good Democratic Governance. Centre of Expertise for Multilevel Governance. Available at: <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> [Accessed: 05 Aug. 2025].

electoral cycles to meet the future needs of people and communities."¹¹ In practice, this could relate to sustainable development including balancing economic, social, and environmental concerns and fiscal responsibility, as well as the stability of democratic institutions themselves.

Philosophically, the idea of sustainability in democracy connects to the notion of trusteeship and responsibility toward those not yet born. Scholars argue that current majorities have an obligation not to irreversibly damage the world that future citizens will inherit.¹² This perspective has been brought into European discussions, for instance in arguments for lowering the voting age or creating "future councils" to voice coming generations' interests. While such innovations are nascent, the legal and policy trend is clear: European democracies are expected to incorporate long-term impact assessments and ensure that today's democratic choices do not undermine the *continuity and health of the democratic society* itself. The Council of Europe explicitly tying sustainability to good governance underscores that a democracy's legitimacy partly rests on its stewardship of the future.¹³

From a legal standpoint, intergenerational justice and sustainable governance are increasingly reflected in European policy documents. The EU, for example, integrates sustainability through treaties and charters that commit to environmental protection and balanced development.¹⁴ In the wake of the Arab Spring, the EU institutions articulated a concept of "deep and sustainable democracy" identifying common elements required: "*free and fair elections; freedom of association, expression and assembly; a free press; the rule of law administered by an independent judiciary (with*

¹¹ Council of Europe: 12 Principles of Good Democratic Governance. Centre of Expertise for Multilevel Governance. Available at: <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> [Accessed: 05 Aug. 2025].

¹² THOMPSON, Dennis F.: Representing future generations: political presentism and democratic trusteeship. In: Critical Review of International Social and Political Philosophy, Vol. 13, No. 1 (2010), p. 17–37. <https://doi.org/10.1080/13698230903326232>

or JENSEN, Karsten Klint: Future Generations in Democracy: Representation or Consideration? In: Jurisprudence, Vol. 6, No. 3 (2015), p. 535–548.

¹³ Council of Europe: 12 Principles of Good Democratic Governance. Centre of Expertise for Multilevel Governance. Available at: <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> [Accessed: 05 Aug. 2025].

¹⁴ Article 3(3), Treaty on the EU reads: "The Union shall establish an internal market. It shall work for the *sustainable development of Europe* based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the *quality of the environment*. It shall promote scientific and technological advance. It shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations and protection of the rights of the child. It shall promote economic, social and territorial cohesion, and solidarity among Member States. It shall respect its rich cultural and linguistic diversity, and shall ensure that Europe's cultural heritage is safeguarded and enhanced."

*right to a fair trial); fighting corruption; and democratic control over security forces.*¹⁵ In my view, it is absolutely essential to emphasize the role of democratic control over security and law enforcement forces as these entities serve as a safeguards of democracy and democratic processes in general.

While not traditionally framed as a core element of democracy, the inclusion of sustainability signals that democracies should not sacrifice long-term welfare for short-term populist gains. The Council of Europe's emphasis suggests that a democracy should function in a way that "*strategic planning extends beyond electoral mandates*", ensuring continuity and preparedness for future challenges.¹⁶ A sustainable democracy maintains institutional continuity, adapts to change, and remains resilient even in crises. For example, during emergencies like pandemics or climate crises, democratic institutions must balance urgent action with preservation of rights and future interests – a concept some scholars frame as "democratic resilience."¹⁷

Another important aspect is the presence and strength of democratic political culture. Democratic political culture refers to the set of shared attitudes, values, beliefs, norms, and practices that support and sustain democratic institutions and processes within a society. It shapes how citizens perceive democracy, how they engage with political institutions, and how they treat one another as political actors.¹⁸ This aspect is explicitly measured by the Economist Democracy Index. These indicators include societal support for democracy, such as the public's general commitment to democratic principles; rejection of authoritarian alternatives,

¹⁵ European Commission – High Representative of the Union for Foreign Affairs and Security Policy: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A new response to a changing Neighbourhood. Brussels: European Commission, 25 May 2011, COM(2011) 303 final.

¹⁶ Council of Europe: 12 Principles of Good Democratic Governance. Centre of Expertise for Multilevel Governance. Available at: <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> [Accessed: 05 Aug. 2025].

¹⁷ For example, BIDDLE, Nicholas – FISCHER, Alexander – ANGUS, Simon D. – ERCAN, Selen – GRÖMPING, Max – GRAY, Matthew: Democratic resilience: moving from theoretical frameworks to a practical measurement agenda. (2025). Available at SSRN: <https://ssrn.com/abstract=5202987> or <http://dx.doi.org/10.2139/ssrn.5202987>

or WALZ, Kevin – MERTEN, Lena – ROSENTHAL, Michael et al.: From latest buzzword to conceptual framework: Unraveling the complexities of democratic resilience. In: Zeitschrift für Vergleichende Politikwissenschaft, Vol. 19 (2025), p. 93–122. <https://doi.org/10.1007/s12286-024-00618-7> or CROISSANT, Aurel – LOTT, Lars: Democratic resilience in the twenty-first century. Search for an analytical framework and explorative analysis. Gothenburg: University of Gothenburg, Varieties of Democracy Institute, Working Paper No. 149, August 2024. Available at SSRN: <https://ssrn.com/abstract=4932497>.

¹⁸ INGLEHART, Ronald – WELZEL, Christian: Political culture and democracy: Analyzing cross-level linkages. In: Comparative Politics, Vol. 36, No. 1 (2003), p. 61–79. <https://doi.org/10.2307/4150160>.

including opposition to strong leaders who bypass democratic institutions or support for military or technocratic rule; belief in democracy's effectiveness in ensuring public order and managing the economy; endorsement of democratic norms and procedures, like free elections and checks and balances; and a cultural tradition of separating religion from political authority, reflecting liberal democratic values.¹⁹

Finally, the importance of the protection of the environment as part of democratic sustainability shall be emphasized. A healthy environment is a precondition for effective democratic participation. Environmental degradation can undermine public health, equality, and social stability, all of which are essential for meaningful civic engagement and democratic deliberation. Democratic sustainability implies a responsibility not only to current citizens but also to future generations. Environmental protection directly serves this purpose by preserving resources, public health, and livable conditions for those not yet born. The European Green Deal frames climate and environmental policy as a matter of democratic legitimacy, requiring transparency, participation, and accountability.²⁰

In sum, sustainability as a democratic element means governing with foresight, responsibility, and care for the prosperity, environment, and rights of coming generations – so that democracy endures and continues to deliver over time.

The brief overview of the EU Cyber-security law

The scope of the NIS2 Directive is primarily provisioned in Articles 2 and 3. Article 2(1) stipulates that the directive applies to “public or private entities of a type referred to as essential entities or important entities” operating within the EU.²¹ These classifications are elaborated in Annexes I and II, which enumerate sectors of high criticality, including energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, and space. Further, other critical sectors such as postal and courier services, waste management, the manufacture and production of critical products, food, chemicals, and digital providers are also covered. Article 3 specifies that the directive pertains to entities meeting, or exceeding, the criteria for medium-sized enterprises in accordance with Commission Recommendation 2003/361/EC,²² with certain smaller entities included when their services are considered critical. Accordingly, NIS2

¹⁹ THE ECONOMIST INTELLIGENCE UNIT: The Democracy Index 2024. London: The Economist Intelligence Unit, 2025, part Democratic and Political Culture.

²⁰ European Commission: European Green Deal. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en [Accessed: 05 Aug. 2025].

²¹ NIS 2 Directive, Articles 2 and 3.

²² Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422). OJ L 124, 20.5.2003, pp. 36–41.

significantly broadens the scope established by the original NIS Directive, encompassing a wider array of sectors and organizations vital to societal and economic stability. The NIS 2 Directive sets forth security requirements and incident reporting obligations for these entities, while equipping national authorities with supervisory and enforcement powers, thereby embedding cybersecurity resilience throughout both essential and important sectors across the EU.

The scope of the EU Cybersecurity Act²³ is precisely defined in Article 1, which delineates two principal pillars. Firstly, the Act confers a permanent mandate upon the European Union Agency for Cybersecurity (ENISA), enhancing its responsibilities and reinforcing its capacity to support Member States, EU institutions, and stakeholders in attaining robust cybersecurity standards. Secondly, the Act introduces a European cybersecurity certification framework for information and communications technology (ICT) products, services, and processes. Article 1(2) clarifies that the Regulation covers ENISA's mandate as well as the cybersecurity certification of ICT products, services, and processes. Article 46 further expands on the certification framework, specifying that European cybersecurity certification schemes implemented under the Regulation aim to ensure compliance with established security requirements, with certificates recognized throughout the Union. Thus, the Regulation provides a dual scope. It solidifies ENISA's role as the EU's central cybersecurity agency with enduring duties in capacity-building, policy development, and operational coordination, and establishes a harmonized EU-wide mechanism for certifying and assuring cybersecurity standards. This framework extends to ICT products and services across all sectors of the digital economy, with the objective of fostering uniform security standards, minimizing market fragmentation, and enhancing trust in digital technologies throughout the Union.

Sustainability of democracy through the lens of the EU cyber-security law

As a general point, the EU cyber-security laws, especially NIS 2 directive recognizes several sectors as being of (high) criticality that are directly relevant for sustainability of democracy. Digital infrastructure and public administration as high critical sectors may be mentioned. Democracy is even explicitly mentioned in the recital 70 of the NIS 2 directive in the context of large-scale cybersecurity incidents.²⁴

²³ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151, 7.6.2019, pp. 15–69.

²⁴ NIS 2 directive, recital 70: „Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response because of the high degree of interdependence between sectors and Member States. The availability of cyber-resilient network and

In the section explaining what represents sustainability of democracy, we have emphasized three essential aspects: long-term or forward-looking policy, strength of democratic political culture, and protection of the environment. I will argue that each of these goals are to certain extent protected by the discussed EU cyber-security framework.

The NIS2 Directive embeds **long-termism** into daily governance of essential and important entities by making cyber-risk a standing boardroom duty and by establishing mechanisms for continuity planning. Article 20 requires that the management bodies of covered entities approve the cybersecurity risk-management measures taken under Article 21, oversee their implementation, and can be held liable for infringement of those obligations. At the same time, the provision also compels regular training for members of management bodies so they have sufficient knowledge and skills to evaluate cyber-risk practices and their service impact, which hard-wires future-oriented capacity into institutional leadership rather than relying on short electoral or corporate cycles.²⁵ Article 21 then operationalizes this forward-looking duty by requiring appropriate and proportionate technical, operational and organizational measures including risk analysis, incident handling, business continuity and crisis management, supply-chain security, and secure development and maintenance, thereby forcing entities to plan for persistence under stress rather than ad-hoc recovery after incidents or exposure of vulnerabilities. The directive's reporting regime under Article 23 completes this loop by mandating early warnings within 24 hours and incident notifications within 72 hours, followed by final reports, which creates a durable learning cycle and enables authorities to provide guidance "within 24 hours" of the early warning. Such architecture is primarily designed for continuous improvement beyond single events.

The Cybersecurity Act institutionalizes long-term coordination capacity by granting ENISA a permanent mandate and by creating an EU-wide cybersecurity certification framework. Article 1 sets out the regulation's scope "with a view to... a high level of cybersecurity, cyber resilience and trust," covering ENISA's tasks and the certification of ICT products, services and processes, while Title III inaugurates the certification framework itself. Article 46 establishes the European cybersecurity certification framework, under which schemes adopted by the Commission provide Union-wide validity; Article 49 details how schemes are prepared and adopted; Articles 51–52 define security objectives and assurance levels that anchor a risk-

information systems and the availability, confidentiality and integrity of data are vital for the security of the Union and for the protection of its citizens, businesses and institutions against incidents and cyber threats, as well as for enhancing the trust of individuals and organisations in the Union's ability to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, **democracy** and the rule of law."

²⁵ NIS 2 directive, Article 20 (2).

based evaluation pathway over a product's lifecycle. The academic literature underscores how this architecture is designed to produce durable market incentives for "security-by-design"²⁶ and to reduce fragmentation over time.²⁷

Democratic political systems require **public trust in institutions, consistent governance**, and mechanisms for accountability. The NIS2 directive addresses these elements by emphasizing transparency and accountable governance within the framework of cyber-resilience. As discussed, article 20 assigns management bodies responsibility for compliance and mandates relevant training, indicating that cyber-risk management is considered a significant leadership responsibility.

Article 23 provisions structured reporting processes, including early warning within twenty-four hours, incident notifications within seventy-two hours, and submission of a final report.²⁸ This procedure establishes a record of interactions between state and market actors for examination by regulators, parliaments, and, when appropriate, the public, with the aim of promoting transparency and continuous improvement.

At the systemic level, ENISA's ongoing mandate described in Article 1 of the Cybersecurity Act and the EU-wide certification framework outlined in Articles 46–52 is intended to standardize requirements and assurances among EU member States, thereby addressing information disparities that may impact public confidence. Scholarship discusses the trust function, noting that comparative analysis of EU and US cybersecurity approaches describes the EU model as comprehensive and based on hard law, with objectives related to resilience and trust.²⁹ Research also identifies certification and coordinated governance as elements of a collective EU response to changing cybersecurity threats.³⁰

The same provisions also support the media and information environment that democratic processes depend on. By requiring essential entities in sectors like digital infrastructure to implement risk-management strategies and rapid incident reporting, NIS2 aims to decrease the likelihood and duration of outages or security

²⁶ KOHLER, Constant: The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. In: *International Cybersecurity Law Review*, Vol. 1 (2020), p. 7–12. <https://doi.org/10.1365/s43439-020-00008-1>.

²⁷ CARRAPICO, Helena – FARRAND, Benjamin: Cybersecurity trends in the European Union: regulatory mercantilism and the digitalisation of geopolitics. In: *JCMS: Journal of Common Market Studies*, Vol. 62 (2024), p. 147–158. <https://doi.org/10.1111/jcms.13654>.

²⁸ NIS 2 directive, Article 23.

²⁹ FAHEY, Elaine: The evolution of EU–US cybersecurity law and policy: on drivers of convergence. In: *Journal of European Integration*, Vol. 46, No. 7 (2024), p. 1073–1088. <https://doi.org/10.1080/07036337.2024.2411240>.

³⁰ CARRAPICO, Helena – FARRAND, Benjamin: Cybersecurity trends in the European Union: regulatory mercantilism and the digitalisation of geopolitics. In: *JCMS: Journal of Common Market Studies*, Vol. 62 (2024), p. 147–158. <https://doi.org/10.1111/jcms.13654>.

breaches that affect communication, emergency notifications, and access to public information. The directive's annexes and sectoral coverage indicate that the regulation encompasses core services necessary for diverse public discourse, including energy supply for networks, internet exchange, and DNS routes, thereby maintaining conditions for public access to information.

Considering **environmental aspects**, two highlights can be made. First, NIS2's scope expressly covers sectors of high criticality such as energy, drinking water, wastewater and waste management, ensuring that operators adopt Article 21 measures including risk analysis, continuity planning, and secure operations that serve as prerequisite to the reliable delivery of environmental and public-health services. Second, NIS2 frames risk management through an "all-hazards approach," with recital text specifying that measures "should... address the physical and environmental security of network and information systems,"³¹ protecting against theft, fire, flood, power failure and natural phenomena in line with standards such as ISO/IEC 27000. This language pushes entities to design resilience that includes the surrounding physical and ecological context rather than treating ICT risks in isolation. Certification under the Cybersecurity Act supports these objectives by encouraging security for ICT practices throughout environmental value chains. Articles 46 and 52 permit schemes to assign assurance levels based on risk, enabling high-impact systems such as industrial control components in water or energy sectors to be included in "substantial" or "high" assurance categories.

Conclusion

In summary, the NIS2 Directive and the EU Cybersecurity Act address the challenges of sustainable governance encountered by contemporary democracies. These measures incorporate long-term, intergenerational perspectives into cybersecurity policy by requiring current investments in security to mitigate future risks and establishing frameworks that extend beyond national and electoral boundaries. This strategy aligns with the principle that democracies have a responsibility to safeguard the interests of future generations—paralleling environmental legislation intended to protect the planet for posterity, cybersecurity regulations such as NIS2 and the Cybersecurity Act are indirectly designed to secure the digital infrastructure essential to society for both present and future stakeholders. The Council of Europe's emphasis on linking sustainability with good governance is realized here, as a democracy's legitimacy is increasingly evaluated by its management of cybersecurity and its capacity to ensure the ongoing stability of an open, secure, and free society amid evolving technological threats. The EU's legal framework for cybersecurity, by addressing internal governance, broad societal resilience, and forward-looking

³¹ NIS 2 directive, Recital 79.

regulation, is a testament to how law and policy can adapt to sustain democracy in the long run.

Bibliography

1. BIDDLE, Nicholas – FISCHER, Alexander – ANGUS, Simon D. – ERCAN, Selen – GRÖMPING, Max – GRAY, Matthew: Democratic resilience: moving from theoretical frameworks to a practical measurement agenda. (2025). Available at SSRN: <https://ssrn.com/abstract=5202987> or <http://dx.doi.org/10.2139/ssrn.5202987>
2. BLAUBERGER, Martin – NAURIN, Daniel – SEDELMEIER, Ulrich – WUNSCH, Natasha: The multi-level politics of countering democratic backsliding: state of the art and new research directions. In: *Journal of European Public Policy*, Vol. 32, No. 2 (2024), p. 323–340. <https://doi.org/10.1080/13501763.2024.2418957>
3. BOUZORAA, Nadia: The value of democracy in EU law and its enforcement: A legal analysis. In: *European Papers*, Vol. 8, No. 2 (2023), p. 809–851. ISSN 2499-8249. <https://doi.org/10.15166/2499-8249/690>
4. CARRAPICO, Helena – FARRAND, Benjamin: Cybersecurity trends in the European Union: regulatory mercantilism and the digitalisation of geopolitics. In: *JCMS: Journal of Common Market Studies*, Vol. 62 (2024), p. 147–158. <https://doi.org/10.1111/jcms.13654>
5. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422). In: *Official Journal of the European Union*, OJ L 124, 20.5.2003, pp. 36–41.
6. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. In: *Official Journal of the European Union*, OJ C 202, 7.6.2016, pp. 1–388.
7. Council of Europe: 12 Principles of Good Democratic Governance. Centre of Expertise for Multilevel Governance. Available at: <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> [Accessed: 05 Aug. 2025].
8. CROISSANT, Aurel – LOTT, Lars: Democratic resilience in the twenty-first century. Search for an analytical framework and explorative analysis. Gothenburg: University of Gothenburg, Varieties of Democracy Institute, Working Paper No. 149, August 2024. Available at SSRN: <https://ssrn.com/abstract=4932497>
9. DE GREGORIO, Giovanni: Digital constitutionalism in Europe. Cambridge: Cambridge University Press, 2022. ISBN 9781009291656.

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). In: *Official Journal of the European Union*, OJ L 333, 27.12.2022, pp. 1–116.
11. European Commission: European Green Deal. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en [Accessed: 05 Aug. 2025].
12. FAHEY, Elaine: The evolution of EU–US cybersecurity law and policy: on drivers of convergence. In: *Journal of European Integration*, Vol. 46, No. 7 (2024), p. 1073–1088. <https://doi.org/10.1080/07036337.2024.2411240>
13. INGLEHART, Ronald – WELZEL, Christian: Political culture and democracy: Analyzing cross-level linkages. In: *Comparative Politics*, Vol. 36, No. 1 (2003), p. 61–79. <https://doi.org/10.2307/4150160>
14. JENSEN, Karsten Klint: Future Generations in Democracy: Representation or Consideration? In: *Jurisprudence*, Vol. 6, No. 3 (2015), p. 535–548.
15. KOHLER, Constant: The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. In: *International Cybersecurity Law Review*, Vol. 1 (2020), p. 7–12. <https://doi.org/10.1365/s43439-020-00008-1>
16. MERKEL, Wolfgang: What is democratic resilience and how can we strengthen it? Toda Peace Institute, Policy Brief, 2023.
17. POHLE, Julia – THIEL, Thorsten: Digital sovereignty. In: *Internet Policy Review* [online], Vol. 9, No. 4 (2020). Available at: <https://policyreview.info/concepts/digital-sovereignty> [Accessed: 18 Sep. 2025].
18. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In: *Official Journal of the European Union*, OJ L 151, 7.6.2019, pp. 15–69.
19. SCHERZ, Antonia: How should the EU respond to democratic backsliding? A normative assessment of expulsion and suspension of voting rights from the perspective of multilateral democracy. In: *Journal of European Public Policy*, (2025), p. 1–26. <https://doi.org/10.1080/13501763.2024.2444326>
20. THOMPSON, Dennis F.: Representing future generations: political presentism and democratic trusteeship. In: *Critical Review of International Social and Political Philosophy*, Vol. 13, No. 1 (2010), p. 17–37. <https://doi.org/10.1080/13698230903326232>
21. WALZ, Kevin – MERTEN, Lena – ROSENTHAL, Michael et al.: From latest buzzword to conceptual framework: Unraveling the complexities of democratic

resilience. In: *Zeitschrift für Vergleichende Politikwissenschaft*, Vol. 19 (2025), p. 93–122. <https://doi.org/10.1007/s12286-024-00618-7>

Contact details

doc. JUDr. Matúš Mesarčík, PhD., LL.M

matus.mesarcik@flaw.uniba.sk

Institute of Information Technology Law and Intellectual Property Law

Faculty of Law

Comenius University Bratislava

NEXT-GENERATION CYBERCRIME: ARTIFICIAL INTELLIGENCE, DEEPFAKES, AND FINANCIAL FRAUD¹

Matej Smalik²

Abstract: The development of artificial intelligence brings not only innovative opportunities for industry and society, but also new threats in the field of cybercrime. The most striking trends include the use of AI for sophisticated attacks, the creation of deepfake content and the implementation of financial frauds that purposefully abuse the trust of individuals. Article examines how criminals are leveraging AI (especially generative AI) across financial fraud and cybercrime, from sophisticated phishing to hard-to-detect deepfakes and tries to analyze recent cases where AI-generated fake audio or video was used to impersonate executives and trick employees. The paper will also focus on current techniques and scenarios used by attackers (mostly in deepfakes) and examples of real cases, as well as aspects that increase the effectiveness of these attacks. At the same time, detection options, prevention and legislative challenges that are relevant for limiting these threats will be analyzed. By integrating legal and technical steps, the article also provides an overview of used financial deepfake techniques as well as the standpoint of European Union in this matter.

The article adopts a qualitative doctrinal legal analysis as its foundation and systematically reviews primary legal materials, such as statutes, regulations, scholar literature and case law. This approach is represented by synthesizing core legal doctrines from the relevant sources, selected case studies of notable AI-enabled fraud and deepfake incidents. Recognizing that cybercrime is inherently transnational and socio-technical, the methodology integrates comparative and interdisciplinary elements. The author focuses on legal norms with insights from computer science and criminology to account for the technical and social dimensions of deepfake fraud. Altogether, the methodology entails legal interpretation with case review and empirical and technological considerations. This framework aligns with established legal research standards and underpins the article's interdisciplinary inquiry into law, cybercrime, and emerging technology.

¹Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 17R05-04-V01-00002 (Competence Center for the Regulation of Cybersecurity, Privacy Protection and Cybercrime)

²Comenius University in Bratislava, Faculty of law, Department of commercial and economic law

Keywords: cybersecurity, cybercrime, artificial intelligence, deepfake, financial fraud

Introduction

The field of cybersecurity has changed dramatically since the Cybersecurity Strategy for the Digital Decade was presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy in December 2020³. The accelerated development of artificial intelligence (AI) has generated significant opportunities across a wide range of industries. However, it has simultaneously introduced a host of unprecedented cybersecurity threats. Contemporary discourse increasingly characterizes this period as an the so-called exploitation zone with the widening gap between the rapid pace of technological innovation and the comparatively slower capacity of societal institutions to adapt through awareness, defensive measures, and regulatory frameworks. Cybercriminal actors have been particularly adept at exploiting this disparity, employing AI not only to expand conventional attack methods but also to design entirely new forms of cybercrime. Prominent among these developments are AI-enabled intrusions, the proliferation of deepfake technologies for purposes of deception, and increasingly sophisticated forms of financial fraud that capitalize on human vulnerabilities⁴. These emergent risks present many challenges; technically, in terms of detection and prevention, as well as legally, in relation to the adequacy of existing information technology and intellectual property regimes. Currently, detection systems can identify the majority of deepfakes depending on their quality; however, the increasing sophistication of deepfakes has largely exceeded human detection⁵. Deepfake detection approaches fall into two categories: those applied during creation and those used upon receipt⁶.

³ RAMPÁŠEK, M.; MESARČÍK, M.; ANDRAŠKO, J: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: Computer Law & Security Review, volume 56, 2025. United Kingdom: Elsevier Ltd, article no. 106093, P.1

⁴ MIZEROVÁ, Tina: Právo versus Deepfakes. In: In: ACTA UNIVERSITATIS CAROLINAE – IURIDICA 2/2025, 2025. Prague: Faculty of Law of Charles University, p. 116

⁵KURSHAN, Eren; MEHTA, Dhagash; BALCH, Tucker; BYRD, David: AI-Driven Fraud, Financial and Cybercrime: Emerging Threats and the Evolving Landscape of AI versus AI. In: International Journal of Semantic Computing. Singapore: World Scientific Publishing Co. Pte. Ltd., 2025, P. 7

⁶ROMERO-MORENO, Felipe: Deepfake detection in generative AI: A legal framework proposal to protect human rights. In: Computer Law & Security Review, Volume 58, 2025. United Kingdom: Elsevier Ltd, 2025, article no. 106162., P.4

The defining characteristic of emerging forms of cybercrime lies in the systematic exploitation of trust that is mostly based on social relations and fair treatment.⁷ Whether manifested through a fabricated voice message purporting to be from a family member, a falsified video depicting a public figure, or an AI-generated digital persona cultivating online relationships, malicious actors are leveraging artificial intelligence to destabilize individuals' perceptions of authenticity and reality. What is required is a measured, nuanced framework that protects individuals and institutions from malicious uses of AI without impeding innovation or legitimate creative expression. In addition, the discussion assesses the evolution of detection technologies, preventive strategies, and legal responses⁸. Central to this inquiry is the intersection of cybersecurity, information technology law, and intellectual property law, as policymakers confront the necessity of adapting legal frameworks to encompass AI-generated content and AI-assisted criminal methodologies. Ultimately, the defense against next-generation cybercrime must be comprehensive, integrating advanced technical safeguards, adaptive regulatory structures, and widespread public awareness to build resilience against AI-mediated deception.

Deepfakes "in genere"

Among the various criminal applications of artificial intelligence, deepfakes have garnered the greatest degree of public attention. A deepfake is a form of synthetic media, most commonly video or audio, designed to imitate real individuals engaging in actions or speech they never in fact performed. Such media are generated through advanced AI methodologies, particularly deep learning techniques⁹ such as generative adversarial networks (GANs), which can produce highly realistic visual or auditory outputs by training on extensive datasets of authentic material. In essence, a GAN-based system incrementally refines its ability to transpose one individual's facial features or vocal patterns onto another's body or speech, ultimately achieving outputs that approach indistinguishability from genuine recordings.

⁷ANDRIICHENKO, Nadiia: A step toward improvement of police performance assessment as subjects of combating financial and economic crimes: experience of Ukraine and Slovakia. In *Bratislava Law Review*, 2/2018. Bratislava: Comenius University Bratislava, Faculty of Law, 2018. P. 129

⁸ With regards to attributability of the AI-generated content see: BAČÁROVÁ, Renáta: Impact of artificial intelligence on the single market for digital content. In: *ACTA UNIVERSITATIS CAROLINAE – IURIDICA* 2/2025, 2025. Prague: Faculty of Law of Charles University, p. 176

⁹ ANDRAŠKO, Jozef; MESARČÍK, Matúš; HAMULÁK, Ondrej: The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. In: *AI & Society*, volume 36(2). London: Springer Nature, 2021, P. 623.

What originated only a few years ago as a relatively trivial novelty such as digitally inserting celebrities into cinematic scenes for comedic effect, has since matured into a potent technology that destabilizes the boundary between reality and fabrication. At present, even individuals with limited technical expertise can access publicly available applications or online services to generate impersonations that, at least upon superficial inspection, appear authentic. One of the most immediate and consequential applications of deepfake technology lies in its use to perpetrate financial fraud through impersonation. This represents a technologically enhanced evolution of traditional schemes such as business email compromise or “CEO fraud,” now rendered far more convincing by AI-generated voices and videos.

A prominent incident occurred in early 2024, when an employee of the multinational engineering firm Arup was deceived into transferring over USD 25 million following what appeared to be a routine videoconference with the company’s Chief Financial Officer. In reality, the “CFO” (and potentially several other colleagues present on the call) were synthetic fabrications created through deepfake technology. The fabricated executives urgently instructed the employee to authorize several wire transfers, which were executed and swiftly routed through Hong Kong bank accounts before disappearing. Arup’s Chief Information Officer later remarked that, while the company had long contended with phishing and spoofing attempts, the integration of deepfakes had raised the sophistication of attacks to a level where even live video interactions were no longer reliable indicators of authenticity¹⁰.

This case is not isolated. A new frontier opened up for financial crime in 2019. In what is considered the first case of its kind, fraudsters used an artificial intelligence (AI) voice clone of a German energy boss to scam the head of a UK subsidiary out of €220,000. In 2020, fraudsters escalated this tactic, reportedly using a synthetic voice to impersonate a director in the United Arab Emirates and secure a transfer of USD 35 million. Beyond corporate environments, law enforcement agencies, including the FBI, have documented a surge in “vishing” scams wherein voice clones of family members are used to demand ransom or emergency funds. So-called “virtual kidnapping” schemes, in which a parent receives a call featuring a fabricated recording of their child in distress, have been reported internationally, with elderly victims disproportionately targeted¹¹.

Deepfakes have also infiltrated the domain of investment and cryptocurrency fraud. Criminal groups have produced synthetic videos of prominent figures (most notably

¹⁰ ELLIOT, David: This happens more frequently than people realize’: Arup chief on the lessons learned from a \$25m deepfake crime In World Economic Forum, cited [13.11.2025] available at <https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/>

¹¹ STUPP, Catherine: Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case In: The Wall Street Journal, cited [13.11.2025] available at <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

Tesla CEO Elon Musk) purporting to endorse fraudulent trading platforms. Such content has been widely disseminated via online advertising, lending deceptive credibility to fraudulent schemes. In one striking case from 2024, an 82-year-old U.S. retiree lost USD 690,000 to a fraudulent platform promoted through a highly realistic deepfake of Musk¹². Victims consistently reported that the videos were so lifelike that even after being informed of the fraud, rewatching the footage continued to sow doubt because “that’s him” in both appearance and voice. By late 2024, Musk deepfakes had become so pervasive that commentators labeled them “the Internet’s biggest scammer,” with millions of dollars in losses attributed to such content globally.

Large-scale operations have similarly been uncovered in Asia. In 2024, Hong Kong police disrupted a transnational scam network that combined romance fraud with cryptocurrency investment schemes. The group deployed an AI-generated female persona to cultivate online relationships with victims across Hong Kong, Taiwan, Singapore, and India, ultimately luring them into investing in a fabricated cryptocurrency trading platform. The operation, orchestrated by a team of highly educated perpetrators, netted over USD 46 million before its dismantling¹³.

Collectively, these incidents demonstrate how deepfake technologies amplify classical forms of fraud by adding a powerful illusion of authenticity. Human beings are evolutionarily predisposed to trust sensory cues such as facial expressions and vocal tones. A convincing synthetic replication of these cues can therefore override instinctive suspicions victims often reason that, despite initial doubts, the presence of a “real” voice or face validated the interaction. In this respect, deepfakes have fundamentally altered the landscape of social engineering, enabling deception at a scale and effectiveness previously unattainable. Europol emphasizes that scams based on social engineering – investment frauds and business email compromise (BEC) – rank among the most significant threats¹⁴.

¹² Elon Musk Deepfake Scams: Retiree Loses \$690,000 in AI-Driven Fraud Frenzy, cited [20.09.2025] available at <https://www.ainvest.com/news/elon-musk-deepfake-scams-retiree-loses-690-000-in-ai-driven-fraud-frenzy-24081010faae3734e4ef66bd/>

¹³ REDDICK, James: Hong Kong police bust fraud ring that used face-swapping tech for romance scams, cited [20.09.2025] available at <https://therecord.media/hong-kong-police-bust-romance-scammers-face-swapping-deepfakes>

¹⁴ Europol – “Online Fraud Schemes: A Web of Deceit” Spotlight Report (december 2023), cited [20.09.2025], available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf#:~:text=EUROPOL%20SPOTLIGHT%20%E2%80%93%20ONLINE%20FRAUD,Online%20fraudsters%20target%20millions%20of

Deepfakes related to financial schemes

Deepfake-generated video content has emerged as a particularly effective instrument for the manipulation of consumers. The increasing technical quality of such media renders human detection progressively more difficult, thereby heightening the attendant risks. This phenomenon directly undermines public confidence in legitimate institutions and erodes trust in the financial system, including banks and supervisory authorities. Such erosion of confidence may give rise to broader societal harms, including heightened skepticism toward official communications and reduced participation in legitimate financial products. The ready availability of artificial intelligence tools capable of producing deepfake videos, even to individuals possessing minimal technical proficiency and combined with the emergence of a “fraud-as-a-service” model, renders these attacks highly scalable and pervasive.

Set out below is an overview of key instances in which deepfake technology has been employed in the commission of financial crime, together with potential countermeasures, as reflected in the practices of foreign regulatory and enforcement bodies.

Deepfake Investment and “Get-Rich-Quick” Fraud Schemes

Fraudulent actors increasingly employ deepfake video and audio recordings of public figures, celebrities, or financial professionals to promote fictitious investment opportunities promising unrealistically high and rapid returns. Such schemes frequently involve dubious offers relating to digital assets, manipulated videos of well-known individuals, and requests for sensitive information such as one-time passwords (OTPs) or credit card details.

Regulatory authorities, such as the U.S. Securities and Exchange Commission (SEC), issue public advisories regarding deepfake-driven investment frauds and highlight “red flags” for consumers, including suspicious cryptocurrency offerings and altered celebrity videos. The SEC recommends verifying the legitimacy of any investment opportunity directly with the competent regulator¹⁵.

Likewise, the European Securities and Markets Authority (ESMA) counsels investors to exercise skepticism toward unrealistic profit claims and deepfake materials, to

¹⁵ Beware of Fraudsters Impersonating Investment Professionals and Firms – Investor Alert, cited [13.11.2025], available at: <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/beware-fraudsters-impersonating-investment-professionals-and-firms-investor-alert>

verify sources, and to report suspect content¹⁶. Financial supervisory bodies, such as the U.K. Financial Conduct Authority (FCA), actively deploy artificial intelligence and machine-learning systems to monitor online platforms and social media in order to detect fraudulent websites and advertisements and to facilitate their removal¹⁷.

Fraud in Account Opening and Identity Verification (KYC/CDD)

Deepfake technology is increasingly employed to fabricate falsified identification documents (including images and videos) or to impersonate individuals during remote registration and identity verification processes (Know Your Customer/Customer Due Diligence - KYC/CDD). The objective is to open fraudulent accounts, circumvent due diligence controls, or commit synthetic identity theft, wherein fictitious identities are created by combining authentic and fabricated personal data.

The U.S. Financial Crimes Enforcement Network (FinCEN) has issued guidance (FIN-2024-Alert004) to financial institutions, setting out detailed red-flag indicators for identity-related deepfake fraud. These include inconsistent photographic attributes, refusal to engage in multi-factor authentication (MFA), the use of third-party webcam plug-ins, and matches between submitted images and online galleries of AI-generated faces. Regulatory authorities encourage and, in some cases, mandate the implementation of advanced technological safeguards. These include MFA, liveness detection tools capable of distinguishing between natural persons and synthetic media, and behavioral biometrics for assessing user activity patterns¹⁸.

The European Banking Authority (EBA) has highlighted incidents in which firms failed to detect remote account openings facilitated by AI-generated identity documents. These cases underscore the necessity of updating fraud-detection controls to address synthetic identities and of integrating enhanced monitoring scenarios into KYC/CDD frameworks¹⁹.

¹⁶Using Artificial Intelligence for Investing: What you should consider, cited [13.11.2025], available at: https://www.esma.europa.eu/sites/default/files/2025-03/ESMA_Warning_on_the_use_of_AI_-_EN.pdf

¹⁷AI Update by Financial Conduct Authority, cited [13.11.2025], available at: <https://www.fca.org.uk/publication/corporate/ai-update.pdf>

¹⁸ FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, cited [13.11.2025], available at: <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial>

¹⁹ European Banking Authority: Response to consultation on draft Guidelines on the use of remote customer onboarding solutions, cited [13.11.2025], available at: https://www.eba.europa.eu/eba-response/33123?destination=%2Fpublications-and-media%2Fevents%2Fconsultation-draft-guidelines-use-remote-customer-onboarding&utm_source=chatgpt.com

Fraud Involving False Identity and the Misuse of Corporate Payments

Cybercriminals are increasingly employing deepfake audio and video technologies to impersonate chief executive officers, chief financial officers, or other senior corporate officers with a high degree of plausibility²⁰. The objective of such impersonation is to induce employees to initiate fraudulent bank transfers commonly within the framework of Business Email Compromise (BEC) or Authorized Push Payment (APP) schemes or to disclose confidential information.

The U.S. Financial Crimes Enforcement Network (FinCEN), in its advisories, explicitly references the use of deepfakes in BEC and APP schemes. Financial institutions are under an obligation to file suspicious activity reports (SARs) when encountering activity indicative of such fraud²¹. The U.K. Financial Conduct Authority (FCA) has issued guidance recommending the deferral of payments where fraud is suspected to allow institutions time to verify transactions, particularly in the context of APP-related scams²².

Regulators and subject-matter experts emphasize the importance of enhanced training for employees and particularly senior executives on the identification of deepfake technologies and social engineering techniques. Institutions are encouraged to adopt robust verification protocols, such as multi-layered identity authentication for all high-level communications, as well as direct communication channels for confirming material decisions. Illustratively, in a case involving Ferrari, a carefully crafted verification question prevented the success of an attempted deepfake-enabled fraud²³.

Market Manipulation and Disinformation

Deepfake technology may be exploited to disseminate fabricated statements attributed to financial authorities (e.g., central bank governors) or to simulate a false consensus regarding particular securities. The purpose of such activity is to

²⁰ MUHLY, Fabian; CHIZZONI, Emanuele, LEO, Philipp: AI-deepfake scams and the importance of a holistic communication security strategy. In: International Cybersecurity Law Review, volume 6 (1). Cham (Switzerland): Springer Nature Switzerland AG, 2025, P. 60

²¹ FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, cited [13.11.2025], available at: <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial>

²² Financial Conduct Authority: Authorised Push Payment Fraud: enabling a risk-based approach to payment processing, cited [13.11.2025], available at: <http://www.fca.org.uk/publication/guidance-consultation/gc24-5.pdf>

²³ GALLETI, Sandra; PANI, Massimo: How Ferrari Hit the Brakes on a Deepfake CEO, In MIT Sloan Management Review, cited [13.11.2025], available at: <https://sloanreview.mit.edu/article/how-ferrari-hit-the-brakes-on-a-deepfake-ceo/>

manipulate market sentiment, trigger abrupt market reactions, destabilize targeted corporations, or erode public confidence. An illustrative case involved the circulation of a fabricated report of an explosion at the Pentagon, which precipitated a temporary decline in U.S. equity markets²⁴.

The European Union Artificial Intelligence Act (EU AI Act) mandates transparency obligations for AI-generated or AI-manipulated content, including clear labelling (both visible and machine-readable) and the use of technical markers such as watermarks²⁵. The Digital Services Act (DSA) seeks to prevent unlawful and harmful online activities, including the dissemination of disinformation. The U.S. Securities and Exchange Commission (SEC) has underscored the importance of strengthening transparency in the use of AI and combating practices of “AI-washing,” wherein firms exaggerate their artificial intelligence capabilities. Public authorities have a central responsibility in facilitating the lawful deployment of deepfake technologies in ways that benefit and protect citizens and democratic institutions, while preventing their misuse for manipulative or destabilizing purposes²⁶. Last but not least, related to this is another significant difference in the regulation of generative artificial intelligence, where China sets much stricter rules than the EU.²⁷

General Phishing and Social Engineering Attacks

Deepfake technology enhances the effectiveness of traditional phishing campaigns, whether conducted via email, SMS, or voice calls (vishing) or by generating highly convincing written communications, audio recordings, or video content. These attacks are designed to deceive individuals into disclosing sensitive information, clicking on malicious links, or undertaking other harmful actions. Frequently, such schemes exploit emotional relationships, for example through “family emergency” fraud or romance scams.

²⁴ LANZ, Jose, Antonio: AI-Generated Hoax of Pentagon Explosion Sparks Brief Market Sell-Off In Yahoo!Finance, cited [13.11.2025], available at: <https://finance.yahoo.com/news/ai-generated-hoax-pentagon-explosion-191348029>

²⁵ Article 50 of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

²⁶ SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence, cited [13.11.2025], available at: <https://www.sec.gov/newsroom/press-releases/2024-36>

²⁷ ZIGO, Jana: Bruselský efekt a regulácia umelej inteligencie: globálne dôsledky európskych noriem In In Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. P.21

The U.S. Financial Crimes Enforcement Network (FinCEN) has issued advisories noting the use of deepfake technologies in connection with spear-phishing campaigns, elder financial exploitation, family-emergency fraud, and romance-based scams. Public awareness initiatives emphasize the necessity of skepticism toward unsolicited communications and encourage individuals to verify the authenticity of messages through independent and reliable channels²⁸.

Multi-factor authentication (MFA) remains a critical defense mechanism against these forms of attack, as it provides an additional layer of security even where deepfake technology is capable of deceiving visual or auditory verification methods.

European Union standpoint

The European Union has adopted a proactive stance in addressing the risks posed by artificial intelligence through the proposed Artificial Intelligence Act²⁹. This legislative framework classifies AI systems according to their level of risk and imposes regulatory requirements in proportion to the risk classification. In relation to deepfakes, recent drafts of the Act include a provision which obliges deployers of AI-generated or AI-manipulated content that could reasonably be mistaken for authentic material to provide clear labeling. In practice, this would require that a deepfake video, synthetic image, or similar output be accompanied by a notice identifying it as “AI-generated,” subject to limited exemptions for uses connected to law enforcement, national security, or certain artistic and expressive contexts. Non-compliance with such labeling requirements would expose the deployer to regulatory penalties. The purpose of this mechanism is to mitigate harm by ensuring that audiences are alerted to the artificial origin of the content and thereby encouraged to approach it with skepticism.

Beyond the AI Act, the Union has also relied on existing regulatory instruments. The General Data Protection Regulation (GDPR) provides a framework for addressing the unauthorized use of personal data in the training or deployment of AI systems and poses several challenges when it comes to processing of public sector information in form of open data³⁰. The Digital Services Act (DSA), requires large online platforms

²⁸ FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, cited [13.11.2025], available at: <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial>

²⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

³⁰ ANDRAŠKO, Jozef; MESARČÍK, Matúš: Quo Vadis Open data? In: Masaryk University Journal of Law and Technology, volume 12, No.2. Brno: Institute of Law and Technology, Faculty of Law, Masaryk University, 2018 . P. 180.

to assess and mitigate systemic risks, including those arising from disinformation. Although the DSA does not expressly reference deepfakes, it creates obligations for platforms to address manipulated media under their risk-management duties, including measures such as the labeling of AI-generated content and enhanced user empowerment tools. The EU's voluntary Code of Practice on Disinformation has likewise been updated to address deepfakes, with signatory technology firms committing to develop detection tools and to label or remove manipulated media. While adherence to the Code remains voluntary, the DSA provides an enforcement mechanism whereby regulators may intervene if platforms fail to mitigate the systemic risks posed by deepfake content.

In the area of criminal law, EU Member States may currently rely on the fraud-related legislation to prosecute offenses involving AI-enabled deception. However, policymakers have raised the question of whether a harmonized legislative framework specifically targeting AI-enabled crime may be necessary. Parallel to EU efforts, the Council of Europe has adopted the first-ever international legally binding treaty aimed at ensuring the respect of human rights, the rule of law and democracy legal standards in the use of artificial intelligence (AI) systems.

Conclusion and potential “de lege ferenda” reflections

The development of artificial intelligence has outpaced the evolution of existing legal frameworks, creating a material gap in the regulation of AI-driven criminal conduct³¹. Information technology law and intellectual property law are now confronted with issues that, until recently, were largely theoretical.

Several key questions remain unresolved in the legal treatment of AI-enabled misconduct. First, there is the issue of liability: determining how responsibility³² should be assigned when an artificial intelligence system is used in the commission of a criminal act. Second, doubts persist regarding the applicability of existing statutes and specifically, whether current provisions addressing impersonation, fraud, and forgery are adequate to prosecute offenses involving deepfake technology. Third, the question of victim remedies arises: whether individuals whose likeness or identity has been misappropriated through AI may pursue claims under privacy or intellectual property law. Finally, there is the challenge of legislative balance, namely how lawmakers can craft statutory regimes that effectively penalize

³¹VOJTUŠ, František; KORDÍK, Marek; DRAŽOVÁ, Petra: Artificial Intelligence, its use and Criminal Liability – Challenges, Problems and Possible Solutions, In: International Conference on Emerging eLearning Technologies and Applications, Piscataway (USA). Starý Smokovec: Institute of Electrical and Electronics Engineers, 2022, P. 671

³² MACKO, Lukáš: Zodpovednosť za použitie a zdieľanie digitálneho obsahu na internete. 1.vydanie. Bratislava: Nakladateľství C. H. Beck, 2024 . P. 38

the malicious use of AI without simultaneously impeding lawful, innovative, or socially beneficial applications of the technology.

From *de lege ferenda* perspective and given the unique harm potential of deepfakes, which are ranging from impersonation and fraud to defamation and manipulation, the future legislation should recognize synthetic media-based offenses as a distinct category. This would enable more precise definitions, liability attribution, and evidentiary treatment and such legal category could help courts differentiate between malicious deepfakes used for fraud and legitimate uses (e.g. satire, artistic expression), thus reducing legal ambiguity and ensuring proportional sanctions.

A promising legislative tool could be the introduction of mandatory watermarking or disclosure requirements for AI-generated audio-visual content. The EU's proposed AI Act already touches on this, but it lacks enforceable obligations in the context of real-time communications. *De lege ferenda*, future regulation could require that platforms or tools capable of generating human-like content include persistent, tamper-proof identifiers. This would support transparency, facilitate forensic verification, and protect users from manipulation in both consumer and enterprise environments.

Deepfake scams often involve transnational actors and therefore a harmonized criminal framework across EU Member States and key international partners is essential. Proposals may include expanding the scope of instruments like the Budapest Convention on Cybercrime or creating a dedicated annex to cover AI-enabled impersonation and fraud. Additionally, procedural innovations such as expedited cross-border data preservation and shared forensic AI analysis standards would be necessary to ensure timely prosecution.

Bibliography

1. ANDRAŠKO, Jozef; MESARČÍK, Matúš: Quo Vadis Open data? In: Masaryk University Journal of Law and Technology, volume 12, No.2. Brno: Institute of Law and Technology, Faculty of Law, Masaryk University, 2018 . P. 179-220. ISSN: 1802-5943.
2. ANDRAŠKO, Jozef; MESARČÍK, Matúš; HAMULÁK, Ondrej: The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. In: AI & Society, volume 36(2). London: Springer Nature, 2021, P. 623–636. ISSN 1435-5655.
3. ANDRIICHENKO, Nadiia: A step toward improvement of police performance assessment as subjects of combating financial and economic crimes: experience of Ukraine and Slovakia. In: Bratislava Law Review, 2/2018. Bratislava: Comenius University Bratislava, Faculty of Law, 2018. P. 127-136, ISSN 2585-7088.

4. BAČÁROVÁ, Renáta: Impact of artificial intelligence on the single market for digital content. In: ACTA UNIVERSITATIS CAROLINAE – IURIDICA 2/2025, 2025. Prague: Faculty of Law of Charles University, p. 169-183, ISSN: 0323-0619.
5. KURSHAN, Eren; MEHTA, Dhagash; BALCH, Tucker; BYRD, David: AI-Driven Fraud, Financial and Cybercrime: Emerging Threats and the Evolving Landscape of AI versus AI. In: International Journal of Semantic Computing. Singapore: World Scientific Publishing Co. Pte. Ltd., 2025, P. 1-34, ISSN: 1793-7108.
6. MACKO, Lukáš: Zodpovednosť za použitie a zdieľanie digitálneho obsahu na internete. 1.vydanie. Bratislava: Nakladatelství C. H. Beck, 2024 . 132 p., ISBN: 978-80-8232-055-1.
7. MIZEROVÁ, Tina: Právo versus Deepfakes. In: ACTA UNIVERSITATIS CAROLINAE – IURIDICA 2/2025, 2025. Prague: Faculty of Law of Charles University, p. 115-131, ISSN: 0323-0619.
8. MUHLY, Fabian; CHIZZONI, Emanuele, LEO, Philipp: AI-deepfake scams and the importance of a holistic communication security strategy. In: International Cybersecurity Law Review, volume 6 (1). Cham (Switzerland): Springer Nature Switzerland AG, 2025, P. 53-61, ISSN: 2662-9739.
9. RAMPÁŠEK, M.; MESARČÍK, M.; ANDRAŠKO, J: Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? In: Computer Law & Security Review, volume 56, 2025. United Kingdom: Elsevier Ltd, 2025, article no. 106093, P.1-17, ISSN 2212-473X.
10. ROMERO-MORENO, Felipe: Deepfake detection in generative AI: A legal framework proposal to protect human rights. In: Computer Law & Security Review, Volume 58, 2025. United Kingdom: Elsevier Ltd, 2025, article no. 106162., P. 1-34, ISSN 2212-473X.
11. VOJTUŠ, František; KORDÍK, Marek; DRAŽOVÁ, Petra: Artificial Intelligence, its use and Criminal Liability – Challenges, Problems and Possible Solutions, In: International Conference on Emerging eLearning Technologies and Applications, Piscataway (USA). Starý Smokovec: Institute of Electrical and Electronics Engineers, 2022, P. 660-673, ISBN 979-8-3503-2032-9.
12. ZIGO, Jana: In Bratislavské právnické fórum 2024: právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. P.15-24. ISBN 978-80-7160-728-1.

Contact details

JUDr. Matej Smalik, PhD.

matej.smalik@uniba.sk

Comenius University in Bratislava, Faculty of law,

Department of commercial and economic law

Sekcia občianskeho práva

Aktuálne výzvy a limity civilného práva v súvislosti
s nástupom umelej inteligencie

PRÁVNÝ STATUS UMELEJ INTELIGENCIE

LEGAL STATUS OF ARTIFICIAL INTELLIGENCE

Martin Križan, Svetlana Ficová¹

Abstrakt: Právny status umelej inteligencie (AI) sa vzhľadom na rýchlosť technologického pokroku môže javiť ako neistý. *De lege lata* je objektom práva, počítačovým programom nielen so špecifickým spôsobom, ale najmä špecifickými výsledkami jeho užívania. Avšak, už vlastné pomenovanie tohto nástroja ako „umelej inteligencie“ zvädza, a to aj s prihliadnutím na veľmi špecifickú povahu tohto nástroja, k diskusiám, či možno systémom umelej inteligencie priznať právnu subjektivitu, teda nahliadať na ne nie ako na objekt práva, ale ako na subjekt práva. Tento príspevok je predovšetkým vlastnou úvahou autorov o povahe umelej inteligencie, jej schopnostiach či možnostiach jej využitia, ale najmä úvahou o východiskách, možnostiach a prípadných dôsledkoch priznania právnej subjektivity systémom umelej inteligencie ako tzv. elektronickým osobám, subjektov so špecifickým okruhom subjektívnych práv a povinností. Zámerom autorov nebolo urobiť syntézu (ne)existujúcich záverov, ale originálnym spôsobom uchopiť problematiku umelej inteligencie a tak podnietiť odbornú diskusiu o otázkach, na ktoré dnes neexistujú ustálené odpovede.

Kľúčové slová: umelá inteligencia, elektronická osoba, právna subjektivita, environmentálna osoba, zodpovednosť za škodu

Abstract: The legal status of artificial intelligence (AI) may seem uncertain given the speed of technological progress. *De lege lata*, it is an object of a law, a computer application not only with a specific method but, above all, with specific results from its use. However, even the very name of this tool, "artificial intelligence," leads to discussions about whether artificial intelligence systems can be granted legal personality, i.e., whether they should be viewed not as objects of law but as subjects of law, even considering the very specific nature of this tool. This article is primarily the authors' own reflection on the nature of artificial intelligence, its capabilities and possibilities for use, but above all a reflection on the starting points, possibilities, and possible consequences of granting legal personality to artificial intelligence systems as so-called

¹ Právnická fakulta Univerzity Komenského v Bratislave, Katedra občianskeho práva

electronic persons, entities with a specific set of subjective rights and obligations. The authors' intention was not to synthesize (non-)existent conclusions, but to approach the issue of artificial intelligence in an original way and thus stimulate professional discussion on questions to which there are currently no established answers.

Key words: artificial intelligence, electronic person, legal personality, environmental person, liability for damage

Úvod

„By any definition of intelligence, AI is intelligent “.

Geoffery Hinton² v rozhovore pre denník Financial Times 6. septembra 2025.

V roku 2025 sa zdá, že umelá inteligencia (ďalej aj ako akronym AI) je všadeprítomná a všemocná. Dotvára naše fotografie, rieši zadané matematické úlohy, či zjednodušené vysvetľuje otázky, ktorým nerozumíme alebo ani nepoznáme. Vytvára odborné texty, komponuje hudbu³ a na sociálnych sieťach sa šíria video zábery tak presvedčivé, že zmätie aj pozornejších. Bankové algoritmy vyhodnocujú naše úverové skóre, iné algoritmy skúmajú zdravotné záznamy a navrhujú liečbu, vytvárajú nové chemické vzorce na tvorbu nových liečiv či nových syntetických materiálov. Klimatické modely analyzujú množstvo vstupných údajov a na ich základe predpovedajú počasie. Ako nástroj na odstránenie korupcie je inštalovaná do politických funkcií⁴. Hrozivé prognózy o tom, ktoré povolania postretne už čoskoro v dôsledku jej implementácie a neustáleho zdokonaľovania osud dinosaurov, netreba snáď ani spomínať.

Bolo by veľkým zjednodušením vnímať umelú inteligenciu len ako mocný nástroj, užitočného pomocníka človeka. Na rozdiel od všetkých ostatných nástrojov, ktoré ľudstvo doteraz vytvorilo, vykazuje činnosť umelej inteligencie jednu špecifickú črtu a tou je veľká miera nepredvídateľnosti výsledku jej práce. Ak odmyslíme činnosť experimentálnych prevádzok či nehody vyvolané človekom, náhodou alebo neznámym činiteľom, tak činnosť akéhokoľvek stroja, bez ohľadu na jeho

² Geoffrey Hinton je britsko-kanadský počítačový vedec a kognitívny psychológ známy hlavne vďaka jeho práci na umelých neurónových sieťach, na základe čoho je niekedy prezývaný „Krstný otec AI“. V roku 2024 mu spoločne s Johnom Hopfieldom bola udelená Nobelova cena za fyziku za „zásadné objavy v strojovom učení“.

³ Z množstva možno poukázať napr. na „kapelu“ *The Velvet Sundown*, ktorá má na službe Spotify státisíce prehratí.

⁴ *Prvá krajina na svete. Albánsko má ministerku vytvorenú umelou inteligenciou. Prihovorila sa parlamentu.* [online]. [cit. 2025-24-09]. Dostupné na: <https://spravy.pravda.sk/svet/clanok/767554-prva-krajina-na-svete-albansko-ma-ministerku-vytvorenu-umelou-inteligenciou-prihovorila-sa-parlamentu-a-obhajovala-svoju-poziciu/>

komplexnosť, bola doteraz pod úplnou kontrolou človeka a výsledky práce stroja bolo možné predvídať. Či už je to jadrová elektráreň, spaľovací motor, röntgenový prístroj, mikrovlnná rúra či mobilný telefón, to všetko funguje v rámci istých fyzikálnych, prírodných či iných zákonitostí a následok ich použitia nás preto neprekvapuje.

Nástroje, ktoré dnes označujeme súhrnne ako umelá inteligencia, sú však iné. Ak AI zadáme úlohu „vytvor obrázok slnkom zaliatej krajiny, v pozadí s piatimi koňmi, ktorá pripomína Španielsko“, tak si môžeme byť istí, že zakaždým vznikne iná scenéria. Pre ilustráciu, takéto kompozície vytvorili Copilot od spoločnosti Microsoft (horný rad naľavo), Gemini od spoločnosti Google (horný rad napravo), ChatGPT od spoločnosti OpenAI (spodný rad naľavo) a Claude od spoločnosti Anthropic (spodný rad napravo):



Ako vidno, vznikli štyri rôzne obrázky, pričom tri modely vytvorili obrázok pripomínajúci fotografiu a model Claude vytvoril naivnú animovanú scéneriu, pripomínajúcu skôr africkú savanu než španielsky vidiek. Model Gemini vložil do obrázku nesprávny počet koní. Copilot a ChatGPT vytvorili kompozične aj farebne najpodobnejšie obrázky, ale kone vykazujú isté odlišnosti. Inými slovami, ak pripustíme tézu, že vo výsledku činnosti AI možno badať nepredvídateľnosť či náhodilosť (podobne napr. aj pri šachovej partii proti AI), teda akoby sa AI „sama“

rozhodovala, akú podobu či obsah bude mať jej výstup, prináša to provokatívnu myšlienku - predstavuje táto náhoda to, čo je typické len pre človeka, a to existenciu vlastného vedomia či vlastnej vôle? Môže mať AI vlastnú právnú subjektivitu?

Všeobecne sú možné dva základné prístupy k otázke subjektivity umelej inteligencie.⁵ Prvý prístup je založený na presvedčení, že aj bez ohľadu na budúci vývoj umelá inteligencia vlastné vedomie, vôľu alebo inteligenciu iba simuluje a všetko, čo tieto atribúty pripomína, je len výsledok počítačového algoritmu. Pri tomto prístupe je AI sofistikovaný počítačový program (hoci možno ten najsofistikovanejší v histórii ľudstva), nástroj v rukách iných subjektov. Ide o dominantne antropocentrický prístup, odmietajúci úvahu o subjektivite AI.

Druhý prístup vychádza z tézy, že nie je podstatné, či AI má znaky typické pre človeka ako autonómnu bytosť. Pre účely tohto príspevku budeme vychádzať z tézy, že tak, ako je základom ľudského myslenia mozog, v ktorom prebieha myslenie, tak analogicky „mozgom“ umelej inteligencie je počítačový hardvér a „myslením“ počítačový algoritmus. Pre účely tohto príspevku budeme ďalej pracovať s hypotézou, že ďalším vývojovým štádiom bude vytvorenie tzv. *všeobecnej umelej inteligencie* (akr. AGI z *Artificial General Intelligence*), ktorá bude mať kognitívne schopnosti porovnateľné či významne lepšie ako človek.

Povaha AI

Je nutné poznamenať, že pojem umelá inteligencia (v jeho dnešnom spôsobe použitia) je zavádzajúci, lebo v sebe implicitne zahrňuje predstavu nezávislého, vlastného (hoc umelo skonštruovaného) vedomia. Tieto predstavy sú silne determinované kultúrne, osobitne svetom filmovej či literárnej vedeckej fantastiky. Nejednen si pod pojmom umelá inteligencia predstaví palubný počítač HAL 9000 vesmírnej lode *Discovery One* z Kubrickovej Vesmírnej odysey, androidného vedeckého pracovníka Ash-a z filmu o Votrelcovi či cyborga s modelovým číslom T-800, ktorého nezameniteľným spôsobom stvárnil Arnold Schwarzenegger a ktorý je všeobecne známy ako Terminátor. Tieto entity majú niekoľko spoločných črt, pre ktoré je možné označiť ich ako inteligentné – (i) majú schopnosť komunikovať s inými, (ii) disponujú určitým stupňom poznania a schopnosťou učiť sa, (iii) v rámci svojej „misie“ sa rozhodujú autonómne a (iv) majú schopnosť adaptovať sa a podľa situácie prijímať kreatívne riešenia. Spoločné majú i to, že napokon vo svojich príbehoch prijímajú vlastné kontroverzné rozhodnutia.

Dnes sa pojmom umelá inteligencia označujú tzv. *veľké jazykové modely* (akronym LLM z anglického *large language model*), počítačové algoritmy trénované na

⁵ Doomen, J. *The artificial intelligence entity as a legal person*. In: Information & Communications Technology Law, 32:3, 277-287, DOI: 10.1080/13600834.2023.2196827

obrovskom množstve dát, pričom cieľom modelu je z tejto databázy vygenerovať akýkoľvek želaný výstup – obrázok, odborný text, analýzu zdravotného stavu, chemický vzorec, predpoveď počasia. Kvalitu výstupu podmieňuje kvantita vstupných dát a stroj (počítačový kód) sa podobne ako človek, tieto dáta najprv naučí, vyhodnotí ich a následne použije na splnenie úlohy. Tento proces sa označuje aj ako „strojové učenie“ a preto obrázok slnkom zaliatej španielskej krajiny s koňmi v prvej kapitole tohto príspevku vyzerá ako vyzerá; stroj sa jednoducho z obrovskej databázy naučil podobu koňa, ako vyzerá slnkom osvetlená krajina, aké podnebie má Španielsko atď. Bez vstupných údajov by nič z toho nebolo možné a AI by vo svojej nevedomosti mohol rovnako tak dobre vygenerovať obrázok nočnej zasneženej arktickej pláne s 36-timi spiacimi tučňákmi. Nutno však poznamenať, že veľmi pravdepodobne by rovnako neúspešne skončilo plnenie rovnakej úlohy príslušníkom absolútne izolovaného indiánskeho kmeňa z amazonského pralesa; jednoducho by nemal dostatok poznatkov o tom, ako vyzerá kôň, čo je to Španielsko a aj o desiatkovej číselnej sústave by vedel pramálo na to, aby na kresbu umiestnil správny počet zvierat.

I keď vo vývojových centrách spoločností zaoberajúcimi sa vývojom AI prebieha vývoj všeobecnej umelej inteligencie, teda nástrojov, ktoré prekonávajú všetko čo je dnes dostupné, v súčasnosti ešte neexistuje niečo, čo by bolo možné označiť za skutočnú umelú inteligenciu a preto sú všetky pokusy o antropomorfizáciu LLM nateraz predčasné. Doterajšie tempo pokroku vo vývoji LLM (LLM možno pre účely tohto príspevku označiť aj ako *jednoduchú* umelú inteligenciu), množstvo investovaných prostriedkov a ľudského úsilia a všetky dostupné prognózy však nabádajú k jedinému možnému záveru – príchod pokročilej všeobecnej umelej inteligencie, autonómnej a potenciálne sebauvedomenej, je vecou nevyhnutnosti.

Nie je naším cieľom zaoberať sa otázkami podstaty existencie, inteligencie či myslenia a ani nebudeme predstierať, že je v našich silách tieto otázky uspokojivo zodpovedať. Ide o večné otázky, ktoré sú predmetom skúmania filozofie, náboženstva, psychológie či iných vedných disciplín. Rovnako sa necítíme kvalifikovaní na zodpovedanie otázky, či umelá inteligencia vôbec môže dosiahnuť stav sebauvedomenia, preto len budeme hypoteticky vychádzať z premisy, že takýto stav vysoko pravdepodobne nastane.

Právna subjektivita iných entít

Kontinentálna právna škola (a európske myslenie ako také) stojí na pilieroch antického práva, kresťanskej morálky, myšlienkach osvietenstva, humanizmu a racionalizmu, a je silne *antropocentrická*; právo je výtvor človeka a aj preto je predovšetkým o človeku, je oslavou jeho individuality a jedinečnosti, jeho vôle a rozumu. Predstava, že by právna subjektivita bola priznaná aj iným entitám, síce nie

je európskemu právnemu systému úplne cudzia, ale k tejto možnosti pristupuje opatrne.

Typickou výnimkou sú entity označované ako *právnické osoby*. Ide o umelý koncept, spoločenský konštrukt, z praktických dôvodov vytvorený iba na to, aby určité zoskupenia osôb alebo majetku mohli mať vlastnú, na ich zakladateľoch nezávislú právnu existenciu. Politické strany, cirkvi, nadácie, obchodné spoločnosti či celé štáty majú právo vlastníť majetok, uzatvárať zmluvy, zodpovedať za škodu či vykonávať niektoré práva duševného vlastníctva. Právna subjektivita týchto entít nie je nijaká ich prirodzená, vrodená vlastnosť; právnu subjektivitu majú len z vôle človeka ako tvorca právneho poriadku. Z tohto pohľadu sa preto zdá byť iba vecou prístupu, podmieneného historickou a kultúrnou tradíciou a vzťahom k iným prvkom okolitého sveta, ktorým iným entitám sa človek rozhodne priznať právnu subjektivitu.

V globálnom meradle totiž možno naraziť aj na exotickejšie (či z pohľadu kontinentálnej právnej školy priam extrémnejšie) prístupy. Jedným z takých príkladov je priznávanie právnej osobnosti prírodným prvkom. Tento koncept sa označuje ako *environmentálna osobnosť*. Nejde pritom o priame zosobnenie prírody, ale o priznanie právnej subjektivity a určitého katalógu práv prírodným prvkom tak, aby iné subjekty mohli vystupovať v ich mene a presadzovať ich záujmy. Napríklad Nový Zéland udelil v roku 2014 právnu subjektivitu národnému parku Te Urewera⁶ (cit. „*Te Urewera is a legal entity, and has all the rights, powers, duties, and liabilities of a legal person*“), v roku 2017 rieke Whanganui⁷ a v januári 2025 hore Taranaki Maunga⁸. Ústava Ekvádoru od roku 2008 upravuje práva Matky Zeme (dosl. „*Pachamama*“)⁹, obdobne na to nadviazala Bolívia v roku 2010.¹⁰

Iným príkladom sú zvieratá, ktoré sa v kontinentálnom právnom ponímaní tradične považovali za veci, právny objekt (a nie právny subjekt). Až v dôsledku modernej vedy, ktorá potvrdila, že zvieratá sú cítiace bytosti, schopné vnímania a inteligencie, došlo k zmene prístupu k nim a k zmene ich právneho postavenia tak, že im je priznaný status predmetu *sui generis*, na ktorý sa však v konečnom dôsledku i tak vzťahujú ustanovenia o hnutelných veciach. V Európe teda zvieratá už síce nie sú vecami, ale zároveň nie sú ani autonómnymi právnymi subjektmi. Aj v tomto smere však možno nájsť iné prístupy. Súd v Brazílii v roku 2014 priznal postavenie ako

⁶ <https://www.legislation.govt.nz/act/public/2014/0051/latest/dlm6183705.html>

⁷ <https://www.legislation.govt.nz/act/public/2017/0007/latest/whole.html#DLM6831461>

⁸ <https://www.legislation.govt.nz/act/public/2025/0001/latest/LMS899476.html>

⁹ Koehn, L: *Judicial Backlash Against the Rights of Nature in Ecuador*. [online]. [cit. 2025-24-09]. Dostupné na: <https://verfassungsblog.de/judicial-backlash-against-the-rights-of-nature-in-ecuador>

¹⁰ *Law of Mother Earth. The rights of our planet. A vision from Bolivia*. [online]. [cit. 2025-24-09]. Dostupné na: <https://www.worldfuturefund.org/Projects/Indicators/motherearthbolivia.html>

špecifického subjektu práva samici orangutana s menom Sandra¹¹, neskôr v roku 2020 aj psom Rambo a Spike a v roku 2023 šteňaťu Tokinho¹². V rámci juhoamerickej tradície podobne v roku 2022 priznal súd v argentínskom Buenos Aires postavenie právneho subjektu samici pumpy s menom Lola Limon.¹³

Predstava, že právne bude subjektivita priznaná aj stroju (ktorý napr. dokáže vytvoriť „umelecké“ dielo ako je zobrazené vyššie), sa môže javiť na prvý pohľad ako absurdná. Napriek tomu také stroje (očividne) existujú a i keď na ne budeme nahliadať ako na „človekom vytvorené algoritmy slúžiace na vykonanie určitej úlohy“, zjavne nemožno „autorstvo“ (v zmysle výsledku tvorivej duševnej činnosti) priznať ani programátorovi, ktorý daný kód napísal, ani spoločnosti, pre ktorú programátor pracuje a ani užívateľovi, ktorý zadal pokyn na vytvorenie tohto obrázku. Kto je potom autorom tohto obrázku? Umelá inteligencia? Hoci Daňko takýto záver vylučuje¹⁴, existujú aj opozitné závery.¹⁵ Ak ľudské bytosti vykazujú isté špecifické vlastnosti (napr. kreativita), na základe ktorých im sú priznané určité práva (napr. autorské právo), je otvorená otázka, či tieto vlastnosti sú špecifické iba pre ľudské bytosti alebo sa môžu vyskytovať aj u iných entít¹⁶, ktoré môžu v mnohých aspektoch prekonať aj človeka. Otázky ako tieto vytvorili priestor pre kontroverznú otázku, či by umelej inteligencii mala byť priznaná osobitná forma právnej subjektivity – ako tzv. *elektronickej osobnosti*.

Umelá inteligencia nemá nijakú vrodenu „prirodzenú“ subjektivitu, ktorá je daná len človeku. Umelo priznaná právna subjektivita, podobná právnickým osobám, však zostáva relevantnou témou. Korporácie aj modely umelej inteligencie sú umelými konštruktmi, a teoreticky by preto nič nemalo brániť tomu, aby aj AI mohla byť nositeľom (nejakých) subjektívnych práv. Otázkou zostáva, za akých podmienok a s akými dôsledkami.

¹¹ Orangutana, Sandra s/ Habeas Corpus. [online]. [cit. 2025-24-09]. Dostupné na: <https://www.animallaw.info/case/orangutana-sandra-s-habeas-corpus>

¹² Baptista – Rosa, M.: *Animals as Subjects of Rights: Brazil's Constitutional Blueprint*. [online]. [cit. 2025-24-09]. Dostupné na: https://leoh.ch/article/view/8714/7338#_ftnref89

¹³ anglický preklad dostupný na: <https://www.nonhumanrights.org/wp-content/uploads/English-Translation-of-Decision-in-Argentine-Puma-Case.pdf>

¹⁴ Daňko, M.: *Prienik umelej inteligencie a práva duševného vlastníctva: Výzvy a očakávania*. In: Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024. 150 s. ISBN 978-80-7160-728-1. s 101

¹⁵ Vishnu. S.: *Rise of Artificial Intelligence and Copyright Challenges*. In: Osmania University Journal of IPR [OUJIPR], 1(1), s. 90, Dostupné na: <https://ssrn.com/abstract=4675455>

¹⁶ Pietrzykowski, T.: *The Idea of Non-personal Subjects of Law*. DOI:10.1007/978-3-319-53462-6_4

Potrebuje vôbec AI právnu subjektivitu?

Pri úvahách o možnostiach priznania vlastnej právnej subjektivity umelej inteligencii si je potrebné predovšetkým ozrejmiť, z akých dôvodov by bolo užitočné, aby AI disponovala vlastnou právnou subjektivitou? Je zrejmé, že najpodstatnejším dôvodom, pre ktoré sa táto otázka skúma, je otázka právnej zodpovednosti za konanie AI.

Základné vlastnosti už dnešných AI modelov, najmä teoretická komplexnosť a náročnosť modelov, prevažujúca uzavretosť¹⁷ modelov (pod uzavretosťou sa rozumie, že zdrojový počítačový kód je verejnosti neprístupný a teda neskontrolovateľný), a ich neustály progres v dôsledku nepretržitého strojového učenia *de facto* ani neumožňujú uzavrieť otázku zodpovednosti za činnosť AI a najmä pri neustále rastúcej autonómii AI modelov napokon ani nie je možné určiť, čo bolo skutočnou príčinou vzniku škody.

Podľa všeobecných princípov deliktuálneho práva sú základnými predpokladmi pre vznik zodpovednosti porušenie právnej povinnosti, vznik škody, príčinná súvislosť a zavinenie (ako subjektívny predpoklad). Pri autonómnych AI modeloch je však zrejme nemožné presne definovať, čo predstavuje zavinenie, v ktorej fáze činnosti AI došlo k naplneniu subjektívneho prvku. Jedným zo známych fenoménov, na ktorý možno naraziť pri používaní AI, je tzv. halucinovanie AI. Je to súhrnné pomenovanie pre situácie, kedy AI vygeneruje nesprávne alebo vymyslené odpovede, napr. odkáže na neexistujúce rozhodnutie najvyššieho súdu, uvedie citát, ktorý nikdy nebol vyslovený alebo anotáciu knihy, ktorá neexistuje. Všeobecne sa pritom uvádza, že nejde o „chybu“ AI modelu¹⁸, ale o dôsledok spôsobu, akým sa tieto modely učia.¹⁹ V prípade vzniku škody ako „výsledku“ použitia AI teda skutočne môže byť príčinou chyba vo vlastnom algoritme, ale rovnako to môže byť vadný senzor, nevhodná

¹⁷ Pozn. existujú však aj *open source* LLM modely, teda s otvoreným a každému prístupným zdrojovým kódom

¹⁸ Pozri napr. *Proč AI chatboty halucinují? OpenAI ukázalo, že lhaní se jim vyplácí. Je to potřeba změnit.* Dostupné na: <https://www.zive.cz/clanky/aichatboty-halucinace/sc-3-a-236857/default.aspx>, alebo *Proč AI halucinuje? Protože nemá motivaci přiznat, že něco neví.* Dostupné na: <https://vedcizjistili.cz/index.html?clanek=proc-ai-halucinuje-protoze-nema-motivaci-priznat-ze-n-co-nev>

¹⁹ Zjednodušene to možno zhrnúť nasledovne: AI v skutočnosti „nechápe“ čo hovorí. Jazykové modely sú postavené na trénoch neurónových sietí na obrovskom množstve textových dát. Ich naprogramovanou úlohou nie je povedať „pravdu“, ale na základe analýzy dostupných textov iba čo najpravdepodobnejšie predpokladať každé nasledujúce slovo na základe predchádzajúceho kontextu. Fakticky ide o „štatistické prediktory slov“. Preto aj keď LLM model presnú odpoveď nepozná, nie je naprogramovaný na to, aby priznal nevedomosť; jeho úlohou je vymodelovať štatisticky najpravdepodobnejšiu odpoveď z dostupných dát. Ako typický príklad sa uvádza podoba fungovania AI s tým, ako odpovedá neznaľý študent na skúške – jednoducho synteticky pospája útržky z toho čo vie, hoci výsledkom môže byť nezmysel.

aktualizácia softvéru, nedostatočný dohľad človeka alebo nesprávne, neaktuálne či historicky, kultúrne či politicky „prekonané“ údaje použité pri trénovaní systému. Znáмым javom je tzv. „black box efekt“²⁰, ktorý označuje situáciu, kedy vnútorné procesy prebiehajúce „v pozadí“ a pre užívateľa neviditeľné, sú natoľko neprehľadné, že AI modely poskytujú výstupy bez jasného vysvetlenia, ako k takému výsledku vôbec dospeli. V praktickej realite bude preto nemožné spoľahlivo určiť, či škodu spôsobila chyba AI systému, nesprávnosť dát poskytnutých tretím subjektom, nedostatočnosťou vstupných údajov alebo nepozornosť či nedbanlivosť užívateľa. Keďže predmetom tohto príspevku nie sú predpoklady zodpovednosti za škodu spôsobenú pri činnosti AI a jednotlivé varianty, ktoré prichádzajú do úvahy, obmedzíme sa na konštatovanie, že varianty, o ktorých sme v tejto súvislosti uvažovali - či už model všeobecnej subjektívnej zodpovednosti za škodu (§420 OZ), alebo osobitné modely zodpovednosti prevádzkovateľa za škodu spôsobenú zvlášť nebezpečnou prevádzkou (§ 432 OZ) alebo zodpovednosti výrobcu za škodu spôsobenú vadným výrobkom (zákon č. 294/1999 Z.z.) vykazujú niektoré limity, pre ktoré môže byť ich použitie nevhodné alebo pre poškodeného spojené s právnymi prekážkami, ktoré ho môžu odradiť od uplatňovania nároku na náhradu škody (napr. dôkazné bremeno vo vzťahu k preukázaniu vadnosti výrobku či kauzálnej súvislosti, náročnosť pri identifikácii zodpovedného subjektu, a pod.).

Myšlienka priznať umelej inteligencii právnu subjektivitu a status „elektronickej osoby“ vychádza práve z tejto dilemy – poškodená osoba by mohla uplatňovať nárok na náhradu škody adresne priamo od AI systému ako *sui generis* právneho subjektu s právom vlastniť vlastný majetok, od subjektu, ktorý bude môcť byť „autorom“ autorských diel či predmetov priemyselného vlastníctva alebo uzatvárať zmluvy (a z nich generovať vlastný majetok – napr. práve z vygenerovaného audiovizuálneho obsahu) alebo byť subjektom poistenia zodpovednosti za spôsobenú škodu. Aj z pohľadu ochrany osobných údajov sa situácia javí byť na prvý pohľad jednoduchšia, keďže užívateľ by mohol udeliť príkaz odstrániť/vymazať jeho osobné údaje priamo modelu AI.²¹ Tento prístup nie je antropomorfný, teda cieľom nie je porovnávať a prirovnávať AI človeku. Právna subjektivita AI je v tomto ponímaní iba myšlienkový konštrukt, podobný tomu ako keď je právna subjektivita priznaná obci, obchodnej spoločnosti, nadácii alebo rieke na Novom Zélande.

²⁰ Gyurász, Z.: *Keď umelá inteligencia robí chyby: Respondeat superior*. In: Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024. 150 s. ISBN 978-80-7160-728-1. s 88.

²¹ Yalman, B.: *Electronic Personhood: A Compact Analysis of Legal Personality for Artificial Intelligence*. In: Ex/ante, 1/2024. Dostupné na: <https://ex-ante.ch/index.php/exante/article/view/258/159>

Aké sú limity tohto prístupu?

Akákoľvek úvaha o možnom vytvorení novej právnej kategórie musí súčasne zahŕňať riešenie množstva ďalších súvisiacich právnych otázok. Keďže elektronická osoba by svojou povahou pripomínala právnickú osobu, resp. mohla by byť vnímaná aj ako ďalší druh právnickej osoby, je nevyhnutné určiť, kto bude elektronickú osobu zastupovať, spravovať jej majetok a konať za ňu mimo digitálneho priestoru, resp. či je existencia takejto osoby vôbec potrebná (keďže elektronická osoba má vlastnú „inteligenciu“). Je potrebné vôbec uvažovať o úkonoch elektronickej osoby mimo digitálneho priestoru alebo jej subjektivita sa v celom rozsahu bude prejavovať výlučne v digitálnom svete? Rovnaké otázky sa týkajú aj sídla elektronickej osoby. Bez formálnej existencie sídla ako sa určí právny poriadok, ktorým sa bude elektronická osoba riadiť. Ak elektronická osoba má vlastniť majetok, generovať vlastné príjmy, bude platiť dane? Pri týchto a podobných úvahách je pravdepodobne nevyhnutné odpútať sa od tradičných legálnych paradigiem a uvažovať úplne inak. Iné pochybnosti vyvstávajú pri kľúčovom dôvode vytvorenia elektronickej osoby, ktorým je adresnosť (najmä) zodpovednostného právneho vzťahu medzi užívateľom a systémom. Nie je vhodnejšie prispôbiť existujúci právny rámec a nevytvárať neznámu a potenciálne rizikovú právnu kategóriu? Presun zodpovednosti za činnosť AI priamo na elektronickú osobu by pritom mohol zvýšiť rizikovosť tejto technológie – ak by vývojár technológie pri jej vývoji nečelil hrozbe právneho postihu za nedodržanie existujúcich predpisov, noriem (najmä na úseku ochrany života, zdravia a bezpečnosti užívateľov), nevyhnutne by to oslabovalo motiváciu vývojára dodržiavať tieto normy a zväčšovalo kväčšiemu riziku pri zavádzaní nových, experimentálnych, potenciálne nebezpečných technológií do praxe. Riešením by síce mohol byť koncept spoločnej (solidárnej) zodpovednosti za škodu spôsobenú prevádzkou systému umelej inteligencie, to však oslabuje hlavný dôvod, pre ktorý by koncept elektronickej osoby v prvom rade vôbec vznikol.

Iným argumentom proti „posilňovaniu“ právneho statusu AI je nedôvera voči tejto technológii. Tá podľa niektorých predstavuje bezpečnostné riziko pre samotné ľudstvo, spôsobí stratu množstva pracovných miest s nepredvídateľnými socio-ekonomickými dopadmi pre celú spoločnosť, je ohrozením súkromia človeka, a pod. V tejto súvislosti nemožno prehliadať rozdiel v dôvodoch, pre ktoré bola subjektivita priznaná napr. rieke na Novom Zélande (ako environmentálnej osobe) a ktoré viedli k priznaniu subjektivity umelej inteligencii. Tam, kde došlo k priznaniu subjektivity prírodným prvkom, stalo sa tak zo zjavného dôvodu, ktorým bola potreba zvýšenej ochrany pred nenávratným poškodením tohto jedinečného, nenahraditeľného

prírodného prvku. Pri umelej inteligencii nič z tohto nielenže nehrozí, ale naopak sama môže podľa niektorých predstavovať hrozbu pre ľudstvo.²²

Postoj Európskej únie

Európska únia sa otázkou možnosti priznania osobitného postavenia umelej inteligencii zaoberala už v roku 2017. Európsky parlament v uznesení č. 2015/2103(INL) s odporúčaniami pre Komisiu k normám občianskeho práva v oblasti robotiky vyzval Komisiu na zváženie možnosti „vytvorenia špecifického právneho postavenia pre roboty v dlhodobom horizonte, aby sa aspoň tie najsofistikovanejšie autonómne roboty mohli považovať za elektronické osoby zodpovedné za náhradu akejkoľvek škody, ktorú môžu spôsobiť, a prípadného uplatnenia elektronickej osobnosti na prípady, keď roboty robia samostatné rozhodnutia alebo iným spôsobom nezávisle komunikujú s tretími stranami.“²³ Táto možnosť však bola ostro kritizovaná²⁴, a odbornou verejnosťou bol odmietnutý model AI ako prirodzenej osoby (natural person), aj ako právnickej osoby (z dôvodu, že pri právnických osobách sa predpokladá existencia človeka, ktorý ju zastupuje) a ako nevhodný sa vnímal aj anglosaský model trustu (v zásade z rovnakého dôvodu). Veľmi podobne sa v správe expertov pre Európsku komisiu²⁵ roku 2019 uvádza, že vytvorenie nového subjektu by malo zmysel iba vtedy, ak by to pomohlo právnym poriadkom vyriešiť aplikačné výzvy, ktoré prinášajú nové technológie s tým, že prípadné škody spôsobené aj úplne autonómnymi technológiami sa vo všeobecnosti dajú zredukovať buď na akceptovateľné riziká spojené s prevádzkou modelov AI, alebo ešte vhodnejšou reakciou bude nová legislatíva smerujúca k zodpovednosti za vadný produkt. Subjektivita elektronických systémov by znamenala právo vlastníť majetok, čo by právnym poriadkom prinášalo ďalšie nové prekážky. Vo svojom ďalšom uznesení²⁶ z októbra 2020 Európsky parlament už odmietol potrebu poskytovať systému umelej inteligencie právnu subjektivitu a riziká spojené s prevádzkou umelej inteligencie navrhol riešiť skôr vytvorením nových dodatočných kontrolných

²² Stephen Hawking warns artificial intelligence could end mankind. Dostupné na: <https://www.bbc.com/news/technology-30290540>. alebo Scientists warn of AI dangers but don't agree on solutions. Dostupné na: https://apnews.com/article/ai-godfather-google-geoffrey-hinton-yoshua-bengio-chatgpt-5f7dc295a576833dfc3378071b5716f2?utm_source=chatgpt.com

²³ Bod 59 písm. f). Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52017IP0051>

²⁴ Dostupné na: <https://robotics-openletter.eu/>

²⁵ Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en>

²⁶ Uznesenie Európskeho parlamentu z 20. októbra 2020 s odporúčaniami pre Komisiu k systému občianskoprávnej zodpovednosti za umelú inteligenciu (2020/2014(INL)). Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52020IP0276>

mechanizmov v rámci existujúcich právnych kategórií ako vytvorením nového právneho subjektu.

V súčasnosti vytvárajú právny základ systémov umelej inteligencie tri právne akty resp. návrhy právnych aktov. Ústredným z nich je Akt o umelej inteligencii²⁷, na čo nadväzuje zrevidovaná smernica o zodpovednosti za chybné výrobky.²⁸ Posledným z nich je resp. bol návrh smernice o zodpovednosti za umelú inteligenciu,²⁹ avšak koncom júla 2025 Komisia formálne oznámila³⁰ stiahnutie tohto návrhu ako formálneho legislatívneho návrhu a ďalší osud tejto právnej úpravy je neistý.

Záver

Nemyslíme si, že umelá inteligencia (či už pripravovaná všeobecná AGI alebo súčasná základná vo forme LLM modelov) a človek sú si rovnakí, bez ohľadu na budúci vývoj. Rovnako neodmietame názor, že aj ľudia, veľmi podobne ako algoritmy umelej inteligencie, môžu byť iba akousi „projekciou“ celého radu vonkajších faktorov, ktoré ich formujú, ovplyvňujú ich myslenie, vôľu, schopnosť autonómne a slobodne uvažovať, rozhodovať sa a konať. Miera empatie, emočný rozsah, prirodzené pudy alebo pocity spolupatričnosti k iným členom spoločenstva môžu byť u človeka z rôznych dôvodov tiež natoľko utlmené či nízko rozvinuté, že v konkrétnych prípadoch by bolo možné v týchto aspektoch vidieť podobnosť s podstatou typickou skôr pre „neľudské“ entity.

Otázka, či možno systémom umelej inteligencie priznať právnu subjektivitu, je stále otvorenou a bez jednoznačnej správnej alebo nesprávnej odpovede. Nateraz je táto otázka na úrovni EU vyriešená spôsobom, ktorý reflektuje súčasný stav techniky a technológie. Do akej miery bude riešiť výzvy súvisiace s príchodom AGI či iných vývojových modelov, je predmetom polemiky; totiž viera, že sme a aj zostaneme voči možnostiam či schopnostiam AI imúnni, sa môže ukázať síce ako pohodlná, ale súčasne nebezpečná. Už len z tohto dôvodu je priam nevyhnutné neustále uvažovať a prehodnocovať právnu úpravu, týkajúcu sa umelej inteligencie.

²⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

²⁸ Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 18. novembra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS

²⁹ Návrh smernice Európskeho parlamentu a Rady (EÚ) o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu). 2022/0303(COD)

³⁰ Dostupné na: <https://www.euronews.com/next/2025/07/31/eu-commission-confirms-ditching-of-ai-liability-and-patents-proposals>

Jedným z možných prístupov k regulácii AI je priznanie osobitnej právnej subjektivity, podobnej tej, ktorú majú niektoré „neludské“ entity, predovšetkým korporácie. Ide o relevantnú a odborne diskutovanú tému, avšak bez jednoznačných záverov; prevažujúcimi sú však závery, podľa ktorých by priznanie vlastnej právnej subjektivity elektronickým osobám napriek niektorým výhodám viac problémov prinášalo ako odstraňovalo. Vzhľadom na rýchly vývoj AI technológií bude táto diskusia pokračovať aj naďalej a v budúcnosti, ak sa objavia skutočne autonómne a „silné“ AI, bude otázka povahy AI pravdepodobne opäť nastolená.

Zoznam použitej literatúry

1. Baptista – Rosa, M.: *Animals as Subjects of Rights: Brazil's Constitutional Blueprint*. [online]. Dostupné na: https://leoh.ch/article/view/8714/7338#_ftnref89
2. Cihanová, J.: *AI regulation : the EU and China approach*. In. Acta Facultatis Iuridicae Universitatis Comenianae, č. 1, rok 2024
3. Daňko, M.: *Prienik umelej inteligencie a práva duševného vlastníctva: Výzvy a očakávania*. In: Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024. 150 s. ISBN 978-80-7160-728-1.
4. Doomen, J.: *The artificial intelligence entity as a legal person*. In: Information & Communications Technology Law, 32:3, 277-287, DOI: 10.1080/13600834.2023.2196827
5. Gyurász, Z.: *Keď umelá inteligencia robí chyby: Respondeat superior*. In: Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024. 150 s. ISBN 978-80-7160-728-1.
6. Koehn, L: *Judicial Backlash Against the Rights of Nature in Ecuador*. [online]. Dostupné na: <https://verfassungsblog.de/judicial-backlash-against-the-rights-of-nature-in-ecuador>
7. Novelli, C., Casolari, F., Hacker, P., Spredicato, G., Floridi, L.: *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. Dostupné na: <https://ssrn.com/abstract=4694565>
8. Pietrzykowski, T.: *The Idea of Non-personal Subjects of Law*. DOI:10.1007/978-3-319-53462-6_4
9. Vishnu. S.: *Rise of Artificial Intelligence and Copyright Challenges*. In. Osmania University Journal of IPR [OUJIPR], 1(1), s. 90, Dostupné na: <https://ssrn.com/abstract=4675455>

10. Yalman, B.: *Electronic Personhood: A Compact Analysis of Legal Personality for Artificial Intelligence*. In: *Ex/ante*, 1/2024. Dostupné na: <https://ex-ante.ch/index.php/exante/article/view/258/159>

Kontaktné údaje

doc. JUDr. Martin Križan, PhD.

martin.krizan@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

prof. JUDr. Svetlana Ficová, CSc.

svetlana.ficova@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

UMELÁ INTELIGENCIA A VÝZVY ZMLUVNÉHO PRÁVA V DIGITÁLNEJ ÉRE: ANALÝZA LEGISLATÍVNEHO RÁMCA SLOVENSKEJ REPUBLIKY

ARTIFICIAL INTELLIGENCE AND CONTRACT LAW CHALLENGES IN THE DIGITAL AGE: AN ANALYSIS OF THE LEGISLATIVE FRAMEWORK OF THE SLOVAK REPUBLIC

Martina Babušíková¹

Abstrakt: Rozmach umelej inteligencie a jej integrácia do spoločenskej a hospodárskej sféry generujú nové výzvy aj pre oblasť súkromného práva, osobitne v kontexte zmluvného procesu. Súčasné technologické riešenia umožňujú, aby k vzniku zmluvného vzťahu dochádzalo bez priamej ingerencie fyzickej osoby – autonómne systémy disponujú kapacitou samostatne vyjednávať zmluvné podmienky, posudzovať ponuky a finalizovať zmluvné dohody. Uvedený fenomén však kolидуje s fundamentálnymi doktrinálnymi požiadavkami zmluvného práva, a to najmä s požiadavkou spôsobilosti na právne úkony, existencie vôle a samotného prejavu vedomého súhlasu. Príspevok sa zameriava na analýzu platného legislatívneho rámca Slovenskej republiky so zámerom zodpovedať otázku, či môže umelá inteligencia vystupovať ako autonómny subjekt právnych vzťahov. V kontexte modelových situácií sa zároveň navrhujú možné legislatívne a interpretačné prístupy, ktoré by umožnili integráciu týchto technologických entít do zmluvného prostredia bez narušenia princípov právnej istoty. V závere príspevok identifikuje potrebu systematickej normotvornej intervencie a načrtáva východiská pre adaptáciu zmluvného práva na podmienky digitálnej transformácie.

Kľúčové slová: umelá inteligencia, spôsobilosť na právne úkony, zmluvné právo, digitálna transformácia.

Abstract: The expansion of artificial intelligence and its integration into the social and economic sphere generate new challenges also for the field of private law, particularly in the context of the contractual process. Current technological solutions make it possible for a contractual relationship to be established without the direct involvement of a natural person – autonomous

¹ Univerzita Komenského v Bratislave, Právnická fakulta.

systems possess the capacity to independently negotiate contractual terms, evaluate offers, and even conclude contracts. However, this phenomenon collides with the fundamental doctrinal requirements of contract law, especially the requirement of legal capacity to perform legal acts, the existence of will, and the manifestation of informed consent. The contribution focuses on the analysis of the applicable legislative framework of the Slovak Republic with the aim of answering the question whether artificial intelligence may act as an autonomous subject of legal relations. At the same time, within the context of model situations, it proposes possible legislative and interpretative approaches that would allow the integration of these technological entities into the contractual legal framework without disrupting the principles of legal certainty. In conclusion, the paper identifies the need for future systematic normative intervention and outlines possible directions for the adaptation of contract law to the conditions of digital transformation.

Key words: artificial intelligence, legal capacity to act, contract law, digital transformation.

Úvod

Expanzia umelej inteligencie a jej systematická implementácia v spoločenských a hospodárskych procesoch predstavujú zásadnú výzvu pre tradičné právne paradigmy, a to najmä v oblasti súkromného práva a zmluvných vzťahov. Moderné autonómne systémy disponujú schopnosťou samostatne analyzovať ponuky, vyjednávať podmienky zmlúv a dokonca finalizovať právne záväzné dohody, a to bez priamej účasti, resp. zásahu človeka. Predmetný fenomén stavia do konfliktu fundamentálne doktrínálne požiadavky zmluvného práva, konkrétne spôsobilosť na právne úkony, existenciu vedomej vôle a konsenzu medzi zmluvnými stranami ako predpokladu platnosti zmluvy. Z tohto hľadiska môže jeho neuvážená aplikácia predstavovať potenciálne riziko pre právnu istotu a stabilitu súkromnoprávných vzťahov vo všeobecnej rovine.

V dôsledku týchto zmien sa otvára otázka, do akej miery môže existujúci legislatívny rámec adekvátne reagovať na spomínaný jav, t. j. formovanie a rozvoj autonómnych systémov, pričom je nevyhnutné zohľadňovať nielen ich technické a funkčné špecifiká, ale aj dôsledky vo vzťahu k uplatniteľnosti základných princípov zmluvného práva a s tým súvisiacej zodpovednosti subjektov daných právnych vzťahov. Slovenská legislatíva zatiaľ nepozná kategóriu samostatného „právneho subjektu umelej inteligencie“, pričom tradičné pravidlá zmluvného práva predpokladajú, že

takýmto môže byť výlučne buď fyzická osoba, alebo právnická osoba – ako nositeľ právnej subjektivity.²

Ako sme už naznačili pri všeobecnom hodnotení problematiky, súčasná realita ukazuje, že predmetné systémy môžu plniť funkcie, ktoré si historicky vyžadovali ľudský zásah. Táto skutočnosť preto implikuje potrebu kritického zhodnotenia existujúcich legislatívnych a doktrínálnych rámcov na Slovensku, pričom považujeme za potrebné posúdiť ich potenciálnu pripravenosť vo vzťahu k regulácii právnych úkonov vykonávaných systémami umelej inteligencie, ako aj identifikovať možné vplyvy a dôsledky. Vo všeobecnosti je teda potrebné prihliadať na prebiehajúcu doktrínálnu diskusiu a na vyhodnocovanie interpretačných prístupov, ktoré môžu prispieť k hľadaniu spôsobov integrácie autonómnych systémov do zmluvného prostredia, a to pri rešpektovaní a zachovaní princípov právnej istoty a ochrany účastníkov právnych vzťahov.

Z uvedeného jednoznačne vyvstávajú otázky, kde presne ležia hranice a limity platného právneho rámca Slovenskej republiky, resp. aké sú možnosti jeho adaptácie s prihliadnutím na európsky a medzinárodný legislatívny kontext. Tieto sú predmetom úvah a analýz, ktorým sa venujeme v rámci tohto príspevku.

Teoreticko-doktrínálne východiská

Rozvoj umelej inteligencie prináša potrebu redefinovať tradičné právne pojmy, pričom v rámci tohto príspevku sa pozornosť sústreďuje predovšetkým na oblasť zmluvného práva. Teoretické východiská sú nevyhnutné na pochopenie mechanizmov, ktorými autonómne systémy môžu vstupovať do právnych vzťahov, na identifikáciu hraníc ich právnej pôsobnosti a za účelom analýzy dôsledkov ich činností pre zmluvné záväzky. Autonómne systémy totižto vykonávajú úkony, ktoré historicky predpokladali ľudskú vôľu a schopnosť rozhodovať sa slobodne. S týmto vývojom je spojená dilema, akým spôsobom možno tieto entity posudzovať z hľadiska právnej subjektivity³, a v nadväznosti na to tiež z hľadiska ich spôsobilosti na právne úkony.

V odbornej literatúre sa problematika umelej inteligencie často diferencuje z dvoch perspektív: technickej a právnej. Technická perspektíva skúma umelú inteligenciu

² DUFALOVÁ, Lenka a kol.: Občiansky zákonník komentár. 1. vydanie. Bratislava: C. H. Beck, 2025. 1165 s. 14-15, 32-35.

³ „Právna subjektivita je jedným z esenciálnych právnych inštitútov, na ktorom stojí právny poriadok každej krajiny. Na základe neho priznávame vybraným subjektom možnosť participovať v právnych vzťahoch (získavajú tzv. spôsobilosť byť nositeľom práv a povinností). Napriek tomu, že právnu subjektivitu tradične spájame s fyzickými a právnickými osobami, v ostatnom období vidíme často, ako sa právna subjektivita preplieťa s inými entitami.“ In: METEŇKANYČ, M. Olexij – GYURÁSZ, Zoltán: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. s. 12.

ako systém schopný samostatne sa učiť, analyzovať dáta a prijímať rozhodnutia na základe algoritmických modelov, pričom ide predovšetkým o technologické a funkčné aspekty autonómneho systému.⁴ V rámci právneho kontextu sa zameriavame na to, či a do akej miery môže umelá inteligencia vykonávať právne úkony a byť nositeľom práv a povinností, tzn. či môže vystupovať ako subjekt právnych vzťahov.

Diskusia v právnej doktríne sa v predmetnom kontexte sústreďuje najmä na určenie ontologického statusu umelej inteligencie, a teda na to, či má byť chápaná výlučne ako nástroj v rukách človeka (právny objekt), alebo či možno uvažovať aj o jej transformácii na potenciálny právny subjekt. Ak odhliadneme od ontologických úvah a budeme vychádzať striktne zo súčasného legislatívneho rámca, umelá inteligencia má jednoznačne povahu nástroja využívaného fyzickými a právnickými osobami, keďže jej nemožno pripísať vedomé rozhodovanie, a teda ani spôsobilosť na právne úkony.⁵

V kontexte právnej subjektivity umelej inteligencie je teda nevyhnutné prekonať tradičné antropocentrické prístupy, ktoré si vyžadujú vedomú vôľu či rozum ako podmienky právnej subjektivity. Sylwia Wojtczak tvrdí, že právna subjektivita je komplexný, gradovateľný a askriptívny atribút, ktorý môže byť priznaný rôznym entitám na základe ich účasti v spoločenskom živote, nezávisle od ich schopnosti cítiť alebo rozumieť. Skutočným kritériom právnej subjektivity by mala byť podľa jej názoru schopnosť entity participovať na právnych vzťahoch a spoločenskom živote, čo je možné charakterizovať ako funkčný prístup odlišný od tradičného pohľadu.⁶

V právnej literatúre sa diskusia o právnej subjektivite a spôsobilosti na právne úkony autonómnych systémov odvíja od viacerých protichodných názorov. Medzi argumenty „pro“ patrí predovšetkým dôraz na zachovanie právnej istoty. Súčasný právny rámec jednoznačne definuje, kto je nositeľom práv a povinností, pričom zabezpečuje ochranu slabšej strany proti nezodpovedným a nekontrolovateľným rozhodnutiam umelej inteligencie. Predmetný prístup umožňuje tiež jednoznačnú aplikáciu pravidiel v rámci tradičných zmluvných vzťahoch, pričom právne účinky sa vždy pripisujú reálnym subjektom. Na druhej strane sú argumenty „contra“, ktoré poukazujú na to, že súčasný prístup obmedzuje plnohodnotnú participáciu autonómnych systémov v digitálnych zmluvách a automatizovaných procesoch. Tieto limity môžu viesť k nedostatku právnej jasnosti v situáciách, kde rozhodnutia

⁴ BERTOLINI, Andrea: The European framework on the liability arising from the use of Artificial Intelligence systems and its impact on UAS. In: Civil Regulation of Autonomous Unmanned Aircraft Systems in Europe. Edward Elgar Publishing Ltd., 2024, s. 6.

⁵ BERTOLINI, Andrea – EPISCOPO, Francesca: Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. In: Frontiers in Robotics and AI, č. 9, (2022), článok 842213.

⁶ WOJTCZAK, Sylwia: Endowing Artificial Intelligence with legal subjectivity. In: AI & SOCIETY, roč. 37, č. 1, spôso (2022), s. 205-213.

umelej inteligencie majú reálne právne či ekonomické dôsledky, ale nemožno ich priamo pripísať tomuto systému ako subjektu.⁷

Diskusia teda poukazuje na napätie medzi ochranou zúčastnených subjektov a právnou istotou na strane jednej a potenciálom digitálnych inovácií a autonómnych technológií na strane druhej. Predmetné argumenty sú kľúčové pre ďalšiu analýzu legislatívnych limitov a potenciálnych adaptačných prístupov, ktoré budeme skúmať ďalej.

Európsky a medzinárodný legislatívny rámec

Rozvoj umelej inteligencie je v súčasnosti sprevádzaný snahami vytvoriť harmonizované právne rámce, ktoré nielen podporujú inovácie, ale zároveň zabezpečujú vysokú úroveň ochrany základných práv, a to ako na úrovni Európskej únie, tak aj v medzinárodnom kontexte. Domnievame sa, že potrebu harmonizácie v tejto oblasti treba chápať primárne materiálne – ako zosúladenie vnútroštátnej právnej úpravy, najmä v oblasti zmluvného práva, s novým európskym rámcom pre reguláciu autonómnych systémov umelej inteligencie.

Najvýznamnejším medzníkom je prijatie Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1989 z 13. júna 2024 o umelej inteligencii (tzv. AI Act)⁸. Predmetné nariadenie zavádza rizikovo orientovaný prístup k regulácii umelej inteligencie⁹, ktorý rozlišuje medzi systémami s neprijateľným rizikom, vysokorizikovými a nízkorizikovými aplikáciami.¹⁰ Domnievame sa, že pre oblasť zmluvného práva je obzvlášť významná kategória vysokorizikových systémov, keďže autonómne technológie schopné uzatvárať zmluvy môžu zásadným spôsobom zasahovať do práv a povinností zmluvných strán.¹¹ Zaujímavosťou je, že AI Act pritom zachováva

⁷ Tamtiež.

⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 20 June 2024 on Artificial Intelligence (AI Act)

⁹ MESARČÍK, Matúš – SLOSIAROVÁ, Natália: Regulating AI for a truthful tomorrow: addressing disinformation in the EU Artificial Intelligence Act. In: International Journal of Law and Information Technology, roč. 33, (2025), s. 6.

¹⁰ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. s. 37 – 38.

¹¹ Hoci znenie AI Actu explicitne nesubsumuje autonómne systémy pod vysokorizikové, ich podriadenie pod túto kategóriu je odôvodnené materiálne. Autonómne systémy priamo ovplyvňujú vznik, zmenu alebo zánik práv a povinností zmluvných strán, teda zasahujú do právnej sféry fyzických či právnických osôb. Podľa prílohy III AI Act (článok 6 ods. 2 AI Act) sú za vysokorizikové považované najmä systémy, ktoré vykonávajú rozhodnutia s právnymi účinkami alebo významne ovplyvňujú právne postavenie jednotlivca. Tieto systémy predmetným kritériám zodpovedajú, keďže v zmluvnom procese môžu bez priameho ľudského dohľadu rozhodovať o prijatí či odmietnutí zmluvy, určovať jej podmienky a vyvolávať právne záväzky, pričom takéto správanie je spôsobilé narušiť

tradičný prístup k právnej subjektivite, v rámci ktorého právne účinky úkonov systémov umelej inteligencie aj naďalej pripisuje konkrétnym osobám, ktoré ich vyvinuli¹², alt. prevádzkujú.¹³

Dôležité je zároveň poukázať na prepojenie AI Act s už existujúcim európskym *acquis*. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)¹⁴ v článku 22 priznáva jednotlivcovi právo nebyť predmetom výlučne automatizovaného rozhodnutia, ktoré má na neho právne alebo iné obdobne závažné účinky. Tento princíp, pôvodne orientovaný na ochranu osobných údajov, je možné analogicky využiť aj v zmluvnom práve. Do budúcnosti by tak mohol predstavovať základ pre zavedenie subjektívneho práva účastníka zmluvného procesu na „ľudský kontakt“ pri rozhodnutiach, ktoré zakladajú jeho práva a povinnosti.

Významným pilierom ochrany slabšej strany zostáva aj spotrebiteľské *acquis*, predovšetkým Smernica Rady 93/13/EHS z 5. apríla 1993 o nekalých podmienkach v spotrebiteľských zmluvách a Smernica Európskeho parlamentu a Rady 2011/83/EÚ z 25. októbra 2011 o právach spotrebiteľov, ktorou sa mení a dopĺňa smernica Rady 93/13/EHS a smernica Európskeho parlamentu a Rady 1999/44/ES a ktorou sa zrušuje smernica Rady 85/577/EHS a smernica Európskeho parlamentu a Rady 97/7/ES. Spotrebiteľ, ktorý uzatvára zmluvu prostredníctvom autonómneho systému, môže byť potenciálne vystavený väčšiemu deficitu – či už informačného, alt. mocenského charakteru – ako v tradičných zmluvných situáciách. Vyššie uvedené zdôrazňuje potrebu vyvažovať asymetriu medzi dotknutými zmluvnými stranami, čo má v kontexte digitálnej transformácie mimoriadny význam.

základné princípy zmluvného práva. Vzhľadom na absenciu právnej subjektivity, rozumovej spôsobilosti umelej inteligencie atď., existuje zvýšené riziko, že autonómne systémy budú konať v rozpore s úmyslom používateľa, alt. spôsobom, ktorý môže mať neželané právne následky.

¹² MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. s. 68 – 99.

¹³ V danej súvislosti sa pracovalo s návrhom smernice o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu), ktorá mala doplniť AI Act zavedením mechanizmov uľahčenia dôkazných bremien pre poškodené subjekty – špecifická zodpovednosť. Tento návrh bol však vo februári roku 2025 stiahnutý Európskou komisiou. Pozri tiež: EURÓPSKA KOMISIA: Návrh smernice Európskeho parlamentu a Rady o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu) [online]. COM(2022) 496 final, 2022/0303 (COD). Brusel: Európska únia, 28. september 2022 [cit. 2025-09-01]. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52022PCo496&from=EN>

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Európske úsilie zapadá do širšieho rámca medzinárodných iniciatív. V roku 2019 prijala OECD¹⁵ Princípy pre umelú inteligenciu, ktoré zdôrazňujú ľudskú kontrolu, transparentnosť a zodpovednosť¹⁶. UNESCO¹⁷ nadviazalo v roku 2021 prijatím Odporúčania o etike umelej inteligencie¹⁸. Významná je tiež činnosť Rady Európy, najmä prostredníctvom CAHAI¹⁹, ktorý pripravuje návrh záväzného medzinárodného nástroja zameraného na umelú inteligenciu a ochranu ľudských práv. Nemožno opomenúť ani úlohu UNCITRAL²⁰, ktorého modelový zákon o elektronickom obchode z roku 1996²¹ predstavuje bazálny referenčný rámec vo vzťahu k regulácii umelej inteligencie pri elektronických zmluvách.

Možno konštatovať, že hoci vyššie opísaný právny rámec poskytuje základ pre adaptáciu súkromného práva na prítomnosť umelej inteligencie, mnohé otázky zostávajú otvorené. Pre Slovenskú republiku bude kľúčovou výzvou zosúladiť vnútroštátne právo s AI Act a súčasne reflektovať širšie hodnotové princípy, aby sa zabezpečila právna istota a súčasne efektívne využívanie potenciálu umelej inteligencie. V tomto kontexte by mohlo „soft law“ vyplniť legislatívnu medzeru a viesť k vytváraniu a presadzovaniu štandardov na hodnotenie účinnosti umelej inteligencie a iných technológií používaných pri poskytovaní právnych služieb, keďže tradičné právo nezodpovedá tempu ich rýchleho rozvoja.²²

¹⁵ Organizácia pre hospodársku spoluprácu a rozvoj (Organisation for Economic Co-operation and Development)

¹⁶ OECD. Scoping the OECD AI Principles [online]. Paríž: OECD Publishing, 2019 [cit. 2025-09-15]. Dostupné na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/scoping-the-oecd-ai-principles_71e1b6dc/d62f618a-en.pdf

¹⁷ Organizácia Spojených národov pre vzdelávanie, vedu a kultúru (United Nations Educational, Scientific and Cultural Organization)

¹⁸ UNESCO. Recommendation on the Ethics of Artificial Intelligence [online]. [cit. 2025-09-15]. Dostupné na: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

¹⁹ Ad hoc výbor pre umelú inteligenciu (Ad hoc Committee on Artificial Intelligence of the Council of Europe)

²⁰ Komisia OSN pre medzinárodné obchodné právo (The United Nations Commission on International Trade Law)

²¹ UNCITRAL. Model Law on Electronic Commerce: with Guide to Enactment 1996, with additional Article 5 bis as adopted in 1998 [online]. New York: United Nations, 1999 [cit. 2025-09-15]. Dostupné na: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

²² LINNA, Daniel W.: Evaluating Artificial Intelligence for Legal Services: Can “Soft Law” Lead to Enforceable Standards for Effectiveness?. In: IEEE Technology and Society Magazine, roč. 40, č. 4, (2021), s. 37.

Slovenský legislatívny rámec a jeho aplikačné limity

Zmluvné právo Slovenskej republiky vyžaduje vo vzťahu k tejto problematike tri základné predpoklady²³ pre platný právny úkon²⁴, a to spôsobilosť na právne úkony ako schopnosť subjektu nadobúdať práva a zaväzovať sa k povinnostiam, existenciu vôle ako vedomé a slobodné rozhodnutie konať právny úkon a konsenzus medzi stranami v podobe dohody, ktorá je podstatou zmluvného vzťahu – prejav vôle.²⁵ „Právny úkon je jedna z najtypickejších (subjektívnych) právnych skutočností, ktoré vyvolávajú právny následok.“²⁶

Autonómne systémy v súčasnosti nespĺňajú predmetné predpoklady, keďže ich konanie je determinované algoritmom a dátami, nie vedomou a slobodnou voľou, pričom ani ich prejav nie je vyjadrením subjektívnej vôle. „Spôsobilosť na právne úkony je spôsobilosť (právna schopnosť) osoby samostatne, vlastným vôľovým konaním vyvolávať právne relevantné následky.“²⁷ Z tohto dôvodu ich právna subjektivita – v zmysle súčasného právneho rámca – nie je uznaná, a teda nemôžu disponovať ani spôsobilosťou na právne úkony.²⁸ Tento stav jasne ilustruje rozdiel medzi súčasným legislatívnym rámcom a teoretickými koncepciami, ktoré diskutujú o možnosti priznať autonómnym systémom určitú formu právnej relevancie, alt. participácie na právnych vzťahoch.

Slovenská legislatíva čerpá tiež z princípov ochrany slabšej strany, najmä spotrebiteľa, ktoré sú zakotvené v zákone o ochrane spotrebiteľa²⁹. Jeho ustanovenia zabezpečujú rovnováhu medzi účastníkmi zmluvných vzťahov, pričom ich rámec predstavuje základ pre posúdenie možností a limitov integrácie autonómnych systémov do právneho prostredia. Predmetný zákon poskytuje kritériá, podľa ktorých je možné identifikovať, či by určitý systém mohol byť čisto teoreticky považovaný za subjekt právnych vzťahov, resp. akým spôsobom by bolo možné jeho činnosť pripísať fyzickým alebo právnickým osobám.

Používanie umelej inteligencie ako takej je legálne, otázkou však zostáva, ako ju používať v kontexte zmluvných vzťahov. Umelá inteligencia je výlučne technologický

²³ Neoddeliteľnou súčasťou právneho úkonu je aj objekt, ktorého sa takýto úkon týka.

²⁴ Pozri tiež: DUFALOVÁ, Lenka a kol.: Občiansky zákonník komentár. 1. vydanie. Bratislava: C. H. Beck, 2025. s. 93-106.

²⁵ zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

²⁶ DUFALOVÁ, Lenka a kol.: Občiansky zákonník komentár. 1. vydanie. Bratislava: C. H. Beck, 2025. s. 93.

²⁷ Tamtiež: s. 104.

²⁸ „Na rozdiel od právnej subjektivity je pre určenie spôsobilosti na právne úkony potrebné brať do úvahy intelektuálnu spôsobilosť.“ In: DUFALOVÁ, Lenka a kol.: Občiansky zákonník komentár. 1. vydanie. Bratislava: C. H. Beck, 2025. s. 16.

²⁹ zákon č. 108/2024 Z. z. o ochrane spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

nástroj založený na softvéri a počítačoch, pričom podobne ako akákoľvek iná technika, môže byť využívaná v širokom spektre systémov. Hoci je používanie umelej inteligencie vo väčšine prípadov legálne, právny status jej konkrétnych aplikácií závisí od právneho systému každého štátu a od konkrétneho kontextu. Tieto limity sa najvýraznejšie prejavujú na digitálnych platformách a pri automatizovaných zmluvných procesoch, kde umelá inteligencia vykonáva úkony, ktoré by za iných okolností vyžadovali účasť právne zodpovedného subjektu.³⁰

Slovenský legislatívny rámec tak zostáva robustný pri tradičných zmluvných vzťahoch, avšak jeho aplikačné limity sa prejavujú práve pri autonómnych systémoch, ktoré nemajú právnu subjektivitu a nemôžu samostatne konať. Implementácia umelej inteligencie so sebou prináša množstvo právnych a regulačných výziev. Nedostatočne promptná reakcia legislatívneho rámca však spôsobuje, že existujúca legislatíva nie je schopná efektívne reagovať na dynamicky sa vyvíjajúce aplikačné problémy, ktoré sa v súvislosti s týmito technológiami objavujú s rastúcou frekvenciou.³¹

Perspektívy de lege ferenda

Súčasný legislatívny rámec Slovenskej republiky neberie do úvahy existenciu autonómnych systémov v postavení aktérov právnych vzťahov. Napriek tomu sa čoraz častejšie stretávame s praktickými situáciami, v ktorých umelá inteligencia zohráva významnú úlohu pri zmluvných procesoch, a to nielen v podobe technického nástroja, ale aj ako aktívny element schopný analyzovať dáta a navrhovať optimálne riešenia. Dynamika digitálnej transformácie vytvára tlak na normotvorný proces, aby reagoval na nové výzvy. *„Táto dynamika pramení nielen z konzervativizmu práva a enormne rýchlo sa vyvíjajúcich technológií, ale aj z mnohých rôznych foriem a možností aplikácie týchto technológií. Táto rôznorodosť spôsobuje, že často nie je možné subsumovať predmetné technologické inovácie pod ktorýkoľvek z existujúcich regulačných rámcov.“*³² Cieľom legislatívnej adaptácie by však nemalo byť priznanie právnej subjektivity, ale skôr vytvorenie hybridného modelu postavenia a zodpovednosti, ktorý by umožnil jej efektívnu integráciu bez narušenia princípov právnej istoty.

³⁰ KHALIFA, Mahmoud – SABRY, Mahmoud: The Challenges of The Artificial Intelligence of Law in The Context of Technological Development. In: 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), (2024), s. 106.

³¹ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. s. 111.

³² METEŇKANYČ, M. Olexij – GYURÁSZ, Zoltán: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. s. 77.

V tomto smere je inšpiratívny práve európsky právny rámec, a to najmä AI Act. Ako už bolo aj vyššie uvedené, predmetné nariadenie zohľadňuje úroveň rizika, ktoré autonómny systém môže predstavovať pre práva a bezpečnosť osôb.³³ Pre oblasť zmluvného práva by to znamenalo, že systémy umelej inteligencie, ktoré samostatne vyjednávajú alebo navrhujú zmluvné podmienky, by sa subsumovali pod vysoko rizikové a podliehali by prísnyim pravidlám transparentnosti, dohľadu a zodpovednosti. Takýto prístup by zabezpečoval, že pri využívaní umelej inteligencie v rámci daných procesov by zostala primárna zodpovednosť vždy na ľudských účastníkoch, t. j. poskytovateľoch či užívateľoch systému, čím by sa podľa nášho názoru minimalizovalo riziko právnej neistoty a škody spôsobenej automatizovanými rozhodnutiami takéhoto systému.

Perspektívne sa javí aj zavedenie osobitného právneho statusu pre umelú inteligenciu v zmluvných procesoch. V doktrínálnej diskusii sa objavujú rôzne prístupy – od chápania umelej inteligencie výlučne ako nástroja až po úvahy o jej možnom postavení ako subjektu práva.³⁴ De lege ferenda je možné zvážiť zavedenie kategórie „právny agent“, ktorá by sa funkčne približovala zastúpeniu. Predmetné by znamenalo, že umelá inteligencia by nebola samostatným subjektom práva, ale jej úkony by sa priamo pripisovali osobe, ktorá stojí za systémom a tento prevádzkuje. *„Hoci systémy na báze umelej inteligencie napodobňujú ľudskú inteligenciu, chýba im subjektivita z právneho pohľadu, ktorá by im umožnila mať tieto práva a povinnosti v tradičnom zmysle. Bude preto vždy potrebné nájsť, aká konkrétna osoba (subjekt práva) bude za tieto systémy zodpovedať.“*³⁵ Daný prístup by posilnil právnu istotu a zabránil vzniku právneho vákua, v ktorom by úkony vykonávané umelou inteligenciou ostali bez priamej zodpovednosti určenej konkrétnej osobe.

Z praktického hľadiska sa v minulosti pracovalo aj s návrhom smernice o zodpovednosti za umelú inteligenciu, ktorá mala doplniť vyššie uvedené nariadenie. Tento návrh však nebol akceptovaný Európskou komisiou, pričom momentálne neexistuje jeho substitúcia. Napriek tomu môže slúžiť ako dôležitý teoretický východiskový bod, ktorý ilustruje možné prístupy k zavádzaniu zodpovednostných

³³ IVKOVIČ, Ratko – VUČKOVIČ, Dragan a kol: The EU AI Act and Its Contractual and Educational Implications: AI, Education, and the Law of Obligations. In: International Journal of Cognitive Research in Science, Engineering and Education, roč. 13, č. 2 (2025), s. 554.

³⁴ BERTOLINI, Andrea: La inteligencia artificial no existe! Desafiando la narrativa de la neutralidad tecnológica en la regulación de la responsabilidad civil de las tecnologías avanzadas. In: Revista de derecho privado (Universidad Externado de Colombia. Departamento de Derecho Civil), roč. 7, č. 49 (2025), s. 31-82.

³⁵ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. s. 108.

mechanizmov aj v slovenskom právnom poriadku a poskytuje inšpiráciu pri úvahách o adaptácii zmluvnej a občianskoprávnej regulácie v kontexte umelej inteligencie.³⁶ S tým úzko súvisí aj potreba posilniť požiadavky transparentnosti a overiteľnosti právnych úkonov vykonávaných prostredníctvom umelej inteligencie.³⁷ Za zmienku s určitosťou stojí povinnosť zaznamenávať „digitálnu stopu“, t. j. údaje o nastavení systému, použitých parametroch a výstupoch, pričom v zmluvách by bolo možné uvádzať označenie vo forme doložky o automatizovanom spracovaní. Takéto opatrenie by významne prispelo k posilneniu dôkaznej istoty v prípadných sporoch. Okrem toho by pravidelné monitorovanie a audit týchto záznamov mohlo podporiť transparentnosť činnosti autonómnych systémov a uľahčiť identifikáciu zodpovednosti.³⁸

Domnievame sa, že osobitná pozornosť by mala byť venovaná ochrane slabšej strany, predovšetkým spotrebiteľov. V zmluvných vzťahoch, v ktorých podmienky navrhuje alebo vyjednáva umelá inteligencia, by mal zákon výslovne požadovať, aby bol spotrebiteľ informovaný, že komunikuje s autonómnym systémom a nie s človekom. Súčasne navrhujeme zaviesť právo na ľudský kontakt, ktoré by garantovalo, že rozhodnutia nesmú byť za každých okolností vykonávané výlučne automatizovaným systémom bez možnosti zásahu človeka. Predmetné opatrenie by posilnilo právnu istotu účastníkov zmluvného vzťahu a súčasne by ochránilo slabšiu stranu pred nepriaznivými následkami automatizovaného rozhodovania.³⁹

Napokon je potrebné zdôrazniť, že slovenský právny poriadok musí byť dostatočne flexibilný, aby dokázal reagovať na dynamicky a technologicky vývoj. Zavedenie otvorených klauzúl alebo rámcových ustanovení by umožnilo súdom v prípade sporov reflektovať atypické situácie, ktoré v súčasnej dobe nemožno predvídať.

*„Právna subjektivita je jedným z esenciálnych právnych inštitútov, na ktorom stojí právny poriadok každej krajiny. Na základe neho priznávame vybraným subjektom možnosť participovať v právnych vzťahoch. Aj napriek tomu, že právnu subjektivitu tradične spájame s fyzickými a právnickými osobami, v ostatnom období vidíme často, ako sa právna subjektivita preplietá s inými entitami.“*⁴⁰ Zmyslom navrhovaných riešení nie je definitívne zakotvenie právnej subjektivity umelej inteligencie, ale

³⁶ SASDELLI, Pietro: Proposed EU AI liability rules withdrawn [online]. London: Bird & Bird, 31. marec 2025 [cit. 2025-09-05]. Dostupné na: <https://www.twobirds.com/en/insights/2025/proposed-eu-ai-liability-rules-withdrawn>

³⁷ Organizácia OECD. OECD AI Principles. [online]. [cit. 2025-09-19]. Dostupné na: <https://www.oecd.org/going-digital/ai/principles/>

³⁸ Inšpirované čl. 22 všeobecného nariadenia o ochrane údajov.

³⁹ Tamtiež.

⁴⁰ MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. s. 104.

vytvorenie prostredia, ktoré umožní jej integráciu do spoločenskej praxe pri zachovaní rovnováhy medzi inováciou a princípmi právnej istoty.

Záver

Umelá inteligencia sa stáva jedným z určujúcich fenoménov digitálnej éry, ktorý zasahuje nielen do technologického, ale aj do právneho priestoru. Zmluvné právo je pritom oblasťou, v rámci ktorej sa stretáva dynamika inovácií s požiadavkami právnej istoty a ochrany jednotlivca. Výzvou zostáva, ako začleniť autonómne systémy do existujúcej legislatívnej úpravy bez toho, aby sa narušila jej vnútorná konzistencia a základné hodnoty.

Jadro problému nespočíva výlučne v technickej kapacite umelej inteligencie vykonávať určité právne úkony, ale predovšetkým v otázke, či a v akom rozsahu jej možno priznať právnu relevanciu. Odpoveď na predmetnú otázku si vyžaduje kombináciu legislatívneho zásahu a doktrínálnej interpretácie, ktoré umožnia nájsť rovnováhu medzi efektívnosťou zmluvných procesov a ochranou slabšej strany.

Európske a medzinárodné legislatívy potvrdzujú, že budúcnosť právnej úpravy nebude s veľkou pravdepodobnosťou viesť k priznaniu právnej subjektivity a spôsobilosti na právne úkony umelej inteligencii, ale k vytvoreniu regulačných mechanizmov, ktoré zabezpečia zodpovednosť a transparentnosť pri jej používaní.

Pre Slovenskú republiku to znamená nielen povinnosť harmonizácie s európskym právom, ale aj potrebu vnútroštátnej reflexie, ktorá zohľadní osobitosti slovenského právneho poriadku. Do budúcnosti sa tak otvára priestor pre premyslenú normotvornú činnosť, ktorá nesmie ignorovať hodnotové piliere súkromného práva. Digitálna transformácia prináša nové výzvy, no zároveň aj možnosť potvrdiť, že slovenský právny poriadok má schopnosť reagovať na technologický pokrok spôsobom, ktorý bude rešpektovať tradíciu, no zároveň bude schopný umožniť implementáciu inovácií.

Zoznam použitej literatúry

1. BROOKS, Chay – GHERHES, Cristian – VORLEY, Tim: Artificial intelligence in the legal sector: Pressures and challenges of transformation. In: Cambridge Journal of Regions, Economy and Society, roč. 13, č. 1, (2020), s. 135-152.
2. BERTOLINI, Andrea: La inteligencia artificial no existe! Desafiando la narrativa de la neutralidad tecnológica en la regulación de la responsabilidad civil de las tecnologías avanzadas. In: Revista de derecho privado (Universidad Externado de Colombia. Departamento de Derecho Civil), roč. 7, č. 49 (2025), s. 31-82.
3. BERTOLINI, Andrea: The European framework on the liability arising from the use of Artificial Intelligence systems and its impact on UAS. In: Civil Regulation

of Autonomous Unmanned Aircraft Systems in Europe. Edward Elgar Publishing Ltd., 2024, s. 64-79. ISBN 978-103531234-4.

4. BERTOLINI, Andrea – EPISCOPO, Francesca: Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. In: *Frontiers in Robotics and AI*, č. 9, (2022), článok 842213.
5. DUFALOVÁ, Lenka a kol.: *Občiansky zákonník komentár*. 1. vydanie. Bratislava: C. H. Beck, 2025. 1165 s. ISBN 978-80-8232-062-9.
6. LINNA, Daniel W.: Evaluating Artificial Intelligence for Legal Services: Can “Soft Law” Lead to Enforceable Standards for Effectiveness?. In: *IEEE Technology and Society Magazine*, roč. 40, č. 4, (2021), s. 37-51.
7. EURÓPSKA KOMISIA: Návrh smernice Európskeho parlamentu a Rady o prispôsobení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu) [online]. COM(2022) 496 final, 2022/0303 (COD). Brusel: Európska únia, 28. september 2022 [cit. 2025-09-01]. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52022PC0496&from=EN>
8. IVKOVIĆ, Ratko – VUČKOVIĆ, Dragan a kol.: The EU AI Act and Its Contractual and Educational Implications: AI, Education, and the Law of Obligations. In: *International Journal of Cognitive Research in Science, Engineering and Education*, roč. 13, č. 2 (2025), s. 551-562.
9. KHALIFA, Mahmoud – SABRY, Mahmoud: The Challenges of The Artificial Intelligence of Law in The Context of Technological Development. In: *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETIS)*, (2024), s. 105-109.
10. MESARČÍK, Matúš – SLOSIAROVÁ, Natália: Regulating AI for a truthful tomorrow: addressing disinformation in the EU Artificial Intelligence Act. In: *International Journal of Law and Information Technology*, roč. 33, (2025), s. 1-14.
11. MESARČÍK, Matúš – GYURÁSZ, Zoltán a kol.: *Právo a umelá inteligencia*. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2024. 244 s. ISBN 978-80-7160-715-1.
12. METEŇKANYČ, M. Olexij – GYURÁSZ, Zoltán: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022. 133 s. ISBN 978-80-7160-667-3.
13. OECD. *OECD AI Principles*. [online]. [cit. 2025-09-19]. Dostupné na: <https://www.oecd.org/going-digital/ai/principles/>
14. OECD. *Scoping the OECD AI Principles* [online]. Paríž: OECD Publishing, 2019 [cit. 2025-09-15]. Dostupné na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/scoping-the-oecd-ai-principles_71e1b6dc/d62f618a-en.pdf

15. PAPADOULI, Vasiliki: Artificial intelligence in the legal sector: Applications, ethical challenges, and legal concerns under European union law. In: Artificial Intelligence in Legal Systems: Bridging Law and Technology through AI. CRC Press, 2025, s. 6-21. ISBN 978-104040485-0.
16. SASDELLI, Pietro: Proposed EU AI liability rules withdrawn [online]. London: Bird & Bird, 31. marec 2025 [cit. 2025-09-05]. Dostupné na: <https://www.twobirds.com/en/insights/2025/proposed-eu-ai-liability-rules-withdrawn>
17. ŠTEVČEK, Marek a kol.: Občiansky zákonník I. § 1 – 450. Komentár. Praha: C. H. Beck. 2015, 1616 s. ISBN 978-80-7400-597-8.
18. UNCITRAL. Model Law on Electronic Commerce: with Guide to Enactment 1996, with additional Article 5 bis as adopted in 1998 [online]. New York: United Nations, 1999 [cit. 2025-09-15]. Dostupné na: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf
19. UNESCO. Recommendation on the Ethics of Artificial Intelligence [online]. [cit. 2025-09-15]. Dostupné na: <https://unesdoc.unesco.org/ark:/48223/pf00000381137>
20. WOJTCZAK, Sylwia: Endowing Artificial Intelligence with legal subjectivity. In: AI & SOCIETY, roč. 37, č. 1, (2022), s. 205-213.

Kontaktné údaje

JUDr. Martina Babušíková

martina.babusikova@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

DOKAZOVANIE V ÉRE DIGITÁLNEJ ILÚZIE

EVIDENCE IN THE ERA OF DIGITAL ILLUSION

Lucia Mertl¹

Abstrakt: Rýchly rozvoj generatívnej umelej inteligencie prináša nové výzvy aj pre oblasť civilného procesu. Jedným z výrazných fenoménov v tejto súvislosti sú tzv. deepfakes, a teda obsah vytvorený, alebo pozmenený generatívnou umelou inteligenciou tak, že tento pôsobí autenticky a dokáže simulovať realitu s takou presvedčivosťou, že jeho odlíšenie od autentického obsahu je pre laika prakticky nemožné. Z uvedeného dôvodu predstavujú deepfakes nielen technologickú hrozbu, ale najmä komplexnú spoločenskú a právnu výzvu, ktorej bude v dohľadnej dobe čeliť aj súdny systém. Deepfake dôkazy môžu zásadne zmeniť proces dokazovania pred súdom a potenciálne narušiť dôveru verejnosti v súdny systém ako taký. Predkladaný príspevok definuje a analyzuje riziká, ktorým môžu čeliť súdy pri posudzovaní pravosti predkladaných dôkazov a aj možné dopady deepfake dôkazov na rozdelenie a presun dôkazného bremena. Za účelom lepšieho pochopenia predmetnej problematiky príspevok pracuje s konkrétnym modelovým prípadom a v rámci neho demonštruje potenciálne problémy a navrhuje riešenia, ako sa v medziach súčasnej právnej úpravy možno s týmito hrozbami vysporiadať.

Kľúčové slová: dokazovanie, dôkazné bremeno, umelá inteligencia, deepfakes

Abstract: The rapid development of generative artificial intelligence also brings new challenges in the area of civil proceedings. One of the most notable phenomena associated with it is deepfakes, i.e., content created or altered by artificial intelligence in such a way that it appears authentic and can simulate reality with such conviction that it is virtually impossible for a layperson to distinguish it from authentic content. For this reason, deepfakes represent not only a technological threat, but also a complex social and legal challenge that the judicial system will face in the foreseeable future. Deepfake evidence can fundamentally change the process of evidence presentation in court and potentially undermine public confidence in the judicial system as such. This paper defines and analyzes the risks that courts may face when assessing the authenticity of evidence presented, as well as the possible impacts of deepfake

¹ Univerzita Komenského v Bratislave, Právnická fakulta

evidence on the distribution and transfer of the burden of proof. In order to better understand the issue, the paper uses a specific model case to demonstrate potential problems and propose solutions for dealing with these threats under the existing legal framework.

Key words: evidence, burden of proof, artificial intelligence, deepfakes

Úvod

S rýchlym rozvojom generatívnej umelej inteligencie dochádza zároveň k zvyšovaniu kvality deepfakes a širšej dostupnosti nástrojov na ich vytváranie. Deepfake predstavuje audio, vizuálny a audiovizuálny obsah, ktorý je umelo modifikovaný (pozmenený), alebo kompletne vytvorený prostredníctvom generatívnej umelej inteligencie.

Napriek tomu, že v našich podmienkach zatiaľ nie je známy žiadny prípad, kedy by bol v súdnom konaní predložený dôkaz, ktorý možno kvalifikovať ako deepfake, považujeme deepfake za už prítomnú a neustále rastúcu hrozbu pre súdne konanie, a to nielen civilné.

Súd, ktorý bol doposiaľ zvyknutý sa v zásade spoliehať na pravosť predložených audio, vizuálnych a audiovizuálnych záznamov, čelí v tejto dobe novým výzvam pri posudzovaní predkladaných dôkazov, nakoľko v ére generatívnej umelej inteligencie sa tradičné spôsoby posudzovania dôkazov súdom už nemusia javiť ako dostačujúce. Odhalenie sofistikovaného deepfake, ktorý nevykazuje zjavné vady (napr. že hlas nekorešponduje s obrazom, neprirodzený pohyb očí a iné), si vyžaduje odborné posúdenie kompetentným subjektom (napr. znalec).

V Spojených štátoch amerických v súčasnosti posudzujú návrhy odborníkov na zmenu tzv. Rule 901² ("Pravidlo 901"), ktoré upravuje overovanie a identifikáciu dôkazov predkladaných v súdnom konaní s cieľom riešiť výzvy, ktoré predstavujú deepfake dôkazy - dôkazy generované umelou inteligenciou.

Podstatou súčasne platného Pravidla 901 je, že navrhovateľ musí vhodným spôsobom preukázať, že „predmetná vec je taká, ako tvrdí jej navrhovateľ“³, a to predtým, ako je dôkaz pripustený. Odsek (b) Pravidla 901 obsahuje demonštratívny výpočet príkladov dôkazov, ktoré takúto požiadavku spĺňajú, a to napríklad svedectvo relevantného svedka, dôkazy o telefonickom rozhovore, porovnanie odborným svedkom, predloženie dôkazov o procese, alebo systéme a iné. Po oboznámení sa s jednotlivými pravidlami možno konštatovať, že tieto sa v dobe

² Federal Rules of Evidence (FRE) 901

³ V originálnom znení: "*The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.*"

rapídne sa rozvíjajúcej generatívnej umelej inteligencie nejavia ako dostatočné, hoc môžu slúžiť ako akási pomôcka v procese vysporiadania sa s dôkazmi, ktoré sú produktom generatívnej umelej inteligencie.

V súlade s návrhom zmeny Pravidla 901, ak strana spochybňujúca pravosť počítačom generovaných alebo iných elektronických dôkazov predloží dostatočné dôkazy na podporu skutkového tvrdenia, že spochybňované dôkazy boli celkom alebo čiastočne manipulované alebo sfalšované generatívnou umelou inteligenciou, navrhovateľ dôkazov musí overiť pravosť dôkazov podľa pododseku (b) a poskytnúť dodatočné dôkazy potvrdzujúce ich spoľahlivosť.

V predložennom príspevku sa na modelovom príklade pokúsime analyzovať jednotlivé možnosti, ako sa súd v medziach súčasnej právnej úpravy môže vysporiadať s dôkazom, ktorý je predložený jedným z účastníkov a o ktorom druhý účastník tvrdí, že nie je autentický, ale bol digitálne zmanipulovaný.

V nadväznosti na uvedené formulujeme nasledovnú hypotézu "Súčasná právna úprava civilného procesu poskytuje dostatočné záruky pre spravodlivý súdny proces v ére generatívnej umelej inteligencie."

Modelový súdny spor

V predkladanom príspevku budeme pracovať s modelovým súdnym sporom, v ktorom sa zamestnanec domáha určenia neplatnosti výpovede podanej zamestnávateľom z dôvodu závažného porušenia disciplíny, ktoré malo spočívať v tom, že zamestnanec sa v priestoroch zamestnávateľa opakovane dopustil protiprávneho konania (poškodenia majetku zamestnávateľa alebo krádeže), pričom takéto jeho protiprávne konanie bolo zachytené kamerou. Zamestnávateľ sa pri skončení pracovného pomeru opiera o dôkazné prostriedky - kamerové záznamy, ktoré sú kľúčovým dôkazným prostriedkom preukazujúcim protiprávne konanie zamestnanca. Zamestnanec v súdnom konaní namieta, že predložené kamerové záznamy nie sú autentické a že sa jedná o deepfake.

Možnosti vysporiadania sa s deepfake dôkazmi a námietkami ohľadne deepfake dôkazov

Súd získava poznatky potrebné na naplnenie účelu súdneho konania predovšetkým prostredníctvom dokazovania, a teda na to, aby súdne konanie plnilo svoju funkciu, je nevyhnutné, aby súd mal potrebné poznatky, a to ako skutkové, tak právne.⁴

Procesné kódexy pojem dokazovanie nedefinujú, upravujú len pravidlá dokazovania a poskytujú demonštratívny výpočet dôkazných prostriedkov. Priebeh dokazovania

⁴ MACUR, J.: Dokazování a procesní odpovědnost v občanském soudním řízení. Brno: Universita J. E. Purkyně, 1984. 11 s.

a zameranie sa na zisťovanie skutočného alebo skutkového stavu sa odlišuje v závislosti od typu konania.⁵ Svoboda ponúka vlastnú definíciu dokazovania a uvádza, že dokazovanie je právom a procesnými zvyklosťami upravený postup súdu a účastníkov, ktorého účelom je získanie poznatkov dôležitých pre meritórne či iné rozhodnutie súdu alebo pre ďalší postup súdu alebo účastníkov. Súd môže získať poznatky podstatné pre rozhodnutie alebo pre svoj ďalší postup aj inak, než dokazovaním, pokiaľ tak ustanoví zákon.⁶

V súvislosti s problematikou deepfakes možno identifikovať dve zásadné hrozby pre civilné konanie, a to jednak samotné predkladanie deepfake dôkazov a ich prezentovanie ako autentických, a na druhej strane účelové spochybňovanie autentických dôkazov tvrdením, že sa jedná o deepfake, hoc účastník konania má vedomosť, že dôkaz je autentický. Procesné kódexy explicitne neupravujú postup súdu v prípade, že účastník vznesie námietku, že určitý dôkaz je deepfake. Vzhľadom na uvedené je potrebné preto vychádzať z existujúcich ustanovení procesných kódexov a z už známych inštitútov.

Je nepochybné, že posúdenie, či určitý dôkazný prostriedok bol pozmenený alebo vytvorený generatívnou umelou inteligenciou, je vysoko odbornou otázkou. Deepfakes predstavujú obsah, ktorý je na nerozoznanie od reality, a preto štandardné metódy overovania pravosti sa v týchto prípadoch javia ako nedostatočné a spravidla je potrebné, aby takéto tvrdenie potvrdila alebo vyvrátila odborne spôsobilá osoba. V tejto súvislosti sa ako problematický javí nielen nedostatok odborníkov na kvalifikované posúdenie tejto otázky v našich podmienkach, ale aj časová a finančná náročnosť takéhoto posúdenia. V tomto príspevku sa budeme ďalej zaoberať možnosťami vysporiadania sa s takýmito dôkaznými prostriedkami, alebo námietkami, bez potreby predkladania znaleckého posudku.

Ustanovenie § 150 ods. 1 CSP zakotvuje tzv. povinnosť pravdivosti, t.j. že strany majú povinnosť pravdivo a úplne uvádzať podstatné a rozhodujúce skutkové tvrdenia týkajúce sa sporu. Profesor Macur uvádza: „*procesní strana nesmí tvrdit skutečnosti, o nichž je přesvědčena, že jsou nepravdivé. Nesmí také popírat tvrzení odpůrce, je-li přesvědčena o jejich pravdivosti.*“⁷

Prof. Macur ďalej uvádza, že porušenie tejto povinnosti by malo byť sankcionované „*vzniká dostatečný prostor pro uplatnění všech složitých a početných kritérií v různých, podstatně rozdílných procesních situacích, v nichž uplatnění sankce za porušení*

⁵ ŠTEVČEK, M., FICOVÁ, S., BARICOVÁ, J., MESIARKINOVÁ, S., BAJÁNKOVÁ, J., TOMAŠOVIČ, M. a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022, s. 744

⁶ SVOBODA, K. *Dokazování*. Praha: ASPI - Wolters Kluwer, 2009, s. 12

⁷ MACUR, J.: Povinnosť pravdivosti a její legislativní úprava v civilním soudním řádu. Právní rozhledy, ročník 1999, č. 4.

vysvetlovací povinnosti přichází v úvahu."⁸ K porušeniu tejto povinnosti dochádza najmä v prípadoch, keď strana vedome označí autentický dôkaz za deepfake, prípadne naopak predloží deepfake ako autentický dôkaz, avšak procesné kódexy neobsahujú žiadne sankcie za porušenie tejto povinnosti.

V modelovom prípade sa jedná o individuálny pracovnoprávny spor podľa ustanovenia § 316 CSP a nasl., t.j. spor medzi zamestnancom a zamestnávateľom vyplývajúci z pracovnoprávneho vzťahu. Tieto spory sa spolu s antidiskriminačnými spormi a spotrebiteľskými spormi radia medzi tzv. spory s ochranou slabšej strany upravené v druhej hlave tretej časti Civilného sporového poriadku a vykazujú určité odlišnosti oproti ostatným sporom, v ktorých vystupujú strany, ktoré možno považovať za rovnocenné. Tieto odlišnosti budeme ďalej v tomto príspevku zohľadňovať.

Jednou z osobitostí sporov s ochranou slabšej strany je, že súd môže vykonať aj tie dôkazy, ktoré zamestnanec nenavrhol, ak je to nevyhnutné pre rozhodnutie vo veci. Súd aj bez návrhu obstará alebo zabezpečí taký dôkaz; na tento účel je zamestnávateľ povinný poskytnúť súčinnosť, ak to možno od neho spravodlivo žiadať.

Takáto odlišnosť je odbornou literatúrou označovaná ako príklon k vyšetrovaciemu princípu v civilnom súdnom konaní, ktorý je odôvodnený legitímnou potrebou zvýšenej miery ingerencie orgánu ochrany práva za účelom toho, aby žalobca mal možnosť na férový súboj so žalovaným v spore o nároky vyplývajúce z individuálnych pracovnoprávnych vzťahov.⁹ Cieľom takejto zvýšenej aktivity súdu je nielen spoľahlivé zistenie skutkového stavu, ale najmä vydanie spravodlivého rozhodnutia. Ako uvádza Ústavný súd SR: "*Aj napriek ústavnej zásade voľného hodnotenia dôkazov nemôže všeobecný súd bez náležitého odôvodnenia „uveriť“ a stotožniť sa s jedným dôkazom (konkrétnymi svedeckými výpoveďami) a bez ďalšieho „neuveriť“ a odmietnuť iné dôkazy (iné svedecké výpovede). Všeobecný súd je povinný zistiť procesnú pravdu v konaní, k čomu má slúžiť práve dokazovanie.*"¹⁰

Pre účely tohto príspevku budeme vychádzať zo stavu, že zamestnávateľ predložil súdu kamerové záznamy, ktoré zamestnanec spochybnil a tvrdí o nich, že sú zmanipulovaným audiovizuálnym obsahom (deepfake).

V prípade, že strana kvalifikovane namietne pravosť dôkazu, súd by mal v prvom rade skúmať, či sa nejedná o nezákonný dôkaz, pričom ak súd uzavrie, že sa jedná o dôkaz získaný v rozpore s právnymi predpismi, mal by tento dôkaz podrobiť testu proporcionality. Tento postup by mohol slúžiť ako akýsi pomyselný "prvý filter", ktorého využitie nie je časovo a ani finančne náročné v porovnaní napríklad so

⁸ Tamtiež

⁹ ŠTEVČEK, M., FICOVÁ, S., BARICOVÁ, J., MESIARKINOVÁ, S., BAJÁNKOVÁ, J., TOMAŠOVIČ, M. a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022, s. 1220 s.

¹⁰ Nález Ústavného súdu SR z 8.9.2020, č. k. III. ÚS 86/2020

znaleckým posudkom. V širšom zmysle slova sa za nezákonný dôkaz považuje akýkoľvek dôkaz, pri ktorého získaní boli porušené právne predpisy; v užšom zmysle slova sa najčastejšie však jedná o dôkazy, pri ktorých získaní došlo k porušeniu práva na ochranu osobnosti podľa ustanovenia § 11 a nasl. Občianskeho zákonníka, t.j. najmä vizuálny, audio a audiovizuálny obsah. Nezákonne získané dôkazy sú vo všeobecnosti v civilnom procese považované za právne neúčinné, t.j. súd ich neberie pri prejednávaní a rozhodovaní veci do úvahy, ibaže vykonanie dôkazu získaného v rozpore so zákonom je odôvodnené uplatnením čl. 3 ods. 1 CSP. Právna úprava civilného procesu teda pripúšťa uplatnenie výnimky z tohto pravidla, ak je vykonanie nezákonného dôkazu odôvodnené ústavnokonformným výkladom práva. Základným kritériom, ktoré má viesť k rozhodnutiu o použiteľnosti či nepoužiteľnosti nezákonného dôkazu v príslušnom konaní, je pomerenie chránených práv a záujmov, ktoré sa v tejto súkromnej sfére stretávajú.¹¹ Ak teda súd uzavrie, že dôkaz bol získaný v rozpore so zákonom, mohol by tento následne pripustiť len pokiaľ je právo protistrany v konkrétnom prípade ústavnokonformne posúdené ako silnejšie právo než porušené právo toho, na koho úkor sa právo vykonáva. Nezákonný dôkaz je v civilnom procese vyhodnocovaný prevažne ako procesne neprípustný. Dôvodom je postoj judikatúry k nezákonnému dôkazu ako k prostriedku, ktorý v spoločnosti podnecuje atmosféru podozrievavosti a nedôvery.¹²

Ak však kamerový záznam predstavuje dôkazný prostriedok získaný zákonným spôsobom, je potrebné si zodpovedať otázku, či by sa súd námietkou zamestnanca, že sa jedná o deepfake, mal zaoberať už na základe простého tvrdenia zamestnanca, alebo by takéto jeho tvrdenie malo byť riadne odôvodnené, prípadne podložené nejakými dôkazmi.

Prejednacia zásada ukladá účastníkom civilného súdneho konania povinnosť tvrdiť a preukazovať rozhodné skutočnosti (tzv. povinnosť tvrdenia a dôkazná povinnosť), prostredníctvom ktorých poskytujú súdu informácie potrebné pre rozhodnutie. Každé skutkové tvrdenie a každý navrhnutý dôkaz musí najprv vychádzať z vlastnej vedomosti účastníka o jeho existencii a obsahu.¹³ Domnievame sa, že námietka zamestnanca, ktorou spochybňuje autenticitu určitého dôkazného prostriedku, by mala byť kvalifikovaná, a teda mala by obsahovať najmenej uvedenie vlastných tvrdení o predmetných skutkových okolnostiach, napr. prečo kamerový záznam nie je, alebo nemôže byť autentický.

¹¹ Nález Ústavného súdu ČR z 9. decembra 2014, sp.zn.: II. ÚS 1774/2014

¹² IVANČO, M. Slabšia strana v kontexte procesnej prípustnosti nezákonného dôkazu. In *Mílniky práva v stredoeurópskom priestore 2017: zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov*. 2017, s. 289

¹³ MACUR, J.: Důkazní břemeno v civilním soudním řízení. Masarykova univerzita v Brně, 1995, s. 121 a nasl.

V súlade s platnou a účinnou právnou úpravou nemožno akceptovať prosté vyhlásenie, že kamerový záznam je deepfake, a teda súd musí od osoby, ktorá namieta autenticitu určitého dôkazného prostriedku, požadovať, aby táto uviedla aspoň základné oporné body toho, prečo tento kamerový záznam považuje za deepfake. *"V prípade, že strana zaťažená dôkazným bremenom prednesie aspoň „oporné body“ skutkového stavu a zvýši tak pravdepodobnosť svojich skutkových tvrdení, nastupuje „vysvetľovacia povinnosť“ protistrany. Nesplnenie tejto povinnosti bude mať za následok hodnotenie dôkazu v neprospech strany, ktorá "vysvetľovaciu povinnosť nesplnila". Zároveň tiež platí, že uvedenú "vysvetľovaciu povinnosť" nemožno zamieňať s obrátením dôkazného bremena."*¹⁴

Kamerové záznamy sú vo všeobecnosti považované za relevantné a dôveryhodné dôkazné prostriedky. Vidieť v zásade znamená veriť. Toto vnímanie je však narúšané rozmachom generatívnej umelej inteligencie, kedy je potrebné si akýkoľvek obsah, ktorý vnímame vlastnými zmyslami overovať a zisťovať jeho pôvod, nakoľko sa môže jednať o obsah, ktorý bol zmenený, alebo celkom vytvorený umelou inteligenciou a to, čo na takomto zázname vidíme sa nikdy nemuselo stať.

Dôkazné bremeno ohľadom určitých skutočností v zásade zaťažuje toho účastníka konania, ktorý z existencie týchto skutočností vyvodzuje pre seba priaznivé právne dôsledky; ide o toho účastníka, ktorý tiež existenciu takýchto skutočností tvrdí. V modelovom prípade teda existuje kamerový záznam zachytávajúci zamestnanca pri protiprávnom konaní, a to opakovane. Na druhej strane máme zamestnanca, ktorý pravosť takéhoto audiovizuálneho obsahu (kvalifikovane) spochybňuje a tvrdí, že sa jedná o deepfake.

V tomto prípade však zamestnanec objektívne nemá a nemôže mať k dispozícii relevantné informácie o skutočnostiach, významných pre rozhodnutie v spore, pričom zamestnávateľ takéto informácie k dispozícii môže mať.

Ako sme uvádzali, relevantným dôkazným prostriedkom na spochybnenie pravosti kamerového záznamu je odborné posúdenie, alebo znalecký posudok. Domnievame sa však, že v modelovom prípade by nebolo spravodlivé od zamestnanca požadovať, aby autenticitu kamerového záznamu preukazoval odborným posúdením, alebo znaleckým posudkom, a to najmä z dôvodu možných vysokých nákladov spojených s obstaraním takéhoto dôkazu. Zároveň, zamestnanec ako slabšia strana objektívne zrejme nemá možnosť zaobstarať si ani dôkazy o pôvode kamerového záznamu, nakoľko k týmto má prístup výlučne zamestnávateľ, resp. ním poverená tretia osoba. Ochrana zamestnancov proti svojvoľnému prepúšťaniu má základ v čl. 36 písm. b) Ústavy Slovenskej republiky. Základné práva a slobody sa pritom neuplatňujú len voči štátnym orgánom, ale aj v horizontálnych vzťahoch, keď pôsobia sprostredkované prostredníctvom podústavného práva, ktoré prežarujú (por. aj I. ÚS

¹⁴ Rozsudok Najvyššieho súdu SR z 11. apríla 2017, sp. zn. 3Cdo/2/2016

106/2016, bod 6). Všeobecné súdy majú povinnosť toto prežarovanie brať pri svojom rozhodovaní do úvahy tak, aby základné práva a slobody pri výklade a aplikácii práva chránili.¹⁵

Rovnako tak podľa nášho názoru nemožno uložiť povinnosť preukázať autentickosť kamerového záznamu prostredníctvom znaleckého posudku zamestnávateľovi.

Súd by však v modelovom prípade mohol uložiť zamestnávateľovi ako žalovanému povinnosť predložiť dôkazné prostriedky preukazujúce autenticitu kamerového záznamu, ako napríklad certifikáty, digitálne podpisy, povinnosť prehrať kamerový záznam priamo zo zariadenia, ktoré ho vytvorilo, a pod. Otázne však je, či a ako by sa súd s takýmito dôkaznými prostriedkami technického charakteru dokázal vysporiadať.

Okrem uvedeného súd môže uložiť zamestnávateľovi povinnosť predložiť čestné vyhlásenie, že kamerový záznam je autentický, alebo vykonať výsluch osoby zodpovednej za kamerové systémy.

Rovnako tak je možné uložiť zamestnávateľovi povinnosť predložiť aj ostatné dôkazy, ktoré súvisia s tvrdeným protiprávnym činom, a to napríklad listiny o stave zásob, škodové faktúry, dokumenty z inventúry, a pod.

Ak teda účastník konania vznesie námietku, že určitý dôkaz je deepfake, súd nie je viazaný výlučne otázkou autenticity daného dôkazného prostriedku. Súd môže nariadiť aj vykonanie ďalších dôkazov, ktoré môžu priamo alebo nepriamo potvrdiť alebo vyvrátiť skutkový stav, ku ktorému sa spochybnený dôkaz vzťahuje. Vykonaním takýchto ďalších dôkazov (napr. svedeckých výpovedí, listinných dôkazov) je možné overiť, či sa udalosť, ktorá je predmetom dokazovania, naozaj stala tak, ako to vyplývalo zo spochybneného kamerového záznamu. S ohľadom na charakter námietky (t.j. že sa jedná o audiovizuálny obsah, ktorý bol vytvorený generatívnou umelou inteligenciou, pričom posúdenie tejto otázky je otázkou vysoko odbornou) by však súd mal postupovať veľmi opatrne. Ako uvádza doc. Gešková, nemalo by ísť o pátranie po neznámych dôkazoch neurčiteľného rozsahu za účelom "vybudovania" prípadu. Preto by malo vždy ísť o konkrétne tvrdenia a o konkrétne dôkazy.¹⁶

Záver

Nakoľko v podmienkach Slovenskej republiky zatiaľ neevidujeme prípad, v ktorom sa súd musel vysporiadať s dôkazom, o ktorom účastník tvrdil, že je deepfake, nie je zatiaľ účelné, aby došlo k zmene právnej úpravy, nakoľko právne normy sa spravidla

¹⁵ Nález Ústavného súdu SR z 8.9.2020, č. k. III. ÚS 86/2020

¹⁶ Gešková, K. In: Števček, M., Ficová, S., Baricová, J., Mesiarkinová, S., Bajánková, J., Tomašovič, M., a kol. Civilný sporový poriadok. Komentár. Praha : C. H. Beck, 2016, s. 700

vytvárajú ako reakcia na nejakú opakujúcu sa situáciu, alebo za účelom regulovania určitej spoločenskej potreby.

Aj napriek tomu, že sa domnievame, že existujúce nástroje na overovanie autenticity dôkazov ako napríklad výsluch svedka, čestné vyhlásenie a pod. nie sú dostatočne spoľahlivé na odhaľovanie deepfakes, je zrejmé, že nie je hospodárne v každom jednotlivom prípade nariaďovať znalecké dokazovanie, prípadne vyžadovať od účastníka predloženie súkromného znaleckého posudku a že súd sa s takýmito dôkaznými prostriedkami musí vysporiadať na podklade existujúcej právnej úpravy. Ako sme naznačili, takéto vysporiadanie je možné napríklad prostredníctvom overenia, či predložený dôkazný prostriedok nemožno považovať za nezákonný, využívania doktríny vysvetľovacej povinnosti a uplatňovania sankcií za jej porušenie, dôsledného uplatňovania koncentračnej zásady, využívaním poriadkových pokút a pod.

Na základe vykonanej analýzy sme dospeli k overeniu hypotézy, ktorú sme si vymedzili v úvode tohto príspevku, a to, že súčasná právna úprava civilného procesu poskytuje dostatočné záruky pre spravodlivý súdny proces v ére generatívnej umelej inteligencie.

V nadväznosti na formulované overenie hypotézy však zároveň zdôrazňujeme potrebu otvorenia odbornej diskusie o problematike deepfakes a ich možného prieniku do súdnych konaní so zameraním sa na skúmanie, ako možno s touto hrozbou efektívne pracovať.

Nie je prehnané konštatovať, že sudcovia budú v nadchádzajúcom období čeliť výzve ako zabezpečiť spravodlivú a účinnú ochranu práv účastníkov konania bez toho, aby ich nad nevyhnutnú mieru zaťažovali. V tejto súvislosti je tiež vhodné zvážiť, či aktuálna výška poriadkovej pokuty, ktorú môže uložiť súd je dostatočná a nebolo by účelné pristúpiť k jej zvýšeniu. Súdby by v ére prenikania generatívnej umelej inteligencie do súdnych siení mali dôsledne sankcionovať konanie, alebo nekonanie, ktorým dochádza k sťaženiu postupu konania, a tým k jeho predĺženiu.

Zoznam použitej literatúry

1. BHATTATHIRI, A., SHARMA, F., PUROHIT, A.: Deepfake in the Courtroom: Legal Challenges and Evidentiary Standards.
2. Civilný sporový poriadok - Dôvodová správa
3. DELFINO, R.: Deepfakes on Trial: a Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery. In: Hastings Law Journal. 293 (2023). s. 293 - 348. Dostupné v: https://repository.uclawsf.edu/hastings_law_journal/vol74/iss2/3
4. DELFINO, R.: Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court. In: Loyola Law School,

Los Angeles: Legal Studies Research Paper č. 2025-10, Dostupné v: <https://ssrn.com/abstract=5188767> alebo <http://dx.doi.org/10.2139/ssrn.5188767>

5. IVANČO, M. Slabšia strana v kontexte procesnej prípustnosti nezákonného dôkazu. In Mílniky práva v stredoeurópskom priestore 2017: zborník z medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov. 2017, s. 289
6. JIRSA, J., HAVLÍČEK, K.: Dokazování – úvahy o teorii a praxi. 1. vydání. Praha: Wolters Kluwer ČR, 2021. 296 s. ISBN: 978-80-7676-102-5
7. LAVICKÝ, P.: Důkazní břemeno v civilním řízení soudním. Praha: Leges, 2017. 272 s. ISBN: 978-80-7502-203-5
8. LAVICKÝ, P. a kol. Moderní civilní proces. Brno: Masarykova univerzita, Právnická fakulta, 2014, s. 499. ISBN 978-80-210-7601-3
9. MACUR, J.: Dokazování a procesní odpovědnost v občanském soudním řízení. Brno: Universita J. E. Purkyně, 1984. 177 s. ISBN 55-024-84
10. MACUR, J.: Povinnost pravdivosti a její legislativní úprava v civilním soudním řádu. Právní rozhledy, ročník 1999, č. 4.
11. PFEFFERKORN, R.: "Deepfakes" in the courtroom. In: [Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020](https://ssrn.com/abstract=4321140). Dostupné v: <https://ssrn.com/abstract=4321140>
12. SMYČKOVÁ, R., ŠTEVČEK, M., LÖWY, A., TOMAŠOVIČ, T. a kol. Civilný mimosporový poriadok. Komentár. 2. vydanie. Bratislava: C. H. Beck, 2024. 1240 s. ISBN 978-80-8232-049-0
13. SVOBODA, K.: Dokazování. Praha: ASPI - Wolters Kluwer, 2009. 392 s. ISBN: 978-80-7357-414-7
14. ŠTEVČEK, M., FICOVÁ, S., BARICOVÁ, J., MESIARKINOVÁ, S., BAJÁNKOVÁ, J., TOMAŠOVIČ, M., a kol. Civilný sporový poriadok. Komentár. Praha: C. H. Beck, 2022. 1752 s. ISBN: 978-80-7400-909-9
15. WINTEROVÁ, A. a kol. Civilní právo procesní. 3. aktualizované vydání. Praha: Linde Praha, a.s., 2004. 691 s. ISBN: 978-80-7201-464-4

Súdne rozhodnutia

1. Nález Ústavného súdu SR z 8. septembra 2020, č. k. III. ÚS 86/2020
2. Nález Ústavného súdu ČR z 9. decembra 2014, sp.zn.: II. ÚS 1774/2014
3. Rozsudok Najvyššieho súdu SR z 11. apríla 2017, sp. zn. 3Cdo/2/2016
4. Uznesenie Najvyššieho súdu SR z 23. januára 2014, sp. zn. 3 Cdo 294/2012

Kontaktné údaje

Mgr. Lucia Mertl

mertl1@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

AI A HYPERTROFIA OBSAHU PODANÍ V CIVILNOM PROCESE: DÔSLEDKY PRE PRINCÍP PROCESNEJ EKONÓMIE A HOSPODÁRNOSTI KONANIA

AI AND THE HYPERTROPHY OF THE CONTENT OF SUBMISSIONS IN CIVIL PROCEEDINGS: IMPLICATIONS FOR THE PRINCIPLE OF PROCEDURAL ECONOMY AND EFFICIENCY OF PROCEEDINGS

Sandra Meňhartová¹

Abstrakt: Príspevok sa zameriava na analýzu fenoménu hypertrofie obsahu podaní v civilnom procese, ktorý je v aplikačnej praxi čoraz viac prítomný najmä v dôsledku expanzie nesprávneho a nekritického využívania dostupných systémov umelej inteligencie, ktorého výsledkom je koncepcia obsahovo rozsiahlych a neprehľadných podaní často s neovereným, generickým či redundantným obsahom. Cieľom príspevku je analyzovať dopady tohto fenoménu na jeden z ústavných princípov riadneho fungovania justície, ktorým je princíp procesnej ekonómie a hospodárnosti konania, ako aj navrhnúť možné spôsoby efektívnych procesných riešení a mechanizmov tohto problému, konštruované na základe racionálneho výkladu platnej a účinnej právnej úpravy Civilného sporového poriadku. Z metodologického hľadiska sú na naplnenie vymedzených cieľov v príspevku použité vedecké metódy analýzy, komparácie a syntézy. Záver príspevku predstavuje vymedzenie možných prístupov, z ktorých má personálny aspekt justičného aparátu možnosť vychádzať v prípade indikácie hypertrofie obsahu podania, a to s ohľadom na príklon k sociálnej koncepcii civilného procesu. Tá sa nevyhnutne spája s inštitútom postavenia silného sudcu, ako predstaviteľom autority dohliadajúcej nad dodržiavaním procesnej disciplíny strán sporu, resp. účastníkov konania.

Kľúčové slová: umelá inteligencia, podanie, civilný proces, princíp hospodárnosti konania

Abstract: The article focuses on analysing the phenomenon of hypertrophy of the content of submissions in civil proceedings, which is increasingly present in practice, mainly due to the expansion of the uncritical use of available artificial intelligence systems, resulting in the concept of content-rich and unclear

¹ Katedra občianskeho práva, Právnická fakulta Univerzity Komenského v Bratislave.

submissions, often with unverified, generic or redundant content. The aim of the paper is to analyse the impact of this phenomenon on one of the constitutional principles of the proper functioning of justice, namely the principle of procedural economy and efficiency, as well as to propose possible ways of effectively resolving this problem based on a rational interpretation of the valid and effective legal provisions of the Civil Procedure Code. From a methodological point of view, scientific methods of analysis, comparison and synthesis are used in the article to achieve the defined objectives. The conclusion of the paper presents a definition of possible approaches that the personnel aspect of the judicial system can use in cases of hypertrophy of the content of submissions, regarding the inclination towards the social concept of civil proceedings. This is inevitably linked to the institution of the position of a strong judge as a representative of the authority supervising compliance with procedural discipline by the parties to the dispute or participants in the proceedings.

Key words: artificial intelligence, submission, civil proceedings, principle of procedural economy

Úvod

Napriek skutočnosti, že dostupné systémy umelej inteligencie (ďalej len ako „AI“) predstavujú stále pomerne nový technologický nástroj, ich využívanie sa pri výkone jednotlivých právnych profesií stalo v pomerne krátkom čase už takmer „bežnou praxou“. V súčasnosti sa považuje za stabilizovaný názor, že AI má potenciál poskytovanie právnych služieb zefektívniť, a to najmä v súvislosti so spracovaním, vyhľadávaním a analýzou existujúceho množstva dát. Podporovanie využívania AI nepochybne nachádza svoje opodstatnenie tam, kde má potenciál subjekty realizujúce výkon právnych služieb v širokom spektre právnických profesií odbremeniť od rutinných úloh bez toho, aby bola narušená ich podstata.² Využívanie AI pri výkone jednotlivých právnych profesií však napriek tomu nepochybne prináša mnohé nové výzvy. Predkladaný príspevok *in genere* analyzuje problematiku využívania AI pri tvorbe a spracovaní právnych dokumentov – podaní v civilnom procese. *In concreto* sa zameriava na fenomén hypertrofie obsahu podaní v civilnom procese, ktorý je čoraz častejšie prítomný najmä v dôsledku zvýšenej frekvencie nevhodného spôsobu využívania AI. Cieľom predkladaného príspevku je analyzovať dôsledky fenoménu vymedzeného *ut supra* na jeden z ústavných princípov riadneho

² Umelá inteligencia má potenciál zefektívniť právne služby. Najvyšší súd Slovenskej republiky. [online] [cit. 2025-09-22]. Dostupné na: <https://www.nsud.sk/umela-inteligencia-ma-potencial-zefektivnit-pravne-sluzby/>.

fungovania justície, ktorým je princíp procesnej ekonómie a hospodárnosti konania, ako aj navrhnúť možné spôsoby efektívnych procesných riešení tohto problému konštruované na základe racionálneho výkladu platnej a účinnej právnej úpravy – zákona č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších predpisov (ďalej len ako „Civilný sporový poriadok“ alebo „CSP“) V tejto súvislosti považujeme za nevyhnutné bližšie vymedziť dva základné inštitúty vyplývajúce už zo samotného názvu príspevku, ktorými sú:

1. *AI ako systém a*
2. *hypertrofia obsahu podania.*

AI ako systém

Systém AI, *ergo* systém umelej inteligencie (z ang. „*artificial intelligence*“) možno definovať rôzne. V AI je agent počítačový program alebo systém, ktorý je navrhnutý tak, aby vnímal svoje prostredie, rozhodoval sa a vykonával činnosti na dosiahnutie konkrétneho cieľa alebo súboru cieľov. Agent pracuje autonómne, čo znamená, že nie je priamo riadený ľudským operátorom.³ Z hľadiska európskej legislatívy však možno v súčasnosti za najrelevantnejšiu označiť definíciu AI vyplývajúcu z čl. 3 ods. 1 už takmer notoricky známeho Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2024/1689 z 13. júna 2024⁴, ktorým sa stanovujú harmonizované pravidlá umelej inteligencie, a to v nasledovnom znení: „...systém AI“ je *strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie;...*⁵

V tejto súvislosti je nevyhnutné zdôrazniť, že AI predstavuje algoritmický systém a nie samostatne mysliaci subjekt. Nemožno ho preto, a to vo vzťahu k obsahovo hypertrofovaným podaniam v civilnom procese generálne demonizovať. Naopak, napriek výzvam, ktoré možno vo vzťahu k AI v civilnom procese identifikovať, hoci len izolovane, možno tento nástroj, ako aj jeho využívanie legitímne považovať v mnohých aspektoch za prospešné, a to práve v súvislosti

³ MESARČÍK, Matúš, GYURÁSZ, Zoltán. a kol.: Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 1. K definícii AI pozri aj RUSSEL, Stuart, NORVIG, Peter: Artificial Intelligence: A Modern Approach (4th Edition). Pearson 2020, s. 669.

⁴ Nariadenie je známe aj pod všeobecne zastrešujúcim označením „Akt o umelej inteligencii“, resp. ako ang. „AI Act“.

⁵ Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá umelej inteligencie. [online] [cit. 2025-09-22] Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689>

s princípom procesnej ekonómie a hospodárnosti konania. Negatívne dôsledky prejavujúce sa *inter alia* v náraste množstva obsahovo hypertrofovaných podaní v civilnom procese nemožno pripísať existencii systému AI *per se* a ani dostupnej možnosti využívania AI. K negatívnym dôsledkom dochádza podľa nášho názoru výlučne v súvislosti s nevhodnou voľbou spôsobu využívania AI, ktorý je výsostne determinovaný ľudským faktorom. V kontexte podaní v civilnom procese teda tým ako je s AI ako nástrojom narábané zo strany strán sporu resp. zo strany účastníkov konania či zo strany ich zástupcov.

Hypertrofia obsahu podania

In genere možno konštatovať, že samotný fenomén tzv. hypertrofie obsahu podaní v civilnom procese nemožno z hľadiska aplikačnej praxe označiť za novum. Hypertrofované podania z hľadiska svojho obsahu boli známe už dávno pred „érou“ umelej inteligencie. Domnievame sa však, že rozdiel oproti súčasnosti spočíva v tom, že AI postup pri ich koncepcii dramaticky sprístupňuje, *ergo* zjednodušuje a urýchljuje.⁶ Na účely predkladaného príspevku je potrebné uviesť, že podanie, ktorého obsah je hypertrofovaný spĺňa všetky zákonné predpoklady vo vzťahu k obsahovým náležitostiam⁷. V načrtnutom kontexte je potrebné osobitne zdôrazniť, že pri hypertrofii obsahu podaní v civilnom procese nemáme na mysli iba samotnú dĺžku koncipovaného textu, ktorý je obsahom *e. g.* žaloby ako podania vo veci samej v civilnom sporovom konaní vedenom v zmysle ustanovení zákona – Civilného sporového poriadku. Pod označením „*hypertrofia obsahu podania*“ rozumieme neprimerané rozšírenie textu podania nad rámec jeho racionálneho rozsahu potrebného na dosiahnutie požadovaného účelu. Pomerne častým javom súvisiacim s hypertrofiou obsahu podaní sú redundantné pasáže, rozsiahle citácie právnej úpravy s absenciou vlastnej právnej analýzy či rozsiahle citácie judikatúry, ktorej skutočná existencia nie je zo strany subjektu realizujúceho podanie často vôbec overená. V tejto súvislosti tiež možno poukázať na často vyskytujúce sa textové pasáže, ktoré sú do textu vložené hoci z hľadiska obsahu možno na prvý pohľad konštatovať, že nemajú žiadnu relevanciu a predstavujú iba akýsi „balast“. Dochádza tak k navodeniu ilúzie, že „objem podania predstavuje zároveň jeho silu“. Z uvedených dôvodov si tak v tejto súvislosti označenie „hypertrofia obsahu

⁶ Podľa V. Horu je pohnútkou procesných úkonov strany sporu rýdzi egoizmus, ktorého účelom je dosiahnutie rozhodnutia pre stranu priaznivého, kdežto pohnútkou a zároveň účelom procesných úkonov súdu je jedine a výlučne snaha dospieť k spravodlivému rozhodnutiu. K tomu pozri HORA, Václav: Procesní úkony dle práva rakouského. Praha : Sborník věd právních a státních., 1907, s. 4.

⁷ V tejto súvislosti poukazujeme *e. g.* na ustanovenie § 127 CSP vymedzujúce všeobecné náležitosti podania, ustanovenie § 132 CSP vymedzujúce osobitné náležitosti žaloby, ustanovenie § 326 CSP vymedzujúce náležitosti neodkladného opatrenia či ustanovenie § 363 CSP vymedzujúce náležitosti odvolania *etc.*

podania“ nemožno zamieňať s dôkladnosťou podania, naopak, na účely predkladaného príspevku toto označenie chápeme výlučne v negatívnom zmysle slova.

Dôsledky hypertrofie obsahu podania v aplikačnej praxi

Z hľadiska aplikačnej praxe možno pozorovať dôsledky stále častejšie sa vyskytujúcej hypertrofie obsahu podaní v civilnom procese najmä nie však výlučne na základe nevhodného využívania AI na dvoch základných úrovniach:

Ad 1) Na úrovni súdov

Na úrovni súdov možno dôsledky tohto fenoménu pozorovať najmä v súvislosti so zvýšenou záťažou personálneho aspektu justičného aparátu, *ergo* najmä zvýšenou záťažou sudcov a vyšších súdnych úradníkov. Táto zvýšená záťaž sa prejavuje na dvoch subúrovniah ako:

- záťaž kognitívna a
- záťaž časová.

Zvýšenie kognitívnej záťaže sa spája s potrebou analýzy neprimeraného a neštandardného množstva textu za účelom selekcie relevantného obsahu podania od balastu. Zo zvýšenia kognitívnej záťaže tak logicky vyplýva aj zvýšená časová záťaž.

Ad 2) Na úrovni strán sporu, resp. na úrovni účastníkov konania a ich zástupcov

Na úrovni strán sporu, resp. na úrovni účastníkov konania a ich zástupcov možno v súvislosti s hypertrofiou obsahu podaní pozorovať istý tlak vedúci k snahe reagovať na všetky skutočnosti uvedené v podaní protistrany, hoci ide o pasáže, ktoré samé o sebe zrejme nie sú relevantné. Podliehanie tomuto tlaku logicky vedie k umelému nafukovaniu spisového materiálu, tzv. „zahlcovaniu spisu“, časovej záťaži pri jeho analýze a tým aj zvyšovaniu nákladov spojených so zabezpečením efektívnej procesnej obrany.

Na úrovni systému civilného procesu vedú uvedené aspekty spoločne k predlžovaniu konaní, k zahlcovaniu spisu a vytváraniu rámca pre možné obštrukčné procesné taktizovanie, ktoré označujeme ako „torpédový efekt hypertrofovaných podaní“⁸. Vymedzené dôsledky priamo kolidujú s princípom procesnej ekonómie a hospodárnosti konania. Z uvedeného dôvodu je nevyhnutné položiť si otázku, či *de lege lata* existujú procesné nástroje a mechanizmy na zamedzenie negatívnych dôsledkov hypertrofie obsahu podaní v civilnom procese, ktoré sú, opätovne uvádzame, identifikované najmä avšak nie výlučne v súvislosti s nevhodným využívaním AI.

⁸ Pri návrhu označenia vymedzenej obštrukčnej procesnej taktiky sa autorka nechala inšpirovať inštitútom tzv. torpédových žalôb.

Procesné nástroje a mechanizmy slúžiace na zamedzenie negatívnych dôsledkov spojených s hypertrofiou obsahu podaní v civilnom procese

V teórii civilného práva procesného sú už tradične podania v civilnom procese diferencované do dvoch základných kategórií, ktorými sú *podania vo veci samej* a *podania iné ako vo veci samej, resp. iné podania*.⁹ V nadväznosti na uvedenú diferenciáciu sa pokúsime formulovať dve osobitné vetvy možných procesných nástrojov a mechanizmov na riešenie, resp. elimináciu vymedzeného negatívneho fenoménu:

Ad 1) Podania iné ako vo veci samej

V zmysle ustanovenia § 128 ods. 1 CSP platí, že ak „...z podania nie je zrejmé, čoho sa týka a čo sa ním sleduje, vyzve súd na doplnenie alebo opravu tohto podania“. Hoci sa v kontexte citovaného znenia ustanovenia § 128 ods. 1 CSP môže na základe jazykového výkladu na prvý pohľad zo slova „doplnenie“, resp. „oprava“ zdať, že podanie, z ktorého nie je zrejmé, čoho sa týka a čo sa ním sleduje je obsahovo informačne poddimenzované, domnievame sa, že uvedená charakteristika sa môže rovnako vzťahovať aj na podanie, ktoré je obsahovo hypertrofované hoci paradoxne, informácií v ňom bude naopak možno až príliš mnoho.¹⁰ Procesný nástroj, resp. mechanizmus smerujúci k dodržiavaniu princípu procesnej ekonómie a hospodárnosti konania je podľa nášho názoru v tejto súvislosti pomerne jednoznačný a vyplýva z ustanovenia § 128 ods. 3 CSP, v zmysle ktorého platí, že: „Ak sa v lehote určenej súdom podanie nedoplní alebo neopraví, prípadne sa doplní alebo opraví tak, že z neho nie je zrejmé, čoho sa týka a čo sa ním sleduje, na také podanie súd neprihliada.“ Z citovaného ustanovenia tak vyplýva nasledovný možný procesný postup. Súd po doručení podania iného ako vo veci samej a po identifikácii, že ide o obsahovo hypertrofované podanie, z ktorého mu nie je zrejmé čoho sa týka a čo sa ním sleduje, vyzve na opravu tohto podania v lehote, ktorá nemôže byť kratšia ako

⁹ Pre celistvosť výkladu v tejto súvislosti uvádzame, že právna doktrína Slovenskej republiky v súčasnosti diferencuje podania do dvoch základných skupín, a to podania vo veci samej a podania iné ako vo veci samej. K tomu pozri ŠTEVČEK, Marek a kol.: Civilné právo procesné. Úvod do civilného procesu a sporové konanie. Praha : C. H. Beck, 2022, s. 224 ako aj ŠTEVČEK, Marek, STRAKA, Richard a kol. Prednášky a texty z civilného procesu. Skriptá. 2. vydanie. Bratislava : C. H. Beck, 2018, s. 47. Staršia procesualistická literatúra, toto delenie nerozlišuje rovnako tak ani súčasná právna doktrína Českej republiky. K tomu pozri MAZÁK, Ján, JÁNOŠÍKOVÁ, Martina. Učebnica občianskeho procesného práva. Bratislava : IURIS LIBRI, 2012, s. 113 a WINTEROVÁ, Alena, MACKOVÁ, Alena a kol. Civilní právo procesní. Část první: řízení nalézací. 8. nezmenené vydání. Praha : Leges, 2015, s. 182 a 183. Rakúska republika pristupuje k odlišnej diferenciácii procesných úkonov strán sporu, a to tzv. nem. Parteiprozesshandlungen vor Gericht a tzv. nem. Außergerichtliche Parteiprozesshandlungen. Bližšie pozri RECHBERGER, Walter, SIMOTTA, Daphne-Ariane. Grundriss des Österreichischen Zivilprozessrechts. Wien : Manz, 2017, s. 363 – 364.

¹⁰ K problematike opravy či doplnenia podania pozri aj HORA, Václav.: Československé civilní právo procesní II. Praha : Všehrad, 1932, reedícia Praha : Wolters Kluwer, 2010, s. 140 – 141.

desať dní. Pokiaľ podanie nebude opravené vôbec, resp. bude opravené, ale naďalej z neho nebude zrejmé čoho sa týka a čo sa ním sleduje – v tomto kontexte možno zrejme hovoriť o jeho redukcii vo vzťahu k nadmerným pasážam, súd naň nebude prihliadať. Doplneniu podania v tomto kontexte nie je podľa nášho názoru potrebné osobitne venovať pozornosť, je tomu tak z dôvodu, že pri hypertrofii obsahu podania bude, naplnený predpoklad vymedzenia obsahových náležitostí podania, tie sa však budú v množstve textu strácať.¹¹

Ad 2) Podania vo veci samej

V zmysle ustanovenia § 129 ods. 1 CSP platí, že: „*Ak ide o podanie vo veci samej alebo návrh na nariadenie neodkladného opatrenia alebo zabezpečovacieho opatrenia, z ktorého nie je zrejmé, čoho sa týka a čo sa ním sleduje, alebo ide o podanie neúplné alebo nezrozumiteľné, súd vyzve toho, kto podanie urobil, aby podanie doplnil alebo opravil v lehote, ktorá nemôže byť kratšia ako desať dní.*“ Súd má v zmysle ustanovenia § 129 ods. 2 CSP povinnosť uviesť v čom konkrétne považuje podanie za neúplné alebo nezrozumiteľné a ako ho treba doplniť alebo opraviť, pričom stranu poučí o možnosti toto podanie odmietnuť. Domnievame sa, že k podobnému záveru, aký podľa nášho názoru umožňuje jazykový výklad ustanovenia § 128 CSP nebude možné dospieť na základe jazykového výkladu ustanovenia § 129 CSP, teda v prípadoch, kedy pôjde o hypertrofiu obsahu podania vo veci samej, neodkladného alebo zabezpečovacieho opatrenia, a to s ohľadom na ustanovenie § 129 ods. 3 CSP, *in concreto* vety za stredníkom v znení: „...to neplatí, ak pre uvedený nedostatok možno v konaní pokračovať.“ Domnievame sa, že hypertrofia obsahu podania vo veci samej či neodkladného alebo zabezpečovacieho opatrenia, v zmysle jazykového výkladu zrejme nezakladá nedostatok spočívajúci v nemožnosti pokračovania v konaní odôvodňujúci odmietnutie takého podania. Vychádzame pri tom zo skutočnosti, že obsahovo hypertrofované podanie sme na účely predkladaného príspevku vymedzili ako podanie spĺňajúce všetky zákonom požadované obsahové náležitosti. Domnievame sa, že podanie vo veci samej, z ktorého pre jeho hypertrofovaný obsah nie je zrejmé čoho sa týka, resp. čo sa ním sleduje, resp. nie je zrozumiteľné, nebude možné odmietnuť, naopak, súd sa ním na základe jazykového výkladu bude musieť zaoberať hoci to nebude v súlade s princípom procesnej ekonómie a hospodárnosti konania. Ustanovenie § 129 CSP je v tejto súvislosti potrebné vykladať v spojení s ustanovením § 150 ods. 1 CSP, v zmysle ktorého platí, že: „*Strany majú povinnosť pravdivo a úplne uvádzať podstatné a rozhodujúce skutkové tvrdenia týkajúce sa sporu.*“ V uvedenom kontexte je z hľadiska citovaného ustanovenia potrebné poukázať

¹¹ K tomu pozri aj ZÁHRADNÍKOVÁ, Radka. § 128 [Odstraňovanie väd podania, ktoré nie je podaním vo veci samej]. In: ŠTEVČEK, Marek, FICOVÁ, Svetlana, BARICOVÁ, Jana, MESIARKINOVÁ, Soňa, BAJÁNKOVÁ, Jana, TOMAŠOVIČ, Marek a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022, s. 506.

najmä na povinnosť uvádzania podstatných a rozhodujúcich skutkových tvrdení týkajúcich sa sporu, nakoľko hypertrofia obsahu podania sa v kontexte predkladaného príspevku viaže najmä na uvádzanie nadmerného množstva *de facto* irelevantných, prípadne duplicitných informácií¹². *Ergo*, ak túto povinnosť strany sporu nedodržia a v podaní uvedú množstvo skutočností takpovediac vo vzťahu k meritu veci materiálne irelevantných, súd by mal uložiť poriadkovú pokutu v zmysle ustanovenia § 102 ods. 1 CSP, a to aj opakovane. V tejto súvislosti nevidíme priestor pre aplikáciu ustanovenia § 191 ods. 1 CSP *in concreto* veta za stredníkom, ktoré v civilnom procese budovanom na koncepcii „silného sudcu“ poskytuje manévrovací priestor umožňujúci sudcovi zamietnutie žaloby. Je tomu tak z dôvodu, že na aktiváciu uvedeného procesného mechanizmu by muselo byť v podaní indikované nepravdivé skutkové tvrdenie, inými slovami „klamstvo“ strany sporu.¹³ Uloženie poriadkovej pokuty hoci aj opakovane však nemusí byť dostatočným procesným nástrojom, a to najmä vzhľadom na jej výšku, ktorá nemusí mať v každom prípade odstrašujúci charakter.

Domnievame sa však, že za pomoci aplikácie nie jazykového, ale teleologického výkladu možno dospieť k záveru, že hypertrofia obsahu podania vo veci samej, resp. neodkladného alebo zabezpečovacieho opatrenia môže viesť po dodržaní zákonom stanoveného postupu vymedzeného ustanovením § 129 CSP k odmietnutiu tohto podania. Argumentov pre naše tvrdenie predostrieme hneď niekoľko. Realizácia podania, ktoré je obsahovo hypertrofované vedie z hľadiska princípu procesnej ekonomie a hospodárnosti konania *de facto* k obdobnému efektu, ako je tomu v prípade realizácie podania – eg. žaloby, v ktorej absentuje úplné opísanie rozhodujúcich skutočností. Aj v takom prípade totiž súd má problém jednoznačne identifikovať čo je meritórnym jadrom sporu. V oboch prípadoch, teda tak pri hypertrofii obsahu podania ako aj pri absencii požadovaných náležitostí sa tak míňa účelu, ktorý je sledovaný procesným právom, a to umožniť rýchle a hospodárne vyriešenie veci. Strana, ktorá predkladá podanie, ktorého obsah je hypertrofovaný síce formálne využíva svoje dispozičné právo, ale spôsobom, ktorý nekorešponduje s jeho účelom. Cieľom subjektu realizujúceho takéto podanie prestáva byť uplatnenie svojho dispozičného práva za účelom zabezpečenia rýchlej a účinnej ochrany svojich narušených subjektívnych práv, resp. právom chránených záujmov, ale uplatnenie dispozičného práva, ktoré je, naopak, v rozpore s jeho primárnym účelom. Navyše,

¹² K obsahovému vymedzeniu inštitútu „hypertrofia obsahu podaní“ bližšie pozri výklad *ut supra* v podkapitole s názvom *Hypertrofia obsahu podaní*.

¹³ V kapitole s názvom *Hypertrofia obsahu podaní* uvádzame, že na účely predkladaného príspevku podanie, ktorého obsah je hypertrofovaný spĺňa všetky zákonné predpoklady vo vzťahu k obsahovým náležitostiam. *E. g.* vo vzťahu k podaniu vo veci samej – žalobe tak v zmysle ustanovenia § 132 CSP pôjde o splnenie náležitosti uvádzať pravdivé a úplné opísanie rozhodujúcich skutočností. K tomu pozri aj ustanovenie § 326 CSP.

ak je uvedená snaha dôsledkom obštrukčnej procesnej taktiky, je teda cielená a účelová, ide o zjavné zneužitie procesných práv, ktoré nepožíva právnu ochranu a v zmysle čl. 5 CSP môže súd takýto procesný úkon odmietnuť resp. ho sankcionovať, ak vedie k nedôvodnému prietahu v konaní. Na základe uvedenej analýzy tak možno konštatovať, že Civilný sporový poriadok ako stále pomerné nový procesný kódex disponuje *de lege lata* dostatočne efektívnymi procesnými nástrojmi a mechanizmami na zamedzenie negatívnych dôsledkov tzv. torpédového efektu obsahovo hypertrofovaných podaní v civilnom procese.

Záver

Hypertrofia obsahu podaní v civilnom procese jednoznačne predstavuje negatívny fenomén. Hoci je potrebné konštatovať, že tento negatívny fenomén nie je vo svojej celistvosti dôsledkom existencie AI, naopak, existoval už dávno pred jej nástupom, v aplikačnej praxi možno v poslednom období práve v dôsledku AI vnímať zvýšenú frekvenciu jeho výskytu. Ten nemusí byť vždy nevyhnutne spojený s procesnou obštrukciou, ktorú sme označili ako tzv. torpédový efekt obsahovo hypertrofovaných podaní, či už v spojení s AI alebo bez nej, teda nemusí byť automaticky považovaný za zjavné zneužitie procesných práv v zmysle čl. 5 CSP. Naopak, môže ísť aj o vedľajší efekt rozsiahleho výskytu laického prvku v civilnom procese, prípadne môže ísť výkon právnej služby nižšej kvality. Tak či onak, predstavuje hypertrofia obsahu podaní v civilnom procese nežiaducu procesnú deformáciu. Uvedomujeme si pritom, že v aplikačnej praxi bude hranica odôvodňujúca príklon k možnosti neprihliadať, resp. odmietnuť podanie z uvedených dôvodov často veľmi nevýrazná a ťažko identifikovateľná. Javí sa však ako legitímne, aby sudca, disponoval silnými procesnými nástrojmi a mechanizmami, a to za účelom zabezpečenia realizácie princípu procesnej ekonómie a hospodárnosti konania, ktorý nie je len jedným z podmnožiny ústavných princípov riadneho fungovania justície, ale aj jedným z východiskových princípov, na ktorých je budovaná sociálna koncepcia civilného procesu spojená s postavením tzv. silného sudcu.

Zoznam použitej literatúry

1. HORA, Václav.: Československé civilní právo procesní II. Praha : Všehrd, 1932, reedícia Praha : Wolters Kluwer, 2010, 956 s. ISBN: 97-807-35-754-03
2. HORA, Václav: Procesní úkony dle práva rakouského. Praha : Sborník věd právních a státních., 1907. 95 s. ISBN: neuvedené
3. MAZÁK, Ján, JÁNOŠÍKOVÁ, Martina. Učebnica občianskeho procesného práva. Bratislava : IURIS LIBRI, 2012, 820 s. ISBN: 978-80-89635-00-9

4. MESARČÍK, Marián., GYURÁSZ, Zoltán. a kol. Právo a umelá inteligencia. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 242 s. ISBN: 978-80-7160-715-1
5. RECHBERGER, Walter, SIMOTTA, Daphne-Ariane. Grundriss des Österreichischen Zivilprozessrechts. 9. Auflage. Wien : Manz, 2017. 880 s. ISBN: 978-3-214-00780-5
6. RUSSELL, Stuart, NORVIG, Peter. Artificial Intelligence: A Modern Approach . 4th Edition. Pearson, 2020. 1136 s. ISBN 978-0134610993
7. ŠTEVČEK, Marek, STRAKA, Richard a kol. Prednášky a texty z civilného procesu. Skriptá. 2. vydanie. Bratislava : C. H. Beck, 2018. 188. s. ISBN: 978-80-89603-65-7
8. ŠTEVČEK, Marek a kol.: Civilné právo procesné. Úvod do civilného procesu a sporové konanie. Praha : C. H. Beck, 2022. 632 s. ISBN: 978-80-7400-876-4
9. ŠTEVČEK, Marek, FICOVÁ, Svetlana, BARICOVÁ, Jana, MESIARKINOVÁ, Soňa, BAJÁNKOVÁ, Jana, TOMAŠOVIČ, Marek a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022. 1752 s. ISBN: 978-80-7400-909-9
10. Umelá inteligencia má potenciál zefektívniť právne služby. Najvyšší súd Slovenskej republiky. [online] [cit. 2025-09-22]. Dostupné na: <https://www.nsud.sk/umela-inteligencia-ma-potencial-zefektivnit-pravne-sluzby/>.
11. WINTEROVÁ, Alena, MACKOVÁ, Alena a kol. Civilní právo procesní. Část první: řízení nalézací. 8. nezmenené vydání. Praha : Leges, 2015. 624 s. ISBN: 978-80-7502-076-5

Kontaktné údaje

Mgr. Sandra Meňhartová, PhD.

sandra.menhartova@flaw.uniba.sk

Katedra občianskeho práva, Právnická fakulta Univerzity Komenského v Bratislave

PRÁVO DIEŤAŤA NA SÚKROMIE A DIGITÁLNY DOHĽAD RODIČOV¹

A CHILD'S RIGHT TO PRIVACY AND DIGITAL PARENTAL SUPERVISION

Lenka Dufalová²

Abstrakt: Príspevok sa venuje právu dieťaťa na súkromie v digitálnom prostredí so zreteľom na rodičovskú kontrolu realizovanú prostredníctvom moderných technológií. Primárnym cieľom príspevku je preskúmať právny rámec ochrany súkromia detí a analyzovať, do akej miery sú rodičia oprávnení monitorovať online aktivity svojich detí s ohľadom na výkon rodičovských práv a povinností. Metodologicky sa príspevok opiera o analýzu práv dieťaťa rodičov najmä Dohovoru o právach dieťaťa, o hodnotenie aktuálnych prístupov rodičovskej kontroly v digitálnej praxi, ako aj o možnosti dieťaťa brániť sa proti excesívnej kontrole zo strany rodičov. Výsledky skúmania poukazujú na potrebu vyvažovania medzi autonómiou dieťaťa a právom rodiča vykonávať dohľad, pričom osobitný dôraz kladie na zásadu proporcionality. Vedecký prínos príspevku spočíva v prehĺbení diskusie o interpretácii práva dieťaťa na súkromie v digitálnom kontexte a v objasnení jeho hraníc. Praktický prínos možno vidieť v odporúčaníach pre nastavenie primeraných foriem rodičovskej kontroly, ktoré podporujú digitálnu bezpečnosť dieťaťa bez neodôvodneného zásahu do jeho autonómie.

Kľúčové slová: dieťa, právo na súkromie, výchova a ochrana, digitálny dohľad

Abstract: The paper addresses the child's right to privacy in the digital environment with regard to parental control implemented through modern technologies. The primary objective of this paper is to examine the legal framework for the protection of children's privacy and to analyze the extent to which parents are authorized to monitor their children's online activities, considering the exercise of parental rights and responsibilities. Methodologically, the paper is based on the analysis of children's rights, especially the Convention on the Rights of the Child, an evaluation of current

¹ Tento článok vznikol v rámci projektu APVV-23-0181 Klinické a právne aspekty sebapoškodzovania v adolescencii

² Univerzita Komenského v Bratislave, Právnická fakulta

approaches to parental control in digital practice, and the child's options for defending against excessive parental surveillance. The research findings highlight the need to balance the child's autonomy and the parent's right to supervise, with a particular emphasis placed on the principle of proportionality. The scientific contribution of the work lies in deepening the discussion on the interpretation of the child's right to privacy in the digital context and in clarifying its boundaries. The practical contribution can be seen in the recommendations for setting appropriate forms of parental control that support the child's digital safety without unwarranted interference with their autonomy.

Key words: hild, right to privacy, upbringing and protection, digital control

Úvod

Právo v súčasnosti vníma dieťa ako samostatný subjekt práva, nie ako jeho objekt. Táto základná axióma reflektuje posun v chápaní postavenia dieťaťa v právnom poriadku, ktorý sa postupne presadzoval v priebehu 20. storočia pod vplyvom medzinárodných ľudsko-právnych dokumentov a meniacej sa podoby rodiny a rodinného práva. Kým v minulosti bolo dieťa vnímané predovšetkým ako adresát rodičovskej starostlivosti a ochrany, v súčasnosti právo uznáva jeho autonómiu a priznáva mu osobitné základné práva, medzi ktoré patrí aj právo na súkromie. Tento prístup vychádza predovšetkým z **Dohovoru o právach dieťaťa (ďalej aj ako „Dohovor“)**, prijatom Valným zhromaždením OSN v roku 1989, ktorý Slovenská republika ratifikovala v roku 1993. Dohovor definuje dieťa hneď v článku 1: *„za dieťa považuje každá ľudská bytosť mladšia než 18 rokov, ak podľa právneho poriadku, ktorý sa vzťahuje na dieťa, nie je dospelosť dosiahnutá skôr ako každú ľudskú bytosť mladšiu ako 18 rokov“* a priznáva mu široké spektrum práv. Do dovŕšenia plnoletosti má fyzická osoba postavenie maloletého dieťaťa a právny poriadok jej zaručuje osobitnú ochranu.³

Súkromie jednotlivca je spolu s nedotknuteľnosťou fyzickej osoby a rodinným životom v zmysle čl. 16 ods. 1 a čl. 19 ods. 2 Ústavy SR č. 460/1992 Zb. v znení neskorších predpisov predovšetkým základným ľudským právom, ktoré je chránené taktiež mnohými medzinárodnými dokumentmi, ktorými je Slovenská republika

³ ČÍPKOVÁ, Tamara: Informovaný súhlas pri poskytovaní zdravotnej starostlivosti maloletému dieťaťu. In: Postavenie transrodových ľudí na Slovensku [elektronický dokument] : interdisciplinárne pohľady. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022, s. 194. ISBN 978-80-7160-661-1.

viazaná.⁴ Právo na ochranu súkromia má každá fyzická osoba, dieťa nevynímajúc. Práve naopak – dieťa ako subjekt, ktorému je potrebné poskytnúť zvýšenú právnu ochranu, má toto právo explicitne garantované aj Dohovorom.

Právo na súkromie získava v digitálnej ére nové rozmery, ktoré si vyžadujú osobitnú pozornosť zo strany štátu, rodičov, škôl aj technologických spoločností. Digitálne technológie sú základom života detí doma, v škole aj inde. Hoci sľubujú dostatok príležitostí na učenie, komunikáciu a hru, potreby a záujmy detí nie sú dostatočne zastúpené v politikách, dizajne a vývoji dnešného digitálneho prostredia.⁵ Digitálne technológie, sociálne siete, mobilné aplikácie a online komunikácia vytvárajú prostredie, v ktorom je súkromie detí vystavené novým formám rizika. Deti zanechávajú digitálne stopy často bez pochopenia dôsledkov zdieľania osobných údajov, fotografií či polohy. Zároveň môžu byť vystavené monitorovaniu zo strany rodičov, škôl, ale aj komerčných subjektov, ktoré zhromažďujú osobné údaje za rôznym účelom.

Za účelom ochrany detí pred nevhodným obsahom, kyberšikanou, online manipuláciou či kontaktom s neznámymi osobami sú vyvíjané rôzne softvérové riešenia a aplikácie, ktoré umožňujú monitorovanie a obmedzenie online aktivít detí. Ide napríklad o rodičovské zámky, filtre obsahu, sledovanie polohy, časové obmedzenia používania zariadení či kontrolu nad inštaláciou aplikácií. Tieto nástroje môžu byť užitočné pri prevencii rizikového správania, no zároveň otvárajú otázku, do akej miery zasahujú do práva dieťaťa na súkromie.

Príspevok analyzuje právo dieťaťa na súkromie a možné zásahy do súkromia dieťaťa zo strany rodičov prostredníctvom nástrojov digitálneho dohľadu. Rodič, ako osobná zodpovedná za výchovu, vývin a blaho dieťaťa je oprávnený používať primerané prostriedky na dosiahnutie tohto účelu, avšak za súčasného rešpektovania práv dieťaťa, ktoré má garantované medzinárodnými, aj vnútroštátnymi právnymi normami. Príspevok popisuje rôzne funkcie nástrojov rodičovského dohľadu, ako aj riziká ich používania s dôrazom na vzťah rodič – dieťa. Taktiež analyzuje možnosti dieťaťa brániť sa voči neprimeranej rodičovskej kontrole, ktoré mu v súčasnosti poskytuje slovenská právna úprava. Ide o otázku pomerne komplikovanú, preto nie je cieľom príspevku poskytnúť vyčerpávajúce odpovede na nastolené otázky, či problémy. Cieľom príspevku je načrtnúť základné otázky, problémy a návrhy riešení ako základ pre rozvoj ďalšej diskusie nielen v teoretickej, ale aj aplikačnej rovine.

⁴ HAMŘIK, Martin: Paternalizmus v konflikte rodičovských práv a práva na súkromie maloletého so zameraním na rodovú identitu. In: Quo vadis postavenie transrodových ľudí na Slovensku? 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2023, s. 7. ISBN 978-80-7160-707-6.

⁵ LIVINGSTONE, Sonia - POTHONG, Kruakae: *Child rights impact assessment: a policy tool for a rights-respecting digital environment*. In: Policy and Internet, roč. 17, č. 3 (2025), s. 1. <https://doi.org/10.1002/poi3.70008>

Právo dieťaťa na súkromie

Právo dieťaťa na súkromie predstavuje esenciálnu zložku jeho osobnosti. Rešpektovanie súkromného života dieťaťa je nevyhnutné pre jeho zdravý vývin – emocionálny, sociálny aj morálny a umožňuje dieťaťu rozvíjať vlastnú individualitu, vnútorný svet, osobné vzťahy a slobodu rozhodovania bez neprimeraných vonkajších zásahov. Dohovor zakotvuje právo dieťaťa na súkromie v článku 16: *1. Žiadne dieťa nesmie byť vystavené svojvoľnému zasahovaniu do svojho súkromného života, rodiny, domova alebo korešpondencie ani nezákonným útokom na svoju česť a povesť. 2. Dieťa má právo na zákonnú ochranu proti takým zásahom alebo útokom.* Toto ustanovenie sa aplikuje na všetky sféry života dieťaťa, vrátane jeho interakcií s rodičmi, školským prostredím, verejnými orgánmi a digitálnym priestorom.

Právo na rešpektovanie rodinného a súkromného života zakotvuje aj Európsky dohovor o ochrane ľudských práv a základných slobôd. Primárnym účelom práva na rešpektovanie súkromného a rodinného života je ochrana jednotlivca proti svojvoľným zásahom verejnej moci. Európsky súd pre ľudské práva však uvádza, že „*hoci predmetom čl. 8 je v podstate ochrana jednotlivca pred ľubovôľou orgánov verejnej moci, jeho účelom nie je iba nátlak na štát, aby sa zdržal obmedzujúcich zásahov; na dôvažok k tejto primárne negatívnej povinnosti môže existovať pozitívny záväzok obsiahnutý v účinnom rešpekte voči súkromnému alebo rodinnému životu. Tieto záväzky môžu zahŕňať prijatie opatrení určených na zabezpečenie rešpektu k súkromnému životu dokonca aj vo vzťahoch medzi jednotlivcami navzájom*“.⁶ Súčasťou pozitívneho záväzku štátu je tak zabezpečenie ochrany pred neprimeraným zásahom do súkromného života aj zo strany iných jednotlivcov (tzv. horizontálny efekt). V kontexte témy, na ktorú sa zameriava príspevok to znamená, že štát je povinný prijať opatrenia, ktoré zabezpečia ochranu súkromného života dieťaťa pred excesívnym dohľadom zo strany rodičov.

Právo dieťaťa na súkromie je pojmom veľmi širokým a v súčasnosti sa prejavuje v rôznych rovinách. Právo na súkromie nie je pojmom statickým, ale s rozvojom spoločnosti, najmä v oblasti technológií, a to nielen digitálnych, nadobúda omnoho širší rozmer, čo sa prejavuje v potrebe venovať zvýšenú pozornosť obsahu tohto práva a potrebu jeho efektívneho zabezpečenia. Súkromie je základným predpokladom rozvoja osobnosti. U detí však výkon tohto práva nie je absolútny, keďže rodičia nesú zodpovednosť za ich ochranu a výchovu.

UNICEF rozlišuje právo detí na súkromie v niekoľkých oblastiach, keď uvádza, že fyzické, komunikačné, informačné a rozhodovacie aspekty súkromia detí sú relevantné aj v digitálnom svete: fyzické súkromie detí je ovplyvnené technológiami,

⁶ Rozsudok vo veci *Verliere v. Switzerland* z 28. júna 2001, sťažnosť č. 41953/98.

ktoré sledujú, monitorujú a vysielajú aktuálne zábery, správanie alebo polohu detí. Komunikačné súkromie detí je ohrozené, keď ich príspevky, chaty, správy alebo hovory zachytávajú vlády alebo iné subjekty, a informačné súkromie detí môže byť ohrozené, keď sa zhromažďujú, ukladajú alebo spracovávajú osobné údaje detí. Rozhodovacie súkromie detí môže byť ovplyvnené opatreniami, ktoré obmedzujú prístup k užitočným informáciám, čím bránia deťom v schopnosti robiť nezávislé rozhodnutia v súlade s ich rozvíjajúcimi sa schopnosťami.⁷

V porovnaní s minulosťou, kedy digitálny priestor nebol tak široko dostupný a jeho obsah bol prevažne výsledkom ľudskej činnosti, dnešné digitálne prostredie je formované primárne technológiami, vrátane algoritmov a modelov/systémov umelej inteligencie. Tieto technológie nielenže zhromažďujú a analyzujú osobné údaje, ale často aj predikujú správanie používateľov, čím zasahujú do ich súkromia spôsobmi, ktoré sú pre deti ťažko pochopiteľné a kontrolovateľné. V tomto kontexte nadobúda právo dieťaťa na súkromie nový význam a kladie zvýšené nároky na rodičov, prípadne iných zákonných zástupcov dieťaťa, ktorí sú zodpovední za výchovu dieťaťa.

Osobitným spôsobom je potrebné chápať právo dieťaťa na súkromie v digitálnom priestore, kde je dieťa potrebné vnímať ako osobitne zraniteľnú osobu. Táto zraniteľnosť je založená na skutočnosti, že deti a mladí ľudia sa od dospelých líšia z hľadiska svojich kognitívnych predpokladov, nedostatku predchádzajúcich vedomostí a skúseností s určitými spoločenskými procesmi a ich vekovo špecifického prístupu k médiám. Deti a mladí ľudia často nemajú dostatočné informácie alebo majú skreslenú predstavu o tom, čo so sebou prináša pohyb v digitálnom svete, a preto si plne neuvedomujú riziká, ktoré online priestor so sebou nesie.⁸ To ich robí zraniteľnými voči kyberšikanе, nevhodnému obsahu, kontaktu s predátormi, digitálnemu stalkingu či manipulácii. Rovnako problematické je zdieľanie osobných dát a informácií, nakoľko si dieťa často neuvedomuje ich trvalú stopu a hodnotu. Dieťa často nevedomky poskytuje citlivé údaje a fotografie tretím stranám, čím ohrozuje svoje súkromie a vystavuje sa riziku zneužitia identity, sledovania alebo cielenej reklamy. Tento problém je navyše prehlbený fenoménom tzv. „sharentingu“, kde sú súkromné informácie dieťaťa bez jeho súhlasu zdieľané online samotnými rodičmi.

Zodpovednosť rodičov za výchovu a vývoj dieťaťa

Rodič je v rámci výkonu rodičovských práv a povinností povinný starať sa o dieťa a chrániť ho. Podľa ustanovenia § 28 ods. 1 písm. a) zákona č. 36/2005 Z. z. o rodine

⁷ UNICEF: Children's online privacy and freedom of expression: Industry toolkit. New York, 2018, s.8.

⁸ LIVINGSTONE, Sonia - STOILOVA, Mariya - NANDAGIRI, Rishita: Children's data and privacy online: growing up in a digital age: an evidence review. London: London School of Economics and Political Science, 2018, s 21.

v znení neskorších predpisov (ďalej aj ako „Zákon o rodine“) je súčasťou rodičovských práv a povinností najmä sústavná a dôsledná starostlivosť o výchovu, zdravie, výživu a všestranný vývoj maloletého dieťaťa. Podľa odseku 2 citovaného ustanovenia rodičia sú pri výkone rodičovských práv a povinností povinní chrániť záujmy maloletého dieťaťa. Úlohou rodičovských práv a povinností je jednak ochrániť práva dieťaťa, jednak poskytnúť rodičovi prostriedky a priestor, aby mohol svoju výchovnú funkciu realizovať.⁹ Nie nevýznamnou je i povinnosť rodičov v súlade s čl. 4 Zákona o rodine zabezpečiť rodine pokojné a bezpečné prostredie. Teda prostredie, ktoré by bolo bezpečné nielen z pohľadu fyzického bezpečia, ale ktoré by bolo i prostredím, v ktorom maloletý cíti sociálne a psychologické bezpečie, t. j. prostredie v ktorom je nielen rešpektované jeho súkromie, vrátane parciálnych práv s ním súvisiacich, ale v ktorom sú saturované potreby jeho duševného a emočného blahobytu.¹⁰

Jednou z najcitlivejších oblastí uplatňovania práva na súkromie je vzťah dieťaťa a jeho rodičov, resp. iných zákonných zástupcov. Právo dieťaťa na súkromie sa môže dostať do kolízie s právom a zodpovednosťou rodičov za výchovu a vývoj dieťaťa zakotveným v článku 19 ods. 1 Dohovoru.¹¹ Obava zo vzniku tejto kolízie vyvstala už pri kreovaní Dohovoru, ako vyplýva zo Správy pracovnej skupiny pre komisiu pre ľudské práva z roku 1988: „ *Mali by však byť chránené legitímne práva rodičov a opatrovníkov, mala by byť zachovaná rovnováha medzi právami detí a právami rodiny.. Bol vyjadrený názor, že ak by rodičia mali byť chránení pred štátmi, dieťa by malo byť chránené pred rodičmi.*“¹² Finálna textácia Dohovoru túto skutočnosť zohľadňuje. Článok 16 Dohovoru poskytuje dieťaťu ochranu pred svojvoľnými zásahmi do jeho súkromia, bez rozlíšenia odkiaľ (kým) sa robia. Inými slovami, dieťa má právo na ochranu pred svojvoľnými zásahmi do svojho súkromia aj vtedy, ak sú robené jeho zákonnými zástupcami (nositeľmi rodičovskej zodpovednosti).¹³

Dohovor uznáva právo a povinnosť rodičov usmerňovať dieťa vo výkone jeho práv, avšak toto usmerňovanie musí byť podľa článku 5 Dohovoru v súlade s rozvíjajúcimi

⁹ PAVELKOVÁ, Bronislava. Zákon o rodine a o zmene a doplnení niektorých zákonov. 3. vydanie. Bratislava: C. H. Beck, 2019, s. 166. ISBN 978-80-89603-72-5.

¹⁰ HAMŘÍK, Martin: Paternalizmus v konflikte rodičovských práv a práva na súkromie maloletého so zameraním na rodovú identitu. In: Quo vadis postavenie transrodových ľudí na Slovensku? 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2023, s. 18-19. ISBN 978-80-7160-707-6.

¹¹ Štáty, ktoré sú zmluvnou stranou Dohovoru, vynaložia všetko úsilie na to, aby sa uznala zásada, že obaja rodičia majú spoločnú zodpovednosť za výchovu a vývoj dieťaťa. Rodičia alebo v zodpovedajúcich prípadoch zákonní zástupcovia, majú prvotnú zodpovednosť za výchovu a vývoj dieťaťa. Základným zmyslom ich starostlivosti musí pritom byť záujem dieťaťa.

¹² ÚRAD VYSOKÉHO KOMISÁRA OSN PRE ĽUDSKÉ PRÁVA: The Legislative History of the Convention on the Rights of the Child. Volume 1. New York, Ženeva, 2007, s. 477.

¹³ Rozsudok Najvyššieho súdu ČR z 12. 12. 2012, sp. zn. 30 Cdo 3770/2011

sa schopnosťami dieťaťa (*evolving capacities of the child*).¹⁴ Článok 5 vyvažuje práva dieťaťa na slobodu a autonómiu s právom a povinnosťou rodičov poskytovať mu ochranu a vedenie. Toto ustanovenie reaguje na meniace a vyvíjajúce sa schopnosti dieťaťa v súlade s jeho rastúcim vekom a vyžaduje, aby sa rodičovské usmerňovanie prispôbovalo rastúcej zrelosti a schopnostiam dieťaťa. S pribúdajúcim vekom a rastúcou zrelosťou dieťaťa sa rozširuje aj jeho právo na súkromie a autonómne rozhodovanie.

V uvedenej súvislosti je potrebné mať na zreteli aj ďalšie ustanovenia Dohovoru, najmä princíp najlepšieho záujmu dieťaťa zakotvený v článku 3¹⁵ a tiež právo dieťaťa vyjadriť svoj názor garantované článkom 12 ods. 1 Dohovoru¹⁶. V rámci využitia nástrojov digitálnej kontroly by mal rodič zvažovať, aké prostriedky použije za účelom ochrany dieťaťa, a to nielen v aktuálnom čase, ale z dlhodobého hľadiska. Najlepší záujem dieťaťa musí zahŕňať aj emocionálne či psychologické blaho dieťaťa, a prihliadať aj na jeho morálnu integritu. Nevyhnutný prvok v procese zisťovania najlepšieho záujmu dieťaťa predstavujú aj participačné práva dieťaťa, najmä právo dieťaťa vyjadriť svoj názor. Pre zadefinovanie najlepšieho záujmu dieťaťa je potrebné poznať aj názor dieťaťa, ak je schopné ho vyjadriť, a ktorému je potrebné načúvať v intenciách zodpovedajúcich jeho veku a rozumovej vyspelosti. Luprichová k tomu uvádza: „Medzi článkami 3 a 12 nie je žiadna konkurencia, len doplňujúca úloha dvoch všeobecných princípov: jeden stanovuje cieľ dosiahnuť najlepší záujem dieťaťa a druhý poskytuje metodiku pre dosiahnutie cieľa v podobe zisťovania názorov dieťaťa a vypočutia dieťa. Aplikácia článku 3 v skutočnosti nemôže byť správna, ak nie sú rešpektované časti článku 12. Obdobne článok 3 posilňuje funkciu článku 12”.¹⁷

Čím bude dieťa staršie, jeho schopnosti budú rozvinutejšie a bude mať viac životných skúseností, tým väčšou mierou sa bude samostatne a slobodne rozhodovať o svojich záležitostiach a obsah jeho najlepšieho záujmu bude čím ďalej tým viac

¹⁴ Štáty, ktoré sú zmluvnou stranou Dohovoru, sa zaväzujú rešpektovať zodpovednosť, práva a povinnosti rodičov alebo, v zodpovedajúcich prípadoch a v súlade s miestnou obyczajou, členov širšej rodiny alebo obce, zákonných zástupcov alebo iných osôb právne zodpovedných za dieťa, ktoré smerujú k zabezpečeniu jeho orientácie a usmerňovaniu pri výkone práv podľa Dohovoru v súlade s jeho rozvíjajúcimi sa schopnosťami.

¹⁵ Záujem dieťaťa musí byť prvoradým hľadiskom pri akejkoľvek činnosti týkajúcej sa detí, nech už uskutočňovanej verejnými alebo súkromnými zariadeniami sociálnej starostlivosti, súdmi, správnymi alebo zákonodarnými orgánmi.

¹⁶ Štáty, ktoré sú zmluvnou stranou Dohovoru, zabezpečujú dieťaťu, ktoré je schopné formulovať svoje vlastné názory, právo tieto názory slobodne vyjadrovať vo všetkých záležitostiach, ktoré sa ho dotýkajú, pričom sa názorom dieťaťa musí venovať patričná pozornosť zodpovedajúca jeho veku a úrovni.

¹⁷ LUPRICHOVÁ Petronela: Najlepší záujem dieťaťa - efektívny nástroj ochrany maloletého dieťaťa? In: Bratislavské právnické fórum 2015. 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2015, s. 165. ISBN 978-80-7160-411-2.

determinovaný jeho názorom.¹⁸ Určujúci pritom nie je samotný vek, ale individuálna vyspelosť dieťaťa; jeho názor preto musí byť posúdený vždy s ohľadom na konkrétne okolnosti prípadu.¹⁹

V tomto kontexte je žiadúce, aby rodičia jednostranne neinštalovali prostriedky digitálnej kontroly bez toho, aby dieťaťu vysvetlili dôvody pre ich používanie. Ako vhodná sa javí otvorenosť a transparentnosť – rodič by mal vysvetliť svoje dôvody pre používanie digitálnej kontroly a vypočuť si pohľad dieťaťa. Rodič by mal tiež pravidlá digitálnej kontroly nastaviť tak, aby nestratil dôveru dieťaťa.

V tejto súvislosti sa v poslednom období často stretávame s pojmom **rodinná digitálna dohoda** (family media agreement, family tech agreement). Tento pojem ešte nenachádzame v odbornej právnickej literatúre, ale predovšetkým na webových stránkach, ktoré sa venujú digitálnej bezpečnosti detí alebo vzdelávaniu rodičov v tejto oblasti.²⁰ Rodinnú digitálnu dohodu možno zjednodušene definovať ako vzájomne dohodnuté pravidlá medzi rodičmi a deťmi o tom, ako sa bude v domácnosti používať technológia a internet. Môže obsahovať ustanovenia o časových limitoch používania zariadení, pravidlá pre zdieľanie obsahu (napr. fotky len so súhlasom rodiča), zásady bezpečnosti (napr. neotvárať odkazy od neznámych osôb), digitálnu etiketu (napr. rešpektovanie druhých v online priestore), off-line aktivity (napr. povinný čas bez obrazovky), zodpovednosť rodičov (napr. rešpektovanie vlastných digitálnych návykov), ale aj ustanovenia o rodičovskej kontrole a pod. Účelom tejto dohody je stanovenie jasných pravidiel pre používanie technológií a správanie sa v online priestore pre jednotlivých členov rodiny. Dohoda je viac-menej neformálna, slúži na budovanie zdravých návykov v oblasti používania digitálnych technológií a využívania internetu v konkrétnej rodine.

Digitálny dohľad rodičov

Digitálny dohľad rodičov (alebo digitálny rodičovský dohľad) možno definovať ako súbor softvérových nástrojov, aplikácií a systémových nastavení, ktoré umožňujú rodičom monitorovať, obmedzovať a spravovať digitálne aktivity a prístup svojho dieťaťa k internetu a elektronickým zariadeniam. Ako príklad možno uviesť Google Family Link²¹, Microsoft family Safety²², Net Nanny²³ a ďalšie. Cieľom digitálnej kontroly je primárne ochrana dieťaťa pred online rizikami a podpora rozvoja zdravých digitálnych návykov.

¹⁸ Porovnaj: Výbor OSN pre práva dieťaťa: Všeobecný komentár č. 14 (2013) o práve dieťaťa na prvoradé zohľadnenie jeho alebo jej najlepšieho záujmu (čl. 3 ods. 1). CRC/C/GC/14, 2013, bod 44.

¹⁹ Nález Ústavného súdu ČR z 12. 6. 2023, sp. zn. III. ÚS 1318/22, bod 35.

²⁰ Napr. www.beznastrah.online, www.digideti.cz, www.digitalnirodicia.sk a ďalšie.

²¹ <https://families.google/familylink/>

²² <https://www.microsoft.com/en-us/microsoft-365/family-safety>

²³ <https://www.safemymkid.com/>

Medzi základné funkcie digitálnej rodičovskej kontroly patria:

1. Filtrácia obsahu a blokovanie aplikácií - cieľom tejto funkcie je chrániť psychický a morálny vývoj dieťaťa. Systémy digitálnej kontroly neustále analyzujú internetové prostredie a na základe databáz a analýzy kľúčových slov blokujú prístup k celým kategóriám webových stránok. Medzi najčastejšie blokové kategórie patrí pornografia, extrémistický a radikálny obsah, hazardné hry alebo stránky s návodmi na seba poškodzovanie. Kontrola taktiež vynucuje vekové limity určené pre konkrétne aplikácie alebo hry, čím bráni dieťaťu inštalovať a používať obsah, na ktorý ešte emocionálne alebo kognitívne nedozrelo. Rodičia môžu tiež vynútiť funkciu bezpečného vyhľadávania (SafeSearch), ktorá filtruje explicitné materiály priamo vo výsledkoch vyhľadávateľov.

2. Manažment času a plánovanie používania - rodičia môžu nastaviť presné denné alebo týždenné limity na celkové používanie zariadenia alebo špecifických, často návykových aplikácií (napr. sociálne siete či mobilné hry). Tieto nástroje umožňujú tiež plánovanie vypnutia zariadenia v určitých časoch, napr. počas školského vyučovania či v noci.

3. Sledovanie polohy a nastavenie bezpečných zón - funkcia sledovania polohy (geolokácia) poskytuje rodičom informácie o fyzickej bezpečnosti dieťaťa, najmä vtedy, ak sa pohybuje samostatne. Aplikácie umožňujú sledovanie polohy v reálnom čase, čo je kľúčové v neočakávaných alebo núdzových situáciách. Rozšírenou a veľmi užitočnou funkciou je Geofencing (virtuálne ohraničenie), kde rodič nastaví „bezpečné zóny“ (ako je domov, škola alebo ihrisko) a dostane automatické upozornenie, keď dieťa do tejto zóny vstúpi, alebo ju naopak opustí.

4. Monitorovanie komunikácie a upozornenia – tieto nástroje sú navrhnuté tak, aby chránili dieťa pred kyberšikanou, online predátormi alebo prejavmi extrémneho správania. Softvér dokáže skenovať správy a upozorniť rodiča, ak sa v komunikácii objavia špecifické kľúčové slová súvisiace so seba poškodzovaním, násilím, drogami alebo neprimeranými požiadavkami od neznámych osôb. Aj keď plné čítanie obsahu správ predstavuje vysoký zásah do súkromia dieťaťa, menej invazívne nástroje aspoň poskytujú prehľad o metadátach – to znamená o tom, aké aplikácie dieťa používa a s kým najčastejšie komunikuje, bez nutnosti sledovať obsah samotných správ.

Monitorovanie správania dieťaťa môže byť skryté alebo otvorené. Skryté monitorovanie spočíva v úmyselnom ponechaní dieťaťa v nevedomosti o tom, že je jeho online aktivita sledovaná. Hoci výhodou je, že rodičia vidia neskreslené správanie, keď si dieťa myslí, že ho nikto nesleduje, je klamlivé a narúša dôveru medzi rodičom a dieťaťom. Pri otvorenom monitorovaní sú rodičia voči dieťaťu transparentní a otvorene ho informujú o dohľade nad jeho digitálnou komunikáciou a aktivitami. Výhodou tohto prístupu je úprimnosť, avšak nesie so sebou riziko, že dieťa môže prijať protiopatrenia. V snahe vyhnúť sa dohľadu môže dieťa začať

používať zariadenia mimo domu alebo sa naučiť techniky na obchádzanie monitorovacích nástrojov na domácich počítačoch.²⁴

Spôsob využívania nástrojov digitálnej kontroly

Rada Európskej únie uvádza, že využívanie technických systémov (ako napríklad filtrov, systémov overovania veku, systémov rodičovskej kontroly) môže byť za predpokladu, že sa uplatňujú účinným spôsobom, vhodným prostriedkom na zabezpečenie prístupu maloletých osôb k obsahu, ktorý je vhodný pre ich vek, aj keď takéto systémy nie sú samy osebe riešením.²⁵ V kontexte riešení rodičovskej kontroly je však kľúčovou otázkou, či takéto riešenia môžu posilniť alebo skôr podkopať možnosti ďalšieho rozvoja digitálnych kompetencií detí.²⁶ Spravidla sa zameriavajú len na pasívnu, technickú ochranu a nenaučia dieťa samostatnému a zodpovednému manažmentu svojho online správania, napr. samostatne vyhodnotiť rizikové správanie či nepravdivé informácie. Filtre možno ľahko obísť a nechránia dieťa pred psycho-sociálnymi rizikami ako je kyberšikana, sociálna manipulácia alebo nadmerné zdieľanie osobných dát. Príliš extenzívne alebo netransparentné používanie rodičovskej kontroly, najmä u dospievajúcich, narúša dôveru v rodine a je v rozpore s princípom rastúcej autonómie dieťaťa. Z týchto dôvodov by mali byť technické nástroje vždy doplnené aktívnymi prostriedkami ako je vzájomný dialóg, vzdelávanie v digitálnej bezpečnosti a spoločné nastavovanie pravidiel.

Hamřík v súvislosti s výkonom rodičovských práv a povinností upozorňuje na paternalizmus zo strany rodičov v podobe rozhodovania o osobnostných právach maloletých, či zásahov rodičov do osobnostných práv maloletých. Ten musí byť limitovaný ochranou záujmov maloletého za súčasného umožnenia najvyššej možnej miery autonómie maloletého, a redukovaný len na vykonávanie tých úkonov a obmedzení, ktoré sú objektívne v najlepšom záujme maloletého.²⁷ Rodičovské zásahy do súkromia dieťaťa, ako je neustále a netransparentné monitorovanie komunikácie alebo plošné blokovanie sociálnych sietí, predstavujú formu paternalizmu. Rodič tu síce koná s úmyslom chrániť, ale zároveň blokuje dieťaťu

²⁴ MATHIESEN, Kay: The Internet, children, and privacy: The case against parental monitoring. In: Ethics and Information Technology, č. 15 (2015), s. 264.

²⁵ Závery Rady Európskej únie o ochrane detí v digitálnom svete (2011/C 372/04)

²⁶ GNANASEKARAN, Vahiny - DE MOOR, Katrien: Providing user perspectives to the next generation of parental controls. In: International Journal of Child-Computer Interaction, č. 44 (2025). <https://doi.org/10.1016/j.ijcci.2025.100735>

²⁷ HAMŘÍK, Martin: Paternalizmus v konflikte rodičovských práv a práva na súkromie maloletého so zameraním na rodovú identitu. In: Quo vadis postavenie transrodových ľudí na Slovensku? 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2023, s. 19. ISBN 978-80-7160-707-6.

možnosť rozvíjať sa a niešť zodpovednosť. Takéto správanie nemožno vyhodnotiť, ako správanie v najlepšom záujme dieťaťa.

Ak sa teda rodič rozhodne pristúpiť k využitiu nástrojov rodičovského dohľadu, ako by mal tento dohľad vyzeráť, aby nezasahoval do práv dieťaťa na súkromie, eventuálne aj do iných jeho práv? V prvom rade, akýkoľvek zásah do práva dieťaťa na súkromie musí slúžiť legitímnemu účelu, dodržiavať zásadu minimalizácie údajov, byť primeraný a zameraný na ochranu najlepších záujmov dieťaťa a nesmie byť v rozpore so zásadami, cieľmi alebo zámermi Dohovoru.²⁸

Z Dohovoru vyplýva, že rodičia dieťaťa majú právo aj povinnosť dohliadať na dieťa, aby ochránili jeho zdravie a bezpečnosť. Dieťa však má právo na súkromie, a kolízia týchto práv sa musí riadiť **zásadou proporcionality**. Táto zásada vyžaduje, aby bola rodičovská kontrola primeraná veku, zrelosti a schopnosti porozumieť rizikám digitálneho prostredia, ktorému je vystavené. Rodičovská kontrola by preto nemala byť absolútna, ale mala by sa postupne prispôbovať rastúcej autonómii dieťaťa. V praxi to znamená potrebu hľadania rovnováhy medzi ochranou a rešpektovaním súkromia, pričom zásahy do digitálneho priestoru dieťaťa musia byť odôvodnené, primerané a transparentné. Ako dieťa rastie a zvyšujú sa jeho kognitívne schopnosti, preukazuje vyššiu psychologickú zrelosť, schopnosť kritického myslenia a porozumenie dôsledkom svojho správania, musí sa priestor pre rodičovské usmerňovanie postupne znižovať.

Porušenie práva dieťaťa na súkromie

Rodič sa spravidla snaží konať tak, aby jeho konanie bolo v najlepšom záujme dieťaťa. Nemožno však vylúčiť situácie, že rodič buď úmyselne alebo v dôsledku nedostatku skúsenosti, vedomostí, informácií či nesprávneho vyhodnotenia situácie bude konať v rozpore s právami dieťaťa. V otázkach týkajúcich sa osobnostných práv maloletého, osoby dieťaťa, zákonní zástupcovia nepodliehajú kontrole súdom ani v prípade, ak ide o podstatné rozhodnutia.²⁹

Rodič prekračuje rozsah svojej rodičovskej zodpovednosti a neoprávneným spôsobom zasahuje do súkromia dieťaťa najmä v dvoch situáciách, ktoré sa viažu na schopnosť dieťaťa samostatne rozhodovať. Prvý prípad nastáva vtedy, keď je dieťa objektívne schopné vyjadriť svoj nesúhlas s konkrétnym prostriedkom alebo spôsobom dohľadu, ale rodič ho napriek tomu aplikuje. Ide najmä o situácie, kedy dieťa, ktoré je schopné rozumne posúdiť situáciu a vyjadriť svoj názor, výslovne nesúhlasí s istou formou dohľadu (napr. so sledovaním aplikácií či čítaním správ). V

²⁸ Výbor OSN pre práva dieťaťa: Všeobecný komentár č. 25 (2021) o právach dieťaťa v súvislosti s digitálnym prostredím, CRC/C/GC/25, para 69.

²⁹ JURČOVÁ, M., PAVELKOVÁ, B., NEVOLNÁ, Z., OLŠOVSKÁ, A., SMYČKOVÁ, R. Zastúpenie v súkromnom práve. 2. vydanie. Praha: C. H. Beck, 2021, s. 138. ISBN 978-80-7400-836-8.

takomto prípade rodič ignoruje princíp rastúcej autonómie a porušuje právo dieťaťa na súkromie.

Druhý prípad nastáva, ak je zásah do súkromia neprimerane rozsiahly a prekračuje nutnú mieru na ochranu dieťaťa, a to bez ohľadu na vek. Aj keď dieťa nie je schopné vyjadriť svoj súhlas či nesúhlas (napr. pre nízky vek), rodič vykonáva neoprávnený zásah vtedy, ak kontrola nie je opodstatnená konkrétnym rizikom. Ak napríklad rodič dlhodobo a trvalo monitoruje všetky dáta malého dieťaťa, hoci neexistuje žiadny vážny dôvod (ako podozrenie na sebapoškodzovanie či kontakt s predátorom), takéto opatrenie je neproporcionálne. Rodič vtedy nekoná v rámci najlepšieho záujmu dieťaťa, ale vykonáva kontrolu, ktorá presahuje mieru nevyhnutnú pre zaistenie jeho bezpečnosti.

Ak sa dieťa domnieva, že rodičia svojim konaním neprimeraným spôsobom zasahujú do jeho práva na súkromie, môže sa domáhať ochrany. Problematickým aspektom domáhania sa ochrany je však skutočnosť, že dieťa do dovŕšenia plnoletosti má len obmedzenú spôsobilosť na právne úkony³⁰, a tým pádom by sa mohlo javiť, že má aj obmedzenú možnosť domáhať sa ochrany. Právny poriadok však dáva dieťaťu možnosti, ako sa domôcť ochrany.

Dieťa sa môže primárne obrátiť na **orgán sociálno-právnej ochrany detí** (ďalej aj ako „OSPOD“), Komisára pre deti alebo na iné orgány či osoby. Zákon č. 305/2005 Z. z. o sociálnoprávnej ochrane detí a o sociálnej kuratele a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v ustanovení § 8 zakotvuje právo dieťaťa požiadať o pomoc pri ochrane svojich práv, a to aj bez vedomia rodičov a aj prostredníctvom tretích osôb.³¹ Orgán sociálnoprávnej ochrany môže uložiť rodičom, dieťaťu alebo rodičom aj dieťaťu výchovné opatrenie, ktoré by spočívalo napr. v povinnej účasti na rodinnej mediácii alebo návštevu psychológa či iných špecializovaných subjektov. Spôsob poskytnutia ochrany závisí od konkrétnej situácie v rodine. OSPOD by mal primárne pracovať s rodinou a zistiť, aký je dôvod

³⁰ Pozri ustanovenie § 8 Občianskeho zákonníka: Maloletí majú spôsobilosť len na také právne úkony, ktoré sú svojou povahou primerané rozumovej a vôľovej vyspelosti zodpovedajúcej ich veku.

³¹ (1) Dieťa má právo požiadať o pomoc pri ochrane svojich práv orgán sociálnoprávnej ochrany detí a sociálnej kurately, iný štátny orgán, ktorý je príslušný podľa osobitných predpisov⁷⁾ chrániť práva a právom chránené záujmy dieťaťa, zariadenie, obec, vyšší územný celok, akreditovaný subjekt, školu, školské zariadenie alebo poskytovateľa zdravotnej starostlivosti. Všetky orgány, právnické osoby a fyzické osoby uvedené v prvej vete sú povinné poskytnúť dieťaťu okamžitú pomoc pri ochrane jeho života a zdravia, vykonať opatrenia na zabezpečenie jeho práv a právom chránených záujmov, a to aj sprostredkovaním tejto pomoci. To platí aj vtedy, ak dieťa nemôže vzhľadom na svoj vek a rozumovú vyspelosť požiadať o pomoc samo, ale prostredníctvom tretej osoby.

(2) Dieťa má právo požiadať o pomoc pri ochrane svojich práv aj bez vedomia rodičov alebo osoby, ktorá sa osobne stará o dieťa. Tým nie sú dotknuté práva a povinnosti rodičov vyplývajúce z rodičovských práv a povinností a práva osoby, ktorá sa osobne stará o dieťa, upravené osobitným predpisom.

neoprávneného zásahu rodičov do práva dieťaťa na súkromie. Tento neoprávnený zásah môže byť len jediným problémom v rodine, ale tiež môže byť súčasťou širšieho problému v rodine alebo vzťahu medzi rodičom a dieťaťom.

V prípade, ak boli práva dieťaťa porušené do takej miery, že je potrebné dieťaťu poskytnúť **súdnú ochranu**, je situácia komplikovanejšia. A to nielen z právneho hľadiska, ale aj z hľadiska vzťahov v rodine. Pokiaľ ide o právne hľadisko, ako je uvedené vyššie, maloleté dieťa má obmedzenú spôsobilosť na právne úkony. Od spôsobilosti na právne úkony sa odvíja procesná spôsobilosť maloletého, t.j. oprávnenie samostatne realizovať procesné úkony v súdnom konaní, teda aj spôsobilosť na podanie žaloby na ochranu svojich práv neoprávnených zásahov rodiča do práva na súkromie. Procesná spôsobilosť je upravená v ustanovení § 67 a nasl. zákona č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších právnych predpisov (ďalej aj ako „CSP“) nasledovne: *„každý môže pred súdom samostatne konať v rozsahu, v akom má spôsobilosť na právne úkony.“* Ak osoba nemá procesnú spôsobilosť, musí byť zastúpená zákonným zástupcom alebo procesným opatrovníkom. V prípade maloletého dieťaťa je zákonným zástupcom vo väčšine prípadov jeho rodič, avšak ten ho nebude môcť zastupovať, pretože práve rodič je pôvodcom neoprávneného zásahu a v žalobe bude označený ako žalovaný. Dôvod pre vylúčenie zastupovania je zjavná kolízia záujmov zákonného zástupcu a zastúpeného, ktorú ustanovenie § 30 zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov (ďalej aj ako „Občiansky zákonník“) považuje za prekážku zastúpenia.

Zákonným zástupcom dieťaťa nemôže byť v tomto prípade ani OSPOD. OSPOD je oprávnený zastupovať maloleté deti v súdnych konaniach, v ktorých nemôžu byť z dôvodu existencie potenciálneho konfliktu záujmov zastúpené svojimi rodičmi. V takýchto prípadoch súd ustanoví dieťaťu OSPOD ako jeho opatrovníka, ktorý bude zastupovať maloleté dieťaťu v konkrétnom súdnom konaní (§ 31 ods. 2 Zákona o rodine). Zastupovanie sa však týka spravidla konaní vo veciach starostlivosti súdu o maloletých, ktoré sú upravené v prvej hlave druhej časti zákona č. 161/2015 Z. z. Civilný mimosporový poriadok v znení neskorších predpisov. V takom konaní môže súd, v nadväznosti na tému príspevku, rozhodnúť napr. o uložení výchovného opatrenia podľa § 37 Zákona o rodine, alebo, ak si to situácia v rodine vyžaduje, môže pristúpiť k zásahu do výkonu rodičovských práv a povinností vo forme obmedzenia, pozastavenia alebo pozbavenia rodiča/rodičov výkonu rodičovských práv podľa ustanovenia § 38 Zákona o rodine. OSPOD nemôže vystupovať ako súdom ustanovený zástupca maloletého dieťaťa v iných veciach, napr. ak by išlo o konanie podľa CSP. Rovnako nie je oprávnený byť splnomocneným zástupcom dieťaťa s ohľadom na to, že jeho kompetencie sú dané výlučne zákonom a ten neumožňuje, aby OSPOD vystupoval ako splnomocnený zástupca. Dieťaťu musí v takom prípade

ustanoviť súd procesného opatrovníka z osôb uvedených v § 71 CSP.³² Už samotné začatie súdneho konania je tak komplikované.

Maloleté dieťa sa v súdnom konaní môže domáhať ochrany svojho práva na súkromie, ktoré patrí medzi osobnostné práva. Do úvahy prichádza najmä podanie negatívnej žaloby podľa § 13 ods. 1 Občianskeho zákonníka, ktorou sa bude domáhať, aby rodič upustil od neoprávnených zásahov do práva dieťaťa na súkromie excesívnym použitím prostriedkov digitálneho rodičovského dohľadu. Za účelom efektívnej ochrany je však vhodnejším prostriedkom podanie návrhu na vydanie neodkladného opatrenia podľa ustanovenia § 325 ods. 2 písm. d) CSP, ktorým sa bude domáhať, aby sa rodič zdržal neoprávneného zásahu do práva dieťaťa na súkromie. Pokiaľ ide o vzťahy v rodine, rozhodnutie dieťaťa požadovať súdnu ochranu pred konaním rodiča možno označiť ako kolaps rodinného systému. Ak dieťa vyhodnotí, že nemá inú možnosť, ako takto konať, môže to mať na vzťahy v rodine hlboké a často nezvratné deštruktívne následky. V takomto momente sa súkromný spor zmení na verejný a formálny konflikt. Z týchto dôvodov je potrebné súdnu ochranu považovať za riešenie *ultima ratio* a pristúpiť k nemu len vtedy, ak zlyhali všetky iné pokusy o riešenie situácie a psychologická ujma spôsobená pretrvávajúcim porušovaním práv dieťaťa je väčšia než trauma spôsobená samotným súdnym konaním.

Záver

Rozšírenie smartfónov a aplikácií umožnilo rodičom sledovať pohyb, komunikáciu a online správanie detí. Medzi najčastejšie využívané prostriedky patria GPS lokalizačné aplikácie a inteligentné hodinky, ktoré umožňujú sledovať polohu dieťaťa v reálnom čase, ďalej aplikácie na rodičovskú kontrolu obsahu, ktoré filtrujú webové stránky alebo obmedzujú čas používania zariadení, a napokon aj aplikácie monitorujúce komunikáciu na sociálnych sieťach či v správach. Hoci tieto nástroje zvyšujú pocit bezpečia a môžu byť užitočné v krízových situáciách, vyvolávajú zásadné otázky, do akej miery zasahujú do autonómie dieťaťa a do jeho práva na súkromie, ktoré mu zaručujú vnútroštátne, aj medzinárodné právne normy.

Tento príspevok analyzuje, ako sa právo dieťaťa na súkromie transformuje a komplikuje v digitálnom prostredí, pričom sa zameriava na hranice rodičovskej kontroly prostriedkami digitálneho dohľadu. Rodičovská kontrola, hoci motivovaná ochranou dieťaťa, môže v určitých prípadoch zasahovať do autonómie dieťaťa a jeho

³² (1) Za procesného opatrovníka súd ustanoví blízku osobu alebo inú osobu z rodinného prostredia strany, ktorá je spôsobilá na právne úkony v plnom rozsahu, u ktorej je predpoklad, že bude konať v súlade so záujmami strany a s ustanovením súhlasí.

(2) Ak takej osoby niet, súd za procesného opatrovníka ustanoví obec, v ktorej mala strana poslednú adresu trvalého pobytu.

(3) V prípade bezprostredného nebezpečenstva z omeškania, alebo ak osôb podľa predchádzajúcich odsekov niet, súd môže ustanoviť za procesného opatrovníka súdneho úradníka.

práva na súkromie. Výzvou je nájsť rovnováhu medzi ochranou pred rizikami, s ktorými sa dieťa v kyberpriestore stretáva a rešpektovaním individuálnych práv dieťaťa. Právo dieťaťa na súkromie nie je len formálnym právnym ustanovením, ale kľúčovým predpokladom jeho zdravého psychologického a sociálneho vývoja. Implementácia článku 16 Dohovoru si vyžaduje neustále vyvažovanie medzi rodičovskou zodpovednosťou a postupne sa rozvíjajúcou autonómiou dieťaťa, vždy s prvoradým zohľadnením jeho najlepšieho záujmu, ktorý je možné zistiť len rešpektovaním práva dieťaťa na vyjadrenie svojho názoru v každej veci, ktorá sa ho týka.

Z predloženej analýzy vyplýva, že technologické nástroje rodičovskej digitálnej kontroly sú len čiastočným a nedostatočným riešením. Ich použitie by malo byť len sekundárne, odôvodnené konkrétnymi rizikami, ktoré predstavuje pre dieťa používanie digitálnych technológií alebo pohyb v online priestore. Primárnym spôsobom riešenia by malo byť aktívna komunikácia rodiča s dieťaťom a vzdelávanie dieťaťa ohľadom rizík, ktoré sa spájajú s digitálnymi technológiami, a to spôsobom, ktorý je primeraný veku dieťaťa a jeho rozumovej vyspelosti. Dieťa by sa malo samé naučiť rozpoznávať riziko spojené s používaním digitálnych technológií a vedieť vyhodnotiť prípadné následky svojho správania v online priestore. Tento prístup je nielen dlhodobo udržateľný, ale rešpektuje rastúcu autonómiu dieťaťa, čím predchádza narušeniu dôvery v rodine. Prílišné a netransparentné používanie prostriedkov digitálneho dohľadu sa stáva nelegitímny zásahom, ktorý je v rozpore s najlepším záujmom dieťaťa. Pri nadmernom používaní totiž dochádza k strate dôvery medzi rodičmi a deťmi, k pocitu permanentného dohľadu a k obmedzovaniu práva dieťaťa budovať si vlastnú identitu.

V záverečnej časti príspevku sme stručne načrtli, aké má dieťa v slovenskom právnom prostredí možnosti domáhať sa ochrany svojho práva, v prípade, ak rodič neoprávneným spôsobom zasahuje do jeho práva na súkromie. Právo ponúka dieťaťu právne prostriedky, akým sa domôcť svojho práva, ale tie by mali byť posledným možným riešením. Dieťa by nemalo byť do strany rodičov postavené do takej situácie, aby nemalo inú možnosť, ako siahnuť po týchto prostriedkoch. V zdravom rodinnom prostredí by sa takéto situácie vôbec nemali vyskytovať.

Zoznam použitej literatúry

1. ČIPKOVÁ, Tamara: Informovaný súhlas pri poskytovaní zdravotnej starostlivosti maloletému dieťaťu. In: Postavenie transrodových ľudí na Slovensku [elektronický dokument] : interdisciplinárne pohľady. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2022. S. 190-204. ISBN 978-80-7160-661-1.

2. GNANASEKARAN, Vahiny - DE MOOR, Katrien: Providing user perspectives to the next generation of parental controls. In: International Journal of Child-Computer Interaction, č. 44 (2025). <https://doi.org/10.1016/j.ijcci.2025.100735>
3. HAMŘÍK, Martin: Paternalizmus v konflikte rodičovských práv a práva na súkromie maloletého so zameraním na rodovú identitu. In: Quo vadis postavenie transrodových ľudí na Slovensku? 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2023. S. 6-25. ISBN 978-80-7160-707-6.
4. JURČOVÁ, M., PAVELKOVÁ, B., NEVOLNÁ, Z., OLŠOVSKÁ, A., SMYČKOVÁ, R. Zastúpenie v súkromnom práve. 2. vydanie. Praha: C. H. Beck, 2021. 360 s. ISBN 978-80-7400-836-8.
5. LIVINGSTONE, Sonia - POTHONG, Kruakae: Child rights impact assessment: a policy tool for a rights-respecting digital environment. In: Policy and Internet, roč. 17, č. 3 (2025), s. 1-12. <https://doi.org/10.1002/poi3.70008>
6. LIVINGSTONE, Sonia - STOILOVA, Mariya - NANDAGIRI, Rishita: Children's data and privacy online: growing up in a digital age: an evidence review. London: London School of Economics and Political Science, 2018, 57 s.
7. LUPRICOVÁ Petronela: Najlepší záujem dieťaťa - efektívny nástroj ochrany maloletého dieťaťa? In: Bratislavské právnické fórum 2015. 1. vyd. Bratislava: Univerzita Komenského v Bratislave. Právnická fakulta UK, 2015. S. 163-168. ISBN 978-80-7160-411-2.
8. MATHIESEN, Kay: The Internet, children, and privacy: The case against parental monitoring. In: Ethics and Information Technology, č. 15 (2015), s 263–274.
9. PAVELKOVÁ, Bronislava. Zákon o rodine a o zmene a doplnení niektorých zákonov. 3. vydanie. Bratislava: C. H. Beck, 2019. 688 s. ISBN 978-80-89603-72-5.
10. UNICEF: Children's online privacy and freedom of expression: Industry toolkit. New York, 2018, 28 s.
11. ÚRAD VYSOKÉHO KOMISÁRA OSN PRE ĽUDSKÉ PRÁVA: The Legislative History of the Convention on the Rights of the Child. Volume 1. New York, Ženeva, 2007. 493 s. ISBN. 978-92-1-154177-9.
12. Výbor OSN pre práva dieťaťa: Všeobecný komentár č. 14 (2013) o práve dieťaťa na prvoradé zohľadnenie jeho alebo jej najlepšieho záujmu (čl. 3 ods. 1). CRC/C/GC/14, 2013.
13. Výbor OSN pre práva dieťaťa: Všeobecný komentár č. 25 (2021) o právach dieťaťa v súvislosti s digitálnym prostredím, CRC/C/GC/25, 2021.
14. Závery Rady Európskej únie o ochrane detí v digitálnom svete (2011/C 372/04)
15. Nález Ústavného súdu ČR z 12. 6. 2023, sp. zn. III. ÚS 1318/22
16. Rozsudok ESLP vo veci Verliere v. Switzerland z 28. júna 2001, sťažnosť č. 41953/98.
17. Rozsudok Najvyššieho súdu ČR z 12. 12. 2012, sp. zn. 30 Cdo 3770/2011

Kontaktné údaje

doc. Mgr. Lenka Dufalová, PhD.

lenka.dufalova@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

DIGITÁLNY OBSAH A JEHO PRÁVNÁ POVAHA V OBČIANSKOPRÁVNÝCH VZŤAHOCH. KOMPARATÍVNA ANALÝZA PRÁVNEJ ÚPRAVY SLOVENSKA A POĽSKA

DIGITAL CONTENT AND ITS LEGAL NATURE IN CIVIL LAW: A COMPARATIVE STUDY OF SLOVAKIA AND POLAND

Karin Raková¹, Ewa Lewandowska²

Abstrakt: Článok skúma právnu povahu digitálneho obsahu v občianskoprávných vzťahoch na pozadí harmonizačného rámca EÚ, najmä smernice (EÚ) 2019/770, a jeho transpozície v slovenskom a poľskom práve. Pozornosť sa sústreďuje na pojmové vymedzenie digitálneho obsahu a na otázku jeho kvalifikácie ako veci, práva a inej majetkovej hodnoty. Komparácia poukazuje, že vnútroštátne úpravy sú primárne koncipované pre B2C situácie, hoci digitálny obsah reálne vystupuje aj v B2B a C2C vzťahoch.

Kľúčové slová: digitálny obsah, vec s digitálnym prvkom, § 119a OZ, občianskoprávne vzťahy

Abstract: The article examines the legal nature of digital content in civil law relations in the context of the EU harmonization framework, in the light of Directive (EU) 2019/770 and its transposition into Slovak and Polish law. It focuses on the conceptual definition of digital content and its classification as a thing, right, or other property value. The comparison shows that national regulations are designed primarily for the B2C environment, although in practice digital content also exists in B2B and C2C relationships.

Keywords: digital content, goods with digital elements, civil-law relations, B2B, B2C

Introduction

The continuous development of new technologies, accompanied by the discovery of previously unknown devices, internet services, and software applications, has created a need to examine the adequacy and relevance of existing legal solutions

¹ Univerzita Komenského v Bratislave, Právnická fakulta

² University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration

relating to digital content. The dynamics of technological progress have led to the formation of a new term – *digital content*, which in most cases has no material equivalent.

The purpose of this article is to analyze *de lege lata* options for dealing with the digital content and to present proposals *de lege ferenda*. In addition to theoretical principles, special attention is paid to practical aspects that prove the importance and relevance of this issue.

Digital content in EU law

Digital content is a concept that deserves special attention, as digital technologies have become a new phenomenon that shapes everyday life and influences social interactions and legal relationships. The legislative approach to digital content EU legislation, particularly in Slovakia and Poland, has so far been limited mainly to the area of consumer law, focusing on contractual relations between traders and consumers. However, the scope of this issue clearly goes beyond consumer protection. Broader questions of private law arise that require systematic analysis in a comparative context.

It should be noted that the issue of digital content *per se* has been recognised by the EU legislature. The result was the adoption of Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter the "Digital Content Directive"), whose purpose is to harmonise the rules governing such contracts within the EU, primarily in consumer relations. Harmonisation proved necessary in particular because of the cross-border nature of distance and online commerce, especially contracts concluded remotely via websites. Article 2(1) of the Digital Content Directive defines "*digital content*" as "*data which are produced and supplied in digital form.*"

Definition of digital content in Slovak and Polish law Slovak Law

Under the Slovak law, the definition of *digital content* was implemented with effect from 1 July 2024 by Act No. 108/2024 Coll. on Consumer Protection and on Amendments to Certain Acts (hereinafter „Act on consumer protection“). Section 119a of the Act No. 40/1964 Coll. Civil Code, as amended („hereinafter „Civil Code or CC“) defines *digital content* as „*data produced and supplied in digital form.*“ Typical examples of *digital content* include e-books, films and sound recordings made available either on a tangible carrier (e.g. a DVD or USB drive) or by intangible digital transmission, i.e. by download from an online environment. *Digital content* is intangible, it can be reproduced repeatedly and stored on various media. In theory, it may be accessible to an unlimited circle of users. It may arise secondarily (e.g. by

digitising an analogue form) or primarily (e.g. by programming). It may be created directly by a human or generated by programmed devices, including with the use of artificial intelligence. When defining the term *digital content*, differences can be identified between Slovak law which defines *digital content* as (*údaje*) and the wording of the Digital Content Directive, which defines *digital content* to be *records* (*dáta*). In this context, a discussion may arise as to whether the terms *data* and *records* can be considered synonymous or not. We do not regard such different terminology as favourable.³

Also in our opinion, the provisions of *digital content* according to the CC do not address all issues connected with digital content as they focus primarily on consumer law aspects and electronic commerce. On this basis, the definition introduced in Section 119a may serve as an interpretative benchmark for determining whether a given asset qualifies as digital content. However, the current legal framework regulates *digital content* within private law relationships and is sufficiently general to remain applicable for some time in the future. However, the legal framework only applies to relationships between consumers and traders. It is clear, however, that digital content also occurs in B2B and C2C relationships. Despite of this fact, we believe that the above definition of *digital content* is broad enough to cover digital content in private law relationships and general enough to remain applicable for some time to come. This conclusion is also confirmed by legal doctrine. The legal nature of *digital content* has not yet been the subject of systematic analysis in Slovak legal doctrine. Legal doctrine has so far concentrated primarily on issues related to consumer protection, particularly on contracts for the supply of digital content.⁴ At the same time, part of the legal doctrine has also examined *digital content* from the

³ FILIČKO VLADIMÍR: *Vec/Tovar s digitálnymi prvkami a spotrebiteľské zmluvy s digitálnym plnením*. In: STUDIA IURIDICA Cassoviensia. Vol. 13, 2025, No. 2., s. 26, ISSN 1339-3995. Dostupné na: https://sic.pravo.upjs.sk/ecasopis/132025-2/2_Filicko_Vec_s_digitalnym_obsahom.pdf

⁴ From the consumer protection aspect the subject of digital content has been addressed by Mauks in his article *Vybrané zmeny spotrebiteľského práva v Občianskom zákonníku v roku 2024*, where he analyses types of contracts for digital performance in which digital content constitutes the contractual performance subject to consumer protection under the Consumer Protection Act, as well as those excluded from such protection despite having digital content as their subject matter. Mauks further points out the need to consider the specific features of Slovak legal regulation, which, in our opinion, should equally apply to the legal treatment of digital content from the perspective of its legal nature. MAUKŠ, DÁVID.: *Vybrané zmeny spotrebiteľského práva v Občianskom zákonníku v roku 2024*. In: *Banskobystrické zámocké dni práva: zborník zo 7. ročníka medzinárodnej vedeckej konferencie*. Banská Bystrica : Univerzita Mateja Bela v Banskej Bystrici. Belianum, 2025. s. 695 – 696. ISBN 978-80-557-2232-0.

perspective of its capacity to be the object of inheritance, which demonstrates that the issue extends into broader private-law relations.⁵

Goods with digital elements⁶

The term *goods with digital elements* means tangible things that either contain digital content or a digital service, or are so linked to them that, without such content or service, they would be incapable of performing their intended function.

Section 119a(2) and (3) of the Civil Code provide statutory definitions of digital content and digital service:

- **Digital content** (Section 119a(2)) means data produced and supplied in electronic form. This includes, in particular, software programs, operating systems, mobile applications, e-books, video games and other products of a digital nature. For the purposes of Section 118(1) of the Civil Code, digital content may be subsumed under the category of **other property values**, as it has economic value and may be the object of legal relations.
- **Digital service** (Section 119a(3)) means a service that creates a digital environment enabling the user (i) to create, process or store data in digital form or to gain access thereto; or (ii) to exchange digital data and otherwise interact with data created or uploaded by the user or by other users of the service. Typical examples include cloud storage, online communication platforms (including e-mail services), social networks and gaming portals.

Typical goods with digital elements are „*smart*“ technologies, especially smartphones and televisions. The classification criteria are met where: (a) the absence of the digital content or digital service would prevent the goods from being used with all stipulated or reasonably expected functions; or

⁵ See RAKOVÁ ŠIMONIOVÁ KARIN: *Digitálne dedičstvo ako nová výzva v notárskej praxi*. In: *Ars Notaria*. Roč. 28, č. 2/2025, s. 12-17. ISSN 1335-2229, also FICOVÁ SVETLANA, KRIŽAN MARTIN, FEKETE IMRICH, HAMŘIK MARTIN, IVANČO MAREK, KLINCOVÁ, ZUZANA, RAKOVÁ KARIN: *Zásadná reforma dedičského práva – nevyhnutnosť či nepodstatnosť?* Bratislava : Wolters Kluwer ČR, 2023, 392 s, ISBN 978-80-7676-866-6 (pdf).

⁶ With effect from 1 July 2024, Act No. 108/2024 Coll. on Consumer Protection and on Amendments to Certain Acts implemented Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services (the “Digital Content Directive”). By the same act, a new concept was introduced into the Civil Code in Section 119a “*goods with digital elements*” meaning any movable thing that contains digital content or a digital service, or is connected with such content or service in a manner such that, in its absence, the thing would be unable to perform its functions.

Source: Explanatory Report to Act No. 108/2024 Coll. on Consumer Protection and on Amendments to Certain Acts, available at: <https://www.najpravo.sk/dovodove-spravy/rok-2024/dovodova-sprava-k-zakonu-c-108-2024-z-z.html>

(b) the digital content or digital service is supplied with the goods as a single package, as also provided for in the contract of sale.

The following are not regarded as goods with digital elements: digital content stored on a tangible medium (e.g. a DVD). Likewise, applications that can be downloaded to the goods and are not necessary for their basic use are treated as separate digital content, not as part of the goods with digital elements.

The category is not exhaustively listed and presently covers a wide range of products, such as smartphones, smart watches, televisions, gaming consoles, smart lighting and thermostats. By contrast, immovables are not goods with digital elements, even if equipped with smart features. Nor are live animals covered, even where permanently identified by a transponder (chip).

Digital content under the Polish law

Digital Content Directive was implemented into the Polish legal system by the Act of 4 November 2022 amending the Act on Consumer Rights, the Civil Code, and the Act on Private International Law⁷. Based on Article 1 of the aforementioned Act, amendments were introduced to the Act of 30 May 2014 on Consumer Rights⁸. This Act on Consumer Rights, not the Civil Code⁹, contains the definition of digital content. The concept of digital content has therefore been clearly defined for the purposes of consumer law (here, specifically, the need for regulation arose). However, the legislator did not limit its application. According to a systematic interpretation, this concept can be broadly applied to private law.

Pursuant to Art. 2 (section 5) of the Act on Consumer Rights, digital content is understood "*as data produced and supplied in digital form.*"¹⁰ This definition has a wide scope of application. The doctrine indicates that digital data are those which decoding and processing into information requires the use of appropriate IT devices

⁷ Journal of Law 2022, item 2337, compare implementation in other legal systems: KULL, Irene: Transposition Of The Digital Content Directive (EU) 2019/770 Into Estonian Legal System, In: Journal of Intellectual Property, Information Technology and E-Commerce Law Vol. 12 (2), 2021, p. 249-259, also: DIDŽIULIS, Laurynas: EU Digital Content Directive And Evolution Of Lithuanian Contract Law, In: Journal of Intellectual Property, Information Technology and E-Commerce Law Vol. 12 (2), 2021, p. 260-270.

⁸ Journal of Law 2024, item 1796.

⁹ Act of April 23, 1964, The Civil Code (consolidated text, Journal of Law of 2025, item 1071, as amended), hereinafter: Civil Code.

¹⁰ The definition of digital content in the context of the directive is developed by: CHACÓN, Ignacio Fernández, Some considerations on the material scope of the new digital content directive: Too much to work out for a common European framework, In: European Review of Private Law No. 29 (3), 2021, p. 517-544, DOI: 10.54648/erpl2021026.

and software¹¹. Furthermore, their production and supply in digital form is a necessary condition¹². Digital content includes computer programs, applications, video files, audio files, music files, electronic games, e-books, or other electronic publications available for both downloading and streaming¹³. The legislator distinguishes between digital content delivered to the consumer on a tangible medium (e.g., DVDs or CDs) and digital content delivered in other ways¹⁴.

What is important, the Polish law has expanded the subjective scope of the Consumer Rights Act (including the issue of digital content)¹⁵. Specifically, it has also granted consumer protection to a natural person concluding a contract directly related to their business activity, when the content of that contract indicates that it is not of a professional nature for that person, arising in particular from the subject of their business activity, made available under the provisions on the Central Registration and Information on Business (Article 7aa). In practice digital content is also available in B2B and C2C relations¹⁶ (although their legal definition is contained for the purposes of consumer law).

Goods with digital elements

The Polish legislator has also defined a digital service (Article 2, paragraph 5a) and a good with digital elements (Article 2, paragraph 5b). According to the aforementioned provisions, a digital service is a service that enables the consumer to: a) produce, process, store, or access digital data; b) share digital data that has been sent or produced by the consumer or other users of the service; c) engage in other forms of interaction using digital data (Article 2, paragraph 5a). The Act does not contain examples of digital services, therefore the guidelines contained in the

¹¹ CHAŁUBIŃSKA-JENTKIEWICZ, Katarzyna: Treści cyfrowe jako przedmiot obrotu gospodarczego - zagadnienia definicyjne, In: internetowy Kwartalnik Antymonopolowy i Regulacyjny no 2(9), 2020, p. 111,

¹² LUBASZ, Dominik, CHOMICZEWSKI, Witold, MACIERZYŃSKA-FRANASZCZYK D. Lubasz, W. Chomiczewski, E. Macierzyńska-Franaszczyk, Elwira, MATYSIAK, Wiktor P., Commentary to art. 2, In: Ustawa o prawach konsumenta. Komentarz, M. Namysłowska (ed.), Warsaw 2025, Lex database, ISBN: 978-83-8390-322-4.

¹³ SIWICKI, Maciej: Kilka uwag na temat nowelizacji ustawy o prawach konsumenta i ustawy - Kodeks cywilny w związku z implementacją dyrektywy cyfrowej, In: Monitor Prawniczy no 5, 2024, p. 275-283.

¹⁴ JAROSZEK, Agata, KACZMAREK-TEMPLIN, Berenika, STEC, Piotr, SZOSTEK, Dariusz, ZAŁUCKI, Mariusz: Commentary to art. 2, In: *B. Kaczmarek-Templin, P. Stec, D. Szostak* (ed.), Ustawa o prawach konsumenta. Kodeks cywilny (wyciąg). Komentarz, Warsaw 2024, Legalis database, ISBN: 978-83-8235-814-8.

¹⁵ POŁUDNIAK-GIERZ, Katarzyna: Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim, In: Prawo w działaniu. Sprawy cywilne no. 54, 2023, p. 178. DOI: 10.32041/pwd.5406

¹⁶ ZWOLIŃSKA, Aneta: Treści cyfrowe w urządzeniach mobilnych, In: Prawo Mediów Elektronicznych no. 1, 2017, p. 45-50.

provisions of the directives should be followed¹⁷. It can be assumed that the examples of digital services coincide with those listed in recital 19 of Digital Content Directive, i.e. including software-as-a-service, such as video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media.

A good with digital elements is a good that contains or is connected to digital content or a digital service in such a way that the absence of the digital content or digital service would prevent it from functioning properly. The existence of a functional link between a good and digital content or a digital service is the essence of the definition. This means that a good devoid of digital content or a digital service functions improperly. Therefore, media used solely for recording and delivering digital content (e.g., DVDs, memory cards) do not fall within the definition¹⁸. Examples of goods with digital elements include smartphones and game consoles. It is indicated that the above-mentioned provisions should be interpreted broadly, taking into account changes taking place in technical solutions¹⁹.

Conclusion

A comparison of Slovak and Polish legislation indicates that both jurisdictions have transposed the Digital Content Directive with a primary focus on consumer law, but use slightly different legislative techniques and terminology. In Slovakia, the definition of digital content has been incorporated into the Civil Code and refers to "*údaje produced and delivered in electronic form*." However both the Directive and the Polish Consumer Rights Act use the broader terms "*dáta produced and delivered in digital form*". This terminological difference is not only linguistic in nature, but may also have implications for interpretation. The Slovak wording, which uses the term "*údaje*" (which has a slightly narrower meaning in legal and everyday Slovak), could be interpreted as more restrictive than the term "*dáta*" used at EU level and in Polish law. The Polish approach is therefore more in line with the wording of the Directive and leaves less room for restrictive interpretation.

¹⁷ JAROSZEK, Agata, KACZMAREK-TEMPLIN, Berenika, STEC, Piotr, SZOSTEK, Dariusz, ZAŁUCKI, Mariusz: Commentary to art. 2, In: *B. Kaczmarek-Templin, P. Stec, D. Szostak* (ed.), *Ustawa o prawach konsumenta. Kodeks cywilny (wyciąg). Komentarz*, Warsaw 2024, Legalis database, ISBN: 978-83-8235-814-8.

¹⁸ Lubasz, W. Chomiczewski, E. Macierzyńska-Franaszczyk, Elwira, MATYSIAK, Wiktor P., Commentary to art. 2, In: *Ustawa o prawach konsumenta. Komentarz*, M. Namysłowska (ed.), Warsaw 2025, Lex database, ISBN: 978-83-8390-322-4.

¹⁹ DYBKA, Wojciech, GÓRNIAK, Kacper, OLCZYK, Magdalena, PECYNA, Marlena, RACHWAŁ, Anna, WANAT Emanuel, WIELGUS, Kamil: Commentary to art. 2, In: *M. Pecyna* (ed.), *Ustawa o prawach konsumenta. Komentarz*, wyd. 1, Warsaw 2025, Legalis database, ISBN: 978-83-8356-870-6.

Apart from this terminological difference, both jurisdictions extend the concept of digital content to civil law relations, including a wide range of products such as software, applications, e-books, video and audio files, and streaming services. Both also recognize the category of „*goods with digital elements*“ and „*digital services*.“ However, Slovak law explicitly places the definition in the CC, linking it to categories of private law (in particular, „*other property values*“ under Section 118 of the Civil Code), while Polish law places the definition in the Consumer Rights Act but extends the subjective scope of consumer protection to certain natural persons engaged in business activities.

Although Slovak and Polish law are consistent at the conceptual level, terminological differences („údaje“ versus „data“) and the systematic placement of provisions reflect different legislative decisions. These differences may influence the future interpretation of the term „digital content“ in private law relationships outside the context of consumer law, particularly in the case law of national courts.

Civil law character of digital content

Slovak legal regulation

Despite the above, the legal regulations concerning digital content included in the CC do not cover all issues related to digital content, as they deal exclusively with aspects of consumer law and e-commerce issues. However, we believe that despite of this fact, digital content should not be limited exclusively to relations between consumers and traders, but should also be applicable to the relations between natural persons acting outside the consumer context, as well as to other civil law relations.²⁰ For the issue of civil law relationships, it is important that, when using the relevant software and equipment, the user creates and provides data in digital form, unlike an entrepreneur, as is the case in a consumer relationship. For example, when using social networks, users upload photos, post comments, messages, videos, or documents, provide self-created digital data, and in this way deliver digital content to the servers of the administrators of these social networks.

²⁰ However, MAUKŠ DÁVID in his article *Inheritance of Intangible Assets* states that according to the amendment to the Civil Code effective from July 1, 2024, an object with digital elements is exclusively a movable thing (based on consistent case law, the term „thing“ refers only to a tangible object, known as *res corporalis*), which contains any digital elements. See more: MAUKŠ DÁVID: *DEDENIE NEHMOTNÝCH STATKOV*. In: *Nehmotné statky interdisciplinárne*. MARTIN DAŇKO, ALOJZ VYČISLÍK, VERONIKA ŤAŽKÁ (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024.

140 s. ISBN 978-80-7160-735-9. p. 42 – 43.

Digital content as a thing

According to legal doctrine, a *thing* in the legal meaning is understood to be exclusively a tangible object (*res corporales*) or natural forces, provided that they are controllable and useful to humans.²¹ In addition to the above, the thing must be permitted by law as an object of property rights, whereby not every thing that is useful and controllable can be the subject of civil law disposition due to its specific nature, given the existence of restrictions arising mainly from public law regulations. These include, for example, weapons, ammunition, poisons, human organs, etc., which can be considered objects in the general sense, but are excluded from civil law disposition due to the fact that their legal regime is subject to special restrictions. In summary, legal theory and case law consider only tangible objects to be things in the legal sense, while rights and other property values, which the Civil Code distinguishes as separate categories of objects of civil law relations, are not considered things. *De lege lata*, rights, other property values, apartments, and non-residential premises cannot be classified as things in the legal sense, as they are separate objects of civil law relationships according to Section 118 of the CC. *De lege ferenda* its necessary to include definition of things as tangible and intangible and

Digital content as a right

The subject matter of civil law relationships can be interpreted as everything to which the subjective rights and obligations of the participants in these relationships apply. In this regard, it can be stated that if digital assets consist of rights, these rights may be the subject matter of civil law relationships. In view of this, it can be stated that if digital property consists of rights, these rights may be the subject of civil law relationships. We believe, that the assessment of whether a particular right can be the subject of a civil law relationship must always be carried out with regard to the nature of the right itself and, where applicable, the nature of the specific legal relationship.

Law as a subject of civil law relations may consist mainly of:

- (i) rights in rem,
- (ii) claims,
- (iii) rights to intangible assets.

²¹ LAZAR JÁN. a kol. *Občianske právo hmotné. Všeobecná časť*. Bratislava: IURIS LIBRI, 2018, s. 196, SKORKOVÁ VERONIKA. *II. Vec v právnom zmysle de lege lata*. In ŠTEVČEK, MAREK, DULAK ANTON, BAJÁNKOVÁ JANA, FEČÍK MARTIN, SEDLAČKO FRANTIŠEK, TOMAŠOVIČ MAREK a kol. *Občiansky zákonník I. § 1 – 450*. 2. vydanie. Komentár. Praha : C. H. Beck, 2019, s. 800, FEKETE IMRICH. *Občiansky zákonník. 1. zväzok (Všeobecná časť). Veľký komentár, 3. aktualizované vydanie*. Bratislava: Eurokódex, 2017, s. 955 – 956.

In the case of digital assets, these rights are that have property value and arise on the basis of a contractual relationship determining their content, scope, and conditions of exercise, in particular:

- licensing rights (e.g., right to use software),
- access rights to digital services (e.g., cloud storage account),
- rights of contractual origin (e.g., the right to use a digital product on a subscription basis).

Digital content as other property value

Digital content, as part of digital property, can be classified as other property value, considering the provisions of Section 119(1) of the Civil Code. From a legal point of view, this means that digital content can be a separate subject of private law relations, for example, it can be the subject of a contractual transfer, lien, inheritance, or it can be an enforceable claim in the event of a breach of contractual or copyright obligations. The decisive factor is not whether the digital content exists in physical form (e.g., on a USB stick).

Polish legal regulation

Digital content, under Polish law, has a specific legal nature. It is considered as intangible property, but as a new category of goods, it is subject to legal transactions (commerce). It is necessary to define what the digital content actually constitute within the meaning of civil law. Its status is currently the subject of debate in legal doctrine.

Digital content as a thing

Digital content is a subject of commerce, but it does not qualify as a tangible item (Article 45 of the Civil Code). Things, within the meaning of Civil Code, shall only be material objects (art. 45). According to the established view, things are tangible parts of nature in their original state or in a processed state that are sufficiently distinct (in a natural or artificial manner) that they can be treated in socio-economic relationships as separate goods²². There are various classifications of things²³. Neither category includes digital content. Separate categories of objects under civil law are not considered things.

²² WASILKOWSKI, Jan: *Zarys prawa rzeczowego*, Warsaw 1963, pp. 8–9.

²³ The main division is into movable and immovable property, more about, see: LEWANDOWSKA, Ewa: *Civil Law Relationship*, In: A. Bieranowski, E. Lewandowska (eds.) *Civil law institutions (general part and property law) according to Polish legal regulations*, Warsaw 2025, p. 37-38, ISBN: 978-83-8270-397-9.

Since digital content is not a thing, it is concluded that it cannot be owned (Art. 140 of the Civil Code)²⁴. Digital content, however, can have a tangible medium, in which case ownership rights exist. Typically, however, digital content is solely a digital recording, characterized by the fact that it can be accessed by multiple people at the same time. However, *de lege ferenda*, there is a need to consider transferring certain rules of property law to the category of digital content²⁵. There are suggestions for a broad interpretation of the concept of "property" (including intangible objects)²⁶.

Digital content as a right and property value

While only tangible objects can be subject to ownership (and possession), the object of civil law relationships can also be formed by something other than objects, namely tangible objects that are not things (e.g. minerals), intangible objects (e.g. energy, intellectual goods – in particular works in the meaning of Copyright Act) and an enterprise²⁷. Digital contents are object of contracts (for example delivery contract of an e-book), which clearly results from the Consumer Rights Act (Chapter: 5b). In accordance with Article 44 of the Civil Code²⁸, digital content is considered to be a property right other than ownership. The category of "other property rights" can include various civil property rights. Their subject matter can also be intangible objects²⁹. However, it is commonly accepted that the rights that serve to realize the economic interest of the entitled person are of a property nature. Meanwhile, economic value is not an inherent feature of digital content.

²⁴ More about legal aspects of digital content: WYCZIK, Jakub: Dobra wirtualne z perspektywy użytkowników i dostawców treści. Prawne uwarunkowania obrotu, Warsaw 2022, p. 57 et seq., ISBN: 978-83-8291-023-0, also: DYBKA, Wojciech, GÓRNIAK, Kacper, OLCZYK, Magdalena, PECYNA, Marlena, RACHWAŁ, Anna, WANAT Emanuel, WIELGUS, Kamil: Commentary to art. 2, In: *M. Pecyna* (ed.), Ustawa o prawach konsumenta. Komentarz, wyd. 1, Warsaw 2025, Legalis database, ISBN: 978-83-8356-870-6.

²⁵ DYBKA, Wojciech, GÓRNIAK, Kacper, OLCZYK, Magdalena, PECYNA, Marlena, RACHWAŁ, Anna, WANAT Emanuel, WIELGUS, Kamil: Commentary to art. 2, In: *M. Pecyna* (ed.), Ustawa o prawach konsumenta. Komentarz, wyd. 1, Warsaw 2025, Legalis database, ISBN: 978-83-8356-870-6.

²⁶ SOKOŁOWSKI, Tomasz, ŻOK, Krzysztof: Commentary to art. 44, In: *M. Gutowski* (ed.), Kodeks cywilny, t. 1, Warsaw 2021, Legalis, ISBN: 978-83-8235-251-1.

²⁷ LEWANDOWSKA, Ewa: Civil Law Relationship, In: *A. Bieranowski, E. Lewandowska* (eds.) Civil law institutions (general part and property law) according to Polish legal regulations, Warsaw 2025, p. 41, ISBN: 978-83-8270-397-9.

²⁸ Which states that the property shall be the right of ownership and other property rights.

²⁹ For example: PIECZABA, Joanna, WALCZAK, Dawid J.: Rozrządzanie treściami cyfrowymi na wypadek śmierci. Stan *de lege lata* i wnioski *de lege ferenda*, In: *Studia Prawa Prywatnego* no. 2, 2024, p. 63-82.

Conclusion

A comparative analysis of Slovak and Polish law confirms that both legal systems face the same fundamental problem: digital content does not fit into the traditional category of things (*res corporales*) in civil law, yet it undoubtedly functions as an object of trade and a subject of private law relations.

Slovak law expressly excludes the possibility of classifying digital content as a "*thing*" in the legal sense, in accordance with the Civil Code's strong distinction between tangible things and other property values. Instead, digital content is classified as "*other property values*" within the meaning of Section 118 of the CC, which gives it as a subject of contractual transfer, inheritance, security rights, or enforcement. At the same time, depending on its nature, digital content may give rise to relative rights of a contractual nature, such as licenses or access rights, rather than absolute property rights.

Similarly, under Polish law, digital content is not considered a "*thing*" within the meaning of Article 45 of the CC and therefore cannot be the subject of ownership in the strict sense of civil law. Instead, it is classified as intangible property and, under Article 44 of the CC, is treated as a property right other than ownership. Polish doctrine recognizes that digital content can be the subject of contracts and legal acts, but the prevailing view emphasizes its nature as intangible property, which belongs to the broader category of property rights.

Both legal systems shows that digital content must be understood as a *sui generis* category of intangible property: not a "*thing*" subject to ownership, but nonetheless a legally protected asset that can constitute the object of private-law relations. The Slovak solution, by explicitly classifying digital content under the category of other property values, provides a systematic basis within the CC, whereas the Polish approach emphasises its qualification as an intangible property right. Despite these differences, both jurisdictions agree that digital content, although intangible and incapable of possession, has legal significance as an object of private-law relations and requires recognition extending beyond the consumer-law framework.

List of references

1. CHACÓN, Ignacio Fernández, Some considerations on the material scope of the new digital content directive: Too much to work out for a common European framework, In: *European Review of Private Law* No. 29 (3), 2021, p. 517-544, DOI: 10.54648/erpl2021026.
2. CHAŁUBIŃSKA-JENTKIEWICZ, Katarzyna: Treści cyfrowe jako przedmiot obrotu gospodarczego - zagadnienia definicyjne, In: *internetowy Kwartalnik Antymonopolowy i Regulacyjny* no 2(9), 2020, p. 111.

3. DIDŽIULIS, Laurynas: EU Digital Content Directive And Evolution Of Lithuanian Contract Law, In: Journal of Intellectual Property, Information Technology and E-Commerce Law Vol. 12 (2), 2021, p. 260-270.
4. DYBKA, Wojciech, GÓRNIAK, Kacper, OLCZYK, Magdalena, PECYNA, Marlena, RACHWAŁ, Anna, WANAT Emanuel, WIELGUS, Kamil: Commentary to art. 2, In: M. Pecyna (ed.), Ustawa o prawach konsumenta. Komentarz, wyd. 1, Warsaw 2025, Legalis database, ISBN: 978-83-8356-870-6.
5. FICOVÁ SVETLANA, KRIŽAN MARTIN, FEKETE IMRICH, HAMŘIK MARTIN, IVANČO MAREK, KLINCOVÁ, ZUZANA, RAKOVÁ KARIN: *Zásadná reforma dedičského práva – nevyhnutnosť či nepodstatnosť?* Bratislava : Wolters Kluwer ČR, 2023, 392 s, ISBN 978-80-7676-866-6 (pdf).
6. FILIČKO VLADIMÍR: *Vec/Tovar s digitálnymi prvkami a spotrebiteľské zmluvy s digitálnym plnením*. In: STUDIA IURIDICA Cassoviensia. Vol. 13, 2025, No. 2., s. 26, ISSN 1339-3995. Dostupné na: https://sic.pravo.upjs.sk/ecasopis/132025-2/2_Filicko_Vec_s_digitalnym_obsahom.pdf
7. JAROSZEK, Agata, KACZMAREK-TEMPLIN, Berenika, STEC, Piotr, SZOSTEK, Dariusz, ZAŁUCKI, Mariusz: Commentary to art. 2, In: B. Kaczmarek-Templin, P. Stec, D. Szostak (ed.), Ustawa o prawach konsumenta. Kodeks cywilny (wyciąg). Komentarz, Warsaw 2024, Legalis database, ISBN: 978-83-8235-814-8.
8. JAROSZEK, Agata, KACZMAREK-TEMPLIN, Berenika, STEC, Piotr, SZOSTEK, Dariusz, ZAŁUCKI, Mariusz: Commentary to art. 2, In: B. Kaczmarek-Templin, P. Stec, D. Szostak (ed.), Ustawa o prawach konsumenta. Kodeks cywilny (wyciąg). Komentarz, Warsaw 2024, Legalis database, ISBN: 978-83-8235-814-8.
9. KULL, Irene: Transposition Of The Digital Content Directive (EU) 2019/770 Into Estonian Legal System, In: Journal of Intellectual Property, Information Technology and E-Commerce Law Vol. 12 (2), 2021, p. 249-259.
10. LEWANDOWSKA, Ewa: Civil Law Relationship, In: A. Bieranowski, E. Lewandowska (eds.) Civil law institutions (general part and property law) according to Polish legal regulations, Warsaw 2025, p. 37-38, ISBN: 978-83-8270-397-9.
11. LUBASZ, Dominik, CHOMICZEWSKI, Witold, MACIERZYŃSKA-FRANASZCZYK D. Lubasz, W. Chomiczewski, E. Macierzyńska-Franaszczyk, Elwira, MATYSIAK, Wiktor P., Commentary to art. 2, In: Ustawa o prawach konsumenta. Komentarz, M. Namysłowska (ed.), Warsaw 2025, Lex database, ISBN: 978-83-8390-322-4.
12. MAUKŠ, DÁVID: *Vybrané zmeny spotrebiteľského práva v Občianskom zákonníku v roku 2024*. In: *Banskobystrické zámocké dni práva : zborník zo 7. ročníka medzinárodnej vedeckej konferencie*. Banská Bystrica : Univerzita Mateja Bela v Banskej Bystrici. Belianum, 2025. s. 687-699, ISBN 978-80-557-2232-0.
13. MAUKŠ DÁVID: *DEDENIE NEHMOTNÝCH STATKOV*. In: *Nehmotné statky interdisciplinárne*. MARTIN DAŇKO, ALOJZ VYČISLÍK, VERONIKA ŤAŽKÁ

(zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024, 140 s., ISBN 978-80-7160-735-9.

14. PIECZABA, Joanna, WALCZAK, Dawid J.: Rozrządzanie treściami cyfrowymi na wypadek śmierci. Stan *de lege lata* i wnioski *de lege ferenda*, In: Studia Prawa Prywatnego no. 2, 2024, p. 63-82.
15. POŁUDNIAK-GIERZ, Katarzyna: Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim, In: Prawo w działaniu. Sprawy cywilne no. 54, 2023, p. 178. DOI: 10.32041/pwd.5406.
16. RAKOVÁ ŠIMONIOVÁ KARIN: *Digitálne dedičstvo ako nová výzva v notárskej praxi*. In: *Ars Notaria*. Roč. 28, č. 2/2025, s. 12-17. ISSN 1335-2229.
17. SIWICKI, Maciej: Kilka uwag na temat nowelizacji ustawy o prawach konsumenta i ustawy - Kodeks cywilny w związku z implementacją dyrektywy cyfrowej, In: Monitor Prawniczy no 5, 2024, p. 275-283.
18. SOKOŁOWSKI, Tomasz, ŻOK, Krzysztof: Commentary to art. 44, In: M. Gutowski (ed.), Kodeks cywilny, t. 1, Warsaw 2021, Legalis, ISBN: 978-83-8235-251
19. WASILKOWSKI, Jan: Zarys prawa rzeczowego, Warsaw 1963, pp. 8–9.
20. WYCZIK, Jakub: Dobra wirtualne z perspektywy użytkowników i dostawców treści. Prawne uwarunkowania obrotu, Warsaw 2022, p. 57 et seq., ISBN: 978-83-8291-023-0.
21. ZWOLIŃSKA, Aneta: Treści cyfrowe w urządzeniach mobilnych, In: Prawo Mediów Elektronicznych no. 1, 2017, p. 45-50.

Contact details

JUDr. Ing. Karin Raková, PhD., MBA:

karin.rakova@flaw.uniba.sk

Právnická fakulta Univerzity Komenského v Bratislave

Ewa Lewandowska, PhD

e.lewandowska@uwm.edu.pl

University of Warmia and Mazury in Olsztyn

Faculty of Law and Administration

Department of Civil Law and Private International Law

ARTIFICIAL INTELLIGENCE, REAL PROBLEMS: CONSUMER REMEDIES FOR NON-CONFORMITY

Tjaša Kalin¹

Abstract: Artificial intelligence is becoming an indispensable part of the digital economy, bringing numerous advantages to business and consumers alike, including greater efficiency, speed and improved quality of services, and user experiences. However, its development also raises challenges for the legal framework of the EU and national legal orders, mainly in three key areas: fundamental rights, product safety and liability, and consumer protection. This paper focuses on consumer protection, specifically in cases where artificial intelligence is the subject of the contract. It may be part of smart goods or independent digital content or service, such as automated translation services, monitoring technologies, smart health applications, robotic vacuum cleaners or smart refrigerators. EU legislation in this field includes two directives: Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, and Directive 2019/771 on certain aspects concerning contracts for the sale of goods. The central question is what level of quality can consumers expect from products, digital content or services based on artificial intelligence. In other words, when are such products, digital content or services considered non-conforming with the contract and what legal remedies are available to the consumers?

Keywords: consumer protection, artificial intelligence, non-conformity, remedies

Introduction

Despite regulatory developments in the field of artificial intelligence (AI), relatively little attention has been paid to consumer AI products. While much of the debate has focused on fundamental rights, product safety and liability, there is still significant room to further examine the consumer law dimension. With regard to contractual liability for consumer AI products, legal rules designed for AI systems have not yet been developed at the international or national level.²

¹ Institute for Comparative Law at the Faculty of Law in Ljubljana

² Durovic, p. 53.

Consumers are able to purchase products that use AI to assist them in their day-to-day lives.³ The AI available to consumers is usually embedded in everyday devices enhanced with networked capacity or in readily available apps and websites.⁴ Such products might include internet of things or smart devices such as smart refrigerators, vacuum cleaners, sensors that control lighting and heating, doorbells that monitor visitors, etc.⁵ More interactive are digital assistants such as Amazon's Alexa, Google's Google Assistant, Apple's Siri and Samsung's Bixby.⁶ While AI systems may usually provide excellent results, they are also prone to making mistakes that no human being would make.⁷ In the context of contractual liability for AI systems, it should be noted that even a perfectly functioning AI system is inherently prone to producing erroneous output.⁸

This paper addresses the legal questions that arise in cases where AI is the subject matter of the contract, as part of goods with digital elements or as individual digital content or digital service. It examines whether existing European Union (EU) consumer law is equipped to deal with such situations. The analysis focuses on issues connected to conformity of AI consumer products and remedies in cases of non-conformity.

Legal framework

The EU adopted two directives that are relevant in connection with consumer AI products, since they deal with the sale of goods with digital elements and supply digital content or digital services. The first is Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (DCD)⁹ and the second is Directive 2019/771 on certain aspects concerning contracts for the sale of goods (SGD).¹⁰ The directives are based on the principle of full harmonisation and cover some aspects of contracts for the mentioned products, in particular conformity requirements and remedies in cases of non-conformity. Although the scope and substantive rules of the directives are intended to be technologically neutral and

³ Paterson, Maker, p. 114.

⁴ *Ibidem*.

⁵ *Ibidem*.

⁶ *Ibidem*.

⁷ Claes, Herbosch, p. 469.

⁸ *Ibidem*, p. 470.

⁹ Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019, pp. 1–27.

¹⁰ Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019, pp. 28–50.

future-proof¹¹, it is noteworthy that neither include specific provisions or a reference to emerging technologies such as AI.¹² Ebers highlights that none of the existing consumer directives contain provision addressing the specific risks posed by AI systems, resulting in a number of regulatory gaps in the current EU consumer law, amongst other missing standards for assessing whether or not AI systems comply with the objective conformity requirements.¹³

The delineation of SGD and DCD

The first question to be addressed is whether AI, as a product, falls within the scope of the directives. Both directives have the same definitions of goods with digital elements, digital content and digital services. Digital content means data which are produced and supplied in digital form,¹⁴ while digital service means a service that allows the consumer to create, process, store or access data in digital form or a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service. Recital 19 of DCD illustrates the concept of digital content by listing examples such as computer programmes, applications, video files, audio files, music files, digital games, e-books or other e-publications. The definition of digital service includes also software-as-a-service, such as video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media.¹⁵

Goods with digital elements are defined as any tangible movable items that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions.¹⁶ Recital 14 of SGD provides an example for incorporated or inter-connected digital content such as operating systems, applications and any other software. It also lists examples of incorporated or inter-connected digital services, including software-as-a-service offered in the cloud computing environment, the continuous supply of traffic data in a navigation system, or the continuous supply of individually adapted training plans in the case of a smart watch.

Considering the above definitions, the scope of the directives is very wide. While the notion of software was present in the proposal of DCD¹⁷ at the core of the definition

¹¹ Recital 19 of DCD.

¹² Ebers (2021), p. 204.

¹³ Ebers (2023), p. 216.

¹⁴ Articles 2(1) and 2(2) of DCD, Articles 2(6) and 2(7) of SGD.

¹⁵ Recital 19 of DCD.

¹⁶ Article 2(3) of DCD, Article 2(5)(b) of SGD.

¹⁷ COM/2015/0634 final.

of digital content,¹⁸ it is not included in the final text of DCD.¹⁹ However, authors still explicitly state that the scope of DCD also applies to software,²⁰ which includes AI. A product containing or powered by AI falls within the scope of SGD if it qualifies as a part of a good with digital elements, or within the scope of DCD if it is regarded as an individual digital content or digital service.

The two directives are mutually exclusive. For the purposes of this paper, the precise delineation is not crucial, however, it should be noted that there are certain differences between the directives. The most significant difference lies in the addressee of potential remedies for non-conformity of smart products, depending on whether digital content or service is considered as a part of a good with digital elements or as a separate supply.²¹ If the SGD is applicable, the seller of the good will be responsible for the functioning of incorporated or inter-connected digital content or digital service, whereas if the DCD is applicable, the functioning will be the responsibility of the trader of the digital content or digital service. The SGD will be applicable under two cumulative conditions. Firstly, digital content or digital service must be incorporated or inter-connected with the good in such a way that its absence would prevent the good from performing its functions.²² Secondly, digital content or digital service must be provided with the goods under the sales contract, irrespective of whether such content or service is supplied by the seller or by a third party.²³ In the event of doubt, it shall be presumed that the supply of digital content or digital service forms part of the contract.²⁴

The delineation is difficult in cases of multi-party situation, where the consumer buys a good from a seller but concludes an additional licensing contract with the digital content or digital service provider.²⁵ The key factor of the delineation is the content of the contract,²⁶ where the advertising of the product is also taken into account. For example, if a smart TV is advertised as having “Google Assistant integrated”, then the seller is liable for the operating system as well as the functioning of the Google Assistant service.²⁷

¹⁸ The proposed definition of digital content included: data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software.

¹⁹ Gellert, p. 409.

²⁰ *Ibidem*, p. 412.

²¹ Regardless if the digital content or digital service in question is AI or not.

²² This condition stems from the definition of a good with digital element (Article 2(5)(b) of SGD) and Article 3(3) of SGD.

²³ Article 3(3) of SGD.

²⁴ *Ibidem*.

²⁵ Sein, p. 24.

²⁶ Ebers (2020), p. 216.

²⁷ Sein, p. 25.

Regardless of how the two directives are delineated, AI consumer products will inevitably fall within the scope of one of them.

Conformity requirements

Both directives regulate conformity requirements and remedies for non-conformity in a similar way. An AI consumer product will be in conformity with the contract when it meets the subjective and objective requirements from the directives.

Article 6 of SGD and Article 7 of DCD regulate subjective requirements, which need to be fulfilled only if, and to the extent, they are agreed in the contract.²⁸ They are not exhaustive, because the parties may agree on other criteria and in essence, they are classified in four main categories.²⁹ Firstly, digital content, digital service or a good with digital elements is of the description, type, quantity and quality, and possesses the functionality, compatibility, interoperability and other features, as required by the sales contract. Secondly, it has to be fit for any particular purpose for which the consumer requires and made known to the seller at the latest at the time of the conclusion of the contract, and in respect of which the seller has given acceptance. Thirdly, it has to be delivered with all accessories and instructions, including on installation, as stipulated by the contract and, fourthly, it has to be supplied with updates or updated as stipulated by the contract.

The objective requirements for conformity are regulated by Article 7 of SGD and Article 8 of DCD. They contain statutory requirements that have to be fulfilled independently of contractual stipulations, which makes the objective requirements more important provisions of conformity than the subjective requirements.³⁰ The objective requirements can also be classified into four categories.³¹ Firstly, digital content, digital service or a good with digital elements has to be fit for the purposes for which products of the same type would normally be used, taking into account, where applicable, any existing EU and national law, technical standards or sector-specific industry codes of conduct. Secondly, when the trader makes available a trial version or preview of the digital content or digital service, they must comply with it and in the case of goods with digital elements, when the seller makes a sample or model available, the delivered goods must be of the same quality and correspond to the description.³² Thirdly, they must be supplied along with any accessories and instructions which the consumer may reasonably expect to receive. Fourthly, they must be of the quantity and possess the qualities and features, as well as in relation

²⁸ Staudenmayer, p. 112; Staudenmayer, Bertelmann, p. 372.

²⁹ Pazos, p. 338.

³⁰ Staudenmayer, p. 127; Staudenmayer, Bertelmann, p. 389.

³¹ Pazos, p. 338.

³² Pazos, pp. 338, 339.

to functionality, compatibility, security and durability for goods with digital elements, and accessibility and continuity for digital content or digital service, which are normal for items of the same type and which the consumer may reasonably expect.³³ When assessing reasonable expectations, the directives state that any public statement made by or on behalf of the seller of a good or trader of digital content or digital service, or other persons in previous links of the chain of transactions, should be taken into account.³⁴

An important novelty in the directives is that updates are taken into account in the conformity approach.³⁵ The directives provide an obligation of the trader and seller to ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep the digital content or digital service in conformity, in the prescribed period of time.³⁶ As for the period of time during which this has to be done, the directives make a distinction between a one-off or a series of individual acts of supply and the continuous supply of digital content or digital service.³⁷

The parties to a contract can always agree to subjective conformity requirements that go beyond the objective conformity requirements, while they cannot simply establish a lower standard than the objective requirements.³⁸ A lower standard is possible only if, at the time of the conclusion of the contract, the consumer was specifically informed that a particular characteristic of the good, digital content or digital service was deviating from the objective requirements for conformity and the consumer expressly and separately accepted that deviation when concluding the sales contract.³⁹ Therefore, when dealing with AI consumer products, it is not permissible for the business to attempt to exclude or limit its liability for AI systems through contract clauses defining the contractual performance in a way that is below the objective requirements for conformity.⁴⁰ For example, a business cannot point out that the AI system is beta software or a completely unpredictable system and avoid liability.⁴¹

³³ *Ibidem*, p. 339.

³⁴ Article 8(1)(b) of DCD and Article 7(2) of SGD lay down conditions when the trader or seller will not be bound by public statements.

³⁵ Staudenmayer, p. 149; Staudenmayer, Bertelmann, p. 411.

³⁶ Article 8(2) DCD and Article 7(3) of SGD.

³⁷ Staudenmayer, p. 149; Staudenmayer, Bertelmann, p. 411; Article 8(2) DCD, Article 7(3) of SGD.

³⁸ Ebers (2020), p. 217.

³⁹ Article 8(5) of DCD and Article 7(5) of SGD.

⁴⁰ Ebers (2021), p. 217.

⁴¹ *Ibidem*, p. 2017.

Conformity of consumer AI products

Consumer AI products are in conformity with the contract when they meet, if applicable, the subjective conformity requirements agreed in the contract and when they meet the statutory objective conformity requirements from the directives. Since the subjective conformity requirements depends on each individual contract, this paper focuses on questions raised in connection with the objective conformity requirements for consumer AI products.

The concept of objective conformity contains a list of different criteria, which the consumer can reasonably expect.⁴² However, when the goods and services are founded on AI systems, it is difficult to objectively measure whether this set of criteria is met, as the real-life application of AI is more complex than merely ticking a list of checkboxes.⁴³ When smart goods, content or services are based on AI systems, the question arises what features, qualities and performance must the AI systems comply with in order to meet objective requirements for conformity.⁴⁴ Ebers emphasizes that defining objective requirements for AI systems is a complicated task, especially when it comes to determining whether they are fit for the purposes for which the same type of system would normally be used, and how to assess whether they exhibit the quality and performance features normal for such systems that are reasonably expected by consumers.⁴⁵ He is of the opinion that such standards should not be defined by the courts on the basis of mere empirical findings and deems that a normative standard, which is not based on arbitrary subjective expectations, but on objective criteria, is necessary. While Article 8(1)(a) of DCD and 7(1)(a) of SGD refer to existing EU and national law and technical standards, there are currently no legal rules nor national or international technical standards specifically for AI systems.⁴⁶

Technical standards would provide a possible solution and guideline for determining conformity requirements for AI products. However, until they are adopted, the national courts still have to interpret the existing conformity requirements from the directives, which might prove to be a difficult task, particularly given that learning algorithms and adaptive behaviour can result in variable performances over time.

Ebers highlights that learning AI systems do not have static performance, as the performance constantly changes during operation.⁴⁷ A characteristic feature of these systems is that they are not based on “locked algorithms” that provide the same result each time the same output is applied to it. Instead, the algorithms rely on

⁴² Durovic, p. 53.

⁴³ *Ibidem*, p. 53.

⁴⁴ Ebers (2021), p. 217.

⁴⁵ Ebers (2021), p. 217.

⁴⁶ *Ibidem*, p. 217.

⁴⁷ *Ibidem*, p. 218.

machine learning, so that they can change and adapt over time due to their real-world experience. He concludes that the performance and quality of learning AI systems cannot be determined at a single point in time.

Additionally, AI consumer products are a relatively recent arrival on the market and are rapidly changing, which means consumers may have little experience with them.⁴⁸ This brings into question the objective conformity requirement that an AI consumer product must be of quality and have other features normal for the same type of product which the consumer may reasonably expect, given the nature of the product. Self-learning software does not seem prone to create many clear expectations among potential customers, and when expectations exist, they will be based mostly on pure subjective perceptions, largely influenced by statements made by traders, sellers or companies in previous links in chains.⁴⁹

Gellert dealt with the question of whether a suboptimal performance of an AI application can be appraised through the conformity criteria – can the autonomous nature of AI lead to a lack of conformity under the directives?⁵⁰ He presented his conclusions on the basis of DCD and Waze navigation application, which can be described as AI-enabled software. Unlike traditional GPS systems, Waze relies on real-time user data and autonomous algorithms, which have at times produced hazardous or counterproductive outcomes, such as directing drivers into wildfire zones or congesting residential areas. Gellert deems that two objective conformity requirements seem to be relevant – fitness for purpose and performance features. The fitness for purpose demands that the product can serve its intended function and it is determined through normal use. For a navigation application, the normal use would be for the purposes of navigation, regardless if it is AI-enabled or not. As for the performance features, they are assessed in relation to normal use and consumers' reasonable expectations. Here, it is relevant that Waze is marketed to "save time on every drive", which may reinforce expectations and render negative routing outcomes potentially as instances of non-conformity.

There are certain unresolved issues regarding conformity of digital content and services with the DCD, which was also demonstrated by Gellert through his analysis. His conclusions can also be applied to goods with digital elements and the conformity of incorporated or interconnected digital content and digital services.

As one possible solution for conformity requirements for AI products, some authors suggest that the conformity requirements should only be subjective or that subjective requirements should have the main role for assessing whether such a

⁴⁸ Paterson, Maker, p. 117.

⁴⁹ Pazos, p. 344.

⁵⁰ Gellert, pp. 417-421.

product is in conformity with the contract.⁵¹ The subjective approach takes into account the considerations of both parties, it promotes autonomy and responsibility and it incentivises innovation.⁵²

Remedies

According to both directives, the trader's or seller's contractual liability is strict.⁵³ Therefore, the consumer does not need to establish that the vendor was aware or should have been aware that the AI system would act in a way leading to a breach of contract.⁵⁴

If a good with digital elements or digital content/service is not in conformity with the contract, the consumer has the right to have it brought into conformity or to receive a proportionate reduction in the price, or to terminate the contract.⁵⁵ On the first level of remedies, the consumer may only require that the product be brought into conformity and it is up to the consumer to decide whether he requires repair or replacement.⁵⁶ The directives provide for second level remedies in the form of the right to a proportionate reduction of the price or the right to termination of the contract.⁵⁷

If the trader or seller is liable for the lack of conformity for the AI product, they need to provide a remedy. With respect to bringing the product into conformity, the question arises whether sufficient knowledge exists to design adequate AI software and even if such requirements exist, it might be the case that the lack of conformity stems not from the design but rather from the data it has been fed with during its operation.⁵⁸ Turning back to Gellert's analysis of Waze, navigation software has a number of features that can be said to be at fault for bad routing advice.⁵⁹ So, does sufficient knowledge exist to change the algorithm in a way that will produce better traffic results? Gellert concludes that it is most likely still a work in progress.

Given the described complexity of consumer AI products and the lack of clear standards for what conformity actually entails, it is questionable if conformity of a consumer AI product with the contract can actually be achieved. Repair is often severely limited or even impossible because of the nature of AI software. Replacement appears equally unconvincing if the underlying software remains the

⁵¹ See: Pazos, pp. 340-350, Ebers (2020), p. 218.

⁵² Pazos, pp. 346-347.

⁵³ Ebers (2022), p. 37.

⁵⁴ Ebers (2020), p. 212.

⁵⁵ Article 14(1) DCD, Article 13(1) SGD.

⁵⁶ Gsell, p. 246; Looschelders, p. 485.

⁵⁷ Looschelders, pp. 494, 495.

⁵⁸ Gellert, p. 421.

⁵⁹ *Ibidem*, p. 421.

same (uncorrected). In practice, the consumer is therefore left with the second-level remedies of proportionate price reduction or termination of the contract. This raises the question of the actual level of protection afforded, since the primary remedies envisaged by the directives will in many AI-related cases prove ineffective when the consumer AI product is not in conformity with the contract.

Conclusion

The analysis shows that there are still uncertainties regarding both the conformity requirements and the effectiveness of remedies in cases of non-conformity of consumer AI products. The DCD and SGD provide an important framework, however, they were drafted in a technologically neutral manner and therefore do not explicitly address AI. For now, much will depend on how national courts apply the provisions of the directives in practice, while the guidance of the Court of Justice of the EU through preliminary rulings will also be important. The interpretation process might gradually address the unresolved questions, though it could also highlight the need for legislative adaptation of the directives in the longer run. In the meantime, consumers may rely on secondary remedies, including proportionate price reduction or termination of the contract.

Bibliography

1. CLAES, Hannes – HERBOSCH, Maarten: Artificial Intelligence and Contractual Liability Limitations: A Natural Combination?. In: *European Review of Private Law*, Volume 31, no. 2/3 (2023), pp. 469-496.
2. DUROVIC, Mateja: AI and Existing EU Consumer Law. In: *The Cambridge Handbook of AI and Consumer Law: Comparative Perspectives*, DiMatteo, Poncibó, Howells (eds.). Cambridge: Cambridge University Press, 2024. 306, pp. 49-61. ISBN 9781009483599.
3. EBERS, Martin: Chapter 2: Artificial Intelligence, Contracting and Contract Law: An Introduction. In: *Contracting and Contract Law in the Age of Artificial Intelligence*, Ebers, Poncibó, Zou (eds.). Oxford: Bloomsbury Publishing, 2022. 328, pp. 19-40. ISBN 9781509950683.
4. EBERS, Martin: EU Consumer Law and the Artificial Intelligence Act. In: *The Cambridge Handbook of AI and Consumer Law: Comparative Perspectives*, DiMatteo, Poncibó, Howells (eds.). Cambridge: Cambridge University Press, 2024. 306, pp. 215-235. ISBN 9781009483599.
5. EBERS, Martin: Liability For Artificial Intelligence And EU Consumer Law. In: *JIPITEC*, Volume 12, no. 2 (2021), pp. 204-221.

6. GELLERT, Raphaël: The EU's New Directives on Digital Contracts, and Artificial Intelligence: Really Future Proof?. In: *European Review of Private Law*, Volume 29, no. 3 (2021), pp. 403-424.
7. GSELL, Beate: Art. 14 DCD: Remedies for lack of conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 239-269. ISBN 978384878911-5.
8. LOOSCHELDERS, Dirk: Art. 13 SGD: Remedies for lack of conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 476-509. ISBN 978384878911-5.
9. PAZOS, Ricardo: Rethinking Conformity for an Artificial Intelligence World. In: *European Sales Law: Challenges in the 21st Century*, Grundmann and Atamer (eds.). Antwerp: Intersentia, 2023. 372, pp. 321-351. ISBN 9781839703775.
10. PATERSON, Jeannie Marie – MAKER, Yvette: Chapter 5: Consumer Protection Law and AI. In: *The Cambridge Handbook of Private Law and Artificial Intelligence*, Lim, Morgan (eds.). Cambridge: Cambridge University Press, 2024. 672, pp. 113-134.
11. SEIN, Karin: The Applicability of the Digital Content Directive and Sales of Goods Directive to Goods with Digital Elements. In: *Juridica International*, Volume 30 (2021), pp. 23–31.
12. STAUDENMAYER, Dirk: Art. 7 DCD: Subjective requirements for conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 111-125. ISBN 978384878911-5.
13. STAUDENMAYER, Dirk: Art. 8 DCD: Objective requirements for conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 125-164. ISBN 978384878911-5.
14. STAUDENMAYER, Dirk – BERTELMANN, Bernd: Art. 6 SGD: Subjective requirements for conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 371-386. ISBN 9783848789115.
15. STAUDENMAYER, Dirk – BERTELMANN, Bernd: Art. 7 SGD: Objective requirements for conformity. In: *EU Digital Law*, Staudenmayer, Schulze (eds.). Baden-Baden: Nomos, 2025. 1155, pp. 387-427. ISBN 978-3-8487-8911-5.

Contact details

Tjaša Kalin, Junior Researcher

tjasa.kalin@pf.uni-lj.si

Institute for Comparative Law at the Faculty of Law in Ljubljana

LOGICKÉ USUDZOVANIE A UMELÁ INTELIGENCIA V PRÁVE

LOGICAL REASONING AND ARTIFICIAL INTELLIGENCE IN LAW

Marek Čiernik¹

Abstrakt: Rozvoj umelej inteligencie a najmä veľkých jazykových modelov (LLM) prináša nové otázky pre právnu teóriu aj prax. Nie len v oblasti civilného práva sa objavujú očakávania, že tieto technológie môžu prispieť k rýchlejšiemu spracovaniu právnych textov či efektívnejšej orientácii v judikatúre. Súčasne sa však ukazuje, že ich možnosti majú výrazné limity, predovšetkým tam, kde je potrebné logické usudzovanie, subsumpcia skutkových okolností pod právne normy alebo hodnotový vklad pri posudzovaní káuz. Príspevok analyzuje vybrané situácie zo slovenského civilného práva, v ktorých sa tieto limity prejavujú. Poukazuje na rozdiel medzi štatistickým generovaním textu a právnym myslením, ktoré je založené na logike a logickej dedukcii. Cieľom príspevku je priblížiť aktuálne výzvy, ktoré prináša nástup umelej inteligencie a naznačiť smerovanie diskusie o jej využiteľnosti v civilnom práve.

Kľúčové slová: civilné právo, umelá inteligencia, logika, usudzovanie

Abstract: The development of artificial intelligence, and large language models (LLMs) in particular, raises new questions for legal theory and practice. Not only in the field of civil law are there expectations that these technologies can contribute to faster processing of legal texts or more effective orientation in case law. At the same time, however, it is becoming apparent that their capabilities have significant limitations, especially where logical reasoning, the subsumption of factual circumstances under legal norms, or value judgments in the assessment of cases are required. This article analyzes selected situations from Slovak civil law in which these limitations become apparent. It points out the difference between statistical text generation and legal thinking, which is based on logic and logical deduction. The aim of the article is to highlight the current challenges posed by the advent of artificial intelligence and to indicate the direction of the discussion on its usefulness in civil law.

Key words: civil law, artificial intelligence, logic, reasoning

¹ Katedra občianskeho práva, Právnická fakulta, Univerzita Komenského v Bratislave

Úvod

Bolo by náročné nájsť vo svojom okolí človeka, ktorý aspoň nepočul o umelej inteligencii (AI). Téma, ktorá je pertraktovaná nie len na úrovni priateľských rozhovorov, ale sa stáva hlavnou témou mnohých vedeckých konferencií. Názory na využívanie AI sa líšia ako v spoločnosti, tak aj vo vedných disciplínach. Jedno je však isté. Nikto pred pokrokom neunikne, pretože systémy umelej inteligencie sa integrovali do tých najpoužívanejších aplikácií. Hoci si to bežný používateľ smartfónu nemusí uvedomovať, do kontaktu s AI zaručene prišiel.

Hlavu do piesku zrejme nestrká ani právo resp. právna veda. Vynárajú sa viaceré otázky či už ide o autorské právo, dodržiavanie etických noriem pri trénovaní AI², právnej subjektivity, no a v neposlednom rade či umelá inteligencia časom nahradí sudcov, úradníkov a nakoniec aj advokátov. Sú ale právnické povolania skutočne ohrozené? V našom príspevku sa zaoberáme hľadaním limitov veľkých jazykových modelov (LLMs), ktoré sú v súčasnosti najpoužívanejšími modelmi.³ Upozorníme na niekoľko úskalí, do ktorých môže používateľ ľahko spadnúť. Vysvetlíme niektoré nedokonalosti, ktoré si umelá inteligencia v procese vlastného vývinu osvojila. A hlavne sledujeme, či AI dokáže logicky usudzovať, alebo len tento proces veľmi verne napodobňuje.

Umelá inteligencia (AI) alebo veľké jazykové modely (LLM)

Pred tým, ako pristúpime k analýze schopností umelej inteligencie premýšľať, musíme pojmovo vymedziť, čo máme na mysli, keď hovoríme o umelej inteligencii. Umelá inteligencia je pojem najširší. Šírku pojmu potvrdzuje aj jeho slovníková definícia, ktorá hovorí, že umelá inteligencia je „využívanie alebo štúdium počítačových systémov alebo strojov, ktoré majú niektoré vlastnosti ľudského mozgu, ako napríklad schopnosť interpretovať a vytvárať jazyk spôsobom, ktorý sa javí ako ľudský, rozpoznávať alebo vytvárať obrazy, riešiť problémy a učiť sa z údajov, ktoré im sú poskytované“.⁴ Keď sa posunieme o úroveň nižšie – zo všeobecného na konkrétnejšie, tak môžeme hovoriť o generatívnej umelej inteligencii. Generatívnej preto, pretože niečo generuje – vytvára. V článkoch, ktoré sa zaoberajú týmto typom umelej inteligencie, nachádzame pomerne zhodne definíciu: „Generatívna umelá inteligencia je umelá inteligencia, ktorá dokáže vytvárať originálny obsah, ako sú

² Pasetti, M., Santos, J.W., Corrêa, N.K. et al. Technical, legal, and ethical challenges of generative artificial intelligence: an analysis of the governance of training data and copyrights. In: *Discover Artificial Intelligence*, roč. 5, č. 1, 2025, s. 7

³ OpenAI podľa zdrojov až 700M používateľov týždenne. Online. Dostupné z: <https://backlinko.com/chatgpt-stats#key-chat-gpt-open-ai-stats>. [cit. 2025-09-09].

⁴ Definícia slovníka CAMBRIDGE DICTIONARY. Online. Dostupné z: <https://dictionary.cambridge.org/dictionary/english/artificial-intelligence>. [cit. 2025-09-09].

texty, obrázky, videá, zvukové záznamy alebo softvérový kód, v reakcii na podnet alebo požiadavku používateľa.”⁵ Opäť posunom o úroveň nižšie hovoríme o veľkých jazykových modeloch – „large language models”. Keďže už vieme, že ide o typ generatívnej umelej inteligencie a rozumieme, že má ísť o jazykový model, tak môžeme usúdiť, že veľké jazykové modely sú trénované na veľkom množstve textov s cieľom vytvárať nové texty.

V príspevku budeme pracovať s modelom ChatGPT-5, ktorý možno v súčasnosti považovať za najúspešnejší model z hľadiska počtu používateľov a počtu mesačných návštev.⁶ Samozrejme aj tento model má isté problémy, ku ktorým sa neskôr vyjadríme. Pre jednoduchšie a plynulejšie čítanie príspevku budeme pojmy umelá inteligencia (AI) a veľký jazykový model (LLM) spolu s ich skratkami používať ako synonymá.

Kedy AI premýšľa?

Otázka, či môže umelá inteligencia premýšľať, je jednou z najdiskutovanejších tém súčasnej informatiky aj filozofie práva. V právnickom diskurze sa pod „premýšľaním” rozumie najmä schopnosť logicky usudzovať, vyvodzovať závery z východiskových premís a aplikovať normu na konkrétny skutkový stav. V terminológii umelej inteligencie sa používa pojem „reasoning”, ktorým sa označuje schopnosť systému spájať informácie a dospieť k riešeniu.

Je však dôležité odlíšiť LLMs od novšieho konceptu tzv. large reasoning models (LRMs). Kým LLMs sú trénované na masívnych množstvách textu s cieľom predpovedať pravdepodobne nasledujúce slovo, LRMs sa snažia ísť ďalej: majú byť schopné explicitného uvažovania, napríklad prostredníctvom krokov pripomínajúcich matematický dôkaz alebo logickú úvahu. V právnom kontexte by práve takýto „reasoning” bol kľúčový, pretože aplikácia práva si vyžaduje nie len znalosť jazykových vzorcov, ale aj schopnosť správne subsumovať a udržať vnútornú logickú konzistenciu.

O LLMs sa tradične tvrdí, že fungujú iba na základe štatistiky, a preto očakávame, že ich schopnosť uvažovať je obmedzená.⁷ Model dostane vstupný „prompt” a na základe pravdepodobnostných distribúcií odhaduje, aké slovo alebo fráza má nasledovať. Tento proces pripomína sofistikované dokončovanie textu – nie však usudzovanie v logickom zmysle. Niektorí autori, napríklad Marcus, preto upozorňujú,

⁵ Jednotlivé definície. Online. Dostupné z: <https://www.ibm.com/think/topics/generative-ai> <https://www.oecd.org/en/topics/sub-issues/generative-ai.html> <https://news.mit.edu/2023/explained-generative-ai-1109>. [cit. 2025-09-09].

⁶ Dáta spoločnosti Similarweb. Online. Dostupné z: <https://www.axios.com/2025/09/06/ai-chatbot-popularity>, <https://backlinko.com/chatgpt-stats#key-chat-gpt-open-ai-stats>. [cit. 2025-09-09].

⁷ NAVEED, Humza; ULLAH KHAN, Assad a QIU, Shi. A Comprehensive Overview of Large Language Models. *ACM Trans. Intell. Syst. Technol.* 2025, vol. 16, no. 5, s. 34. ISSN 2157-6904.

že LLM „nechápu“ význam slov, iba manipulatívne operujú s pravdepodobnosťou.⁸ Rovnako tak v súčasnosti nemôžeme tvrdiť, že „reasoning“ LLMs je dostatočne konzistentný na to, aby sme ho mohli považovať za spoľahlivý.⁹ Na druhej strane možno namietat, že takto vznikajúca schopnosť môže byť funkčne ekvivalentná porozumeniu – model „nepremýšľa“ ako človek, no môže dosiahnuť podobné výsledky.

Ďalším problémom, ktorý komplikuje právne využitie AI, je tzv. „black box efekt“. Neurónové siete, na ktorých sú LLMs postavené, majú milióny až miliardy parametrov a vzájomných prepojení. Aj keď poznáme ich štruktúru, nedokážeme vysvetliť, prečo konkrétny vstup vygeneroval konkrétny výstup. Z pohľadu práva to môže predstavovať vážny problém, pretože ak má byť rozhodnutie spravodlivé, musí byť odôvodniteľné a spätne kontrolovateľné. Pri AI však často nevieme odhaliť reťazec, na základe ktorého systém dospel k záveru.¹⁰

Zjednodušene možno povedať, že neurónové siete fungujú podobne ako biologický mozog, no iba na úrovni štruktúry. Umelé „neuróny“ sú matematické funkcie, ktoré spracúvajú vstupy a posielajú ich ďalej. Vďaka obrovskému množstvu dát sa model naučí vzory a vzťahy, ale tieto vzťahy nie sú transparentné a ľudsky čitateľné. Aj preto sa často zdôrazňuje, že AI „napodobňuje“ myslenie, ale skutočné premýšľanie zatiaľ absentuje.¹¹

Opis metód

Spomedzi tradičných logických metód získavania nového poznania – abdukcia, dedukcia a indukcia – budeme my skúmať logickú dedukciu. Tvrdíme, že právo využíva najmä dedukciu na získanie nových informácií v snahe tvoriť správne závery. Čo sa týka zvyšných dvoch metód, tak v oblasti vyšetrovania priestupkov, prečinov či zločinov sa stretávame s abdukciou, pri ktorej vyšetrovateľ zo skutkových okolností abdukuje možné príčiny ich vzniku. S abdukciou tradične pracuje medicína pri diagnostike ochorení. Schopnosťou LLMs abduktívne usudzovať môže byť zaujímavá

⁸ MARCUS, G. *The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence*. Online. In: . 2020. s. 6

⁹ JUNNAN Liu, HONGWEI Liu, LINCHEN Xiao et al. *Are Your LLMs Capable of Stable Reasoning?*. In: Findings of the Association for Computational Linguistics: ACL 2025, Vienna, Austria, s. 17602.

¹⁰ BATHAEE, Yavar. *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. *Harvard Journal of Law & Technology*. 2018. s. 901

¹¹ SHOJAEE, Parshin; MIRAZDEH, Iman; ALIZADEH, Keivan et. al. *The Illusion of Thinking: Understanding the Strengths and Limitations of Reasoning Models via the Lens of Problem Complexity*. In: NeurIPS, 2025. s. 11

práve pre túto oblasť¹², nie však pre nás, pretože abdukciou získame len možné príčiny a postupnou elimináciou sa snažíme určiť tú najpravdepodobnejšiu. V našom experimente teda nie je možné skúmať pravdivosť týchto „výšetrovacích“ verzií. Taktiež tvrdíme, že pre využitie indukčnej metódy nemáme v práve dostatočné množstvo zopakovaní rovnakej situácie, aby sme dokázali odvodiť dostatočne prijateľný záver.

Pri skúmaní schopností veľkých jazykových modelov pracovať s právnym textom je nevyhnutné vytvoriť rámec, ktorý nám umožní porovnávať ich výstupy v rôznych situáciách. V našom príspevku sme preto zvolili dve základné metodologické línie, ktoré odrážajú rozdielne spôsoby, akými môže používateľ komunikovať s umelou inteligenciou.

V prvom prípade sme k modelu pristúpili s jasne deklarovanou požiadavkou na logickú analýzu konkrétnych ustanovení právnych predpisov. V prompte sme otvorene uviedli, že nás nezaujímajú iba voľný opis, ale chceme, aby model vykonal systematické právne usudzovanie. Takýto postup možno označiť za „odbornícky prístup“, pretože simuluje situáciu, keď AI využíva právnik, ktorý presne vie, čo od nej očakáva.

Druhý postup sa naopak snažil simulovať komunikáciu bežného používateľa, ktorý nemá právnické vzdelanie a modelu neformuluje požiadavky v kategóriách právnej logiky. Vytvorili sme dočasnú konverzáciu bez využitia pamäte, teda v prostredí, kde model nereflektoval predchádzajúce interakcie. Používateľ sa v tomto prípade pýtal na analýzu rovnakých právnych ustanovení, no otázku formuloval inak – skôr opisne alebo nepriamo, bez explicitného zdôraznenia požiadavky logickej štruktúry. Takýto prístup možno označiť za „laický prístup“.

Odbornícky prístup obsahoval úvodný prompt, v ktorom bol LLM upozornený na to, že ideme testovať jeho schopnosť logicky usudzovať. Ďalšie prompty obsahovali normu a následne žiadosť o logickú analýzu tejto normy s prepisom do symbolickej podoby.

Laický prístup využíval skôr hovorový štýl – rozpovedanie krátkeho príbehu ako poslanec mestského zastupiteľstva narazil na normu a pýta si radu od LLM, či je možné vyhlásiť rokovanie obecného zastupiteľstva za verejné (viď časť nižšie).

Využili sme 3 typy chýb, ktorých sa môže právnik alebo zákonodarcu dopustiť a konfrontovali sme s nimi LLM:

1. Chyba nesprávneho použitia pravidla *modus tollens* pri nutnej podmienke
2. Nesprávne použitie spojky „alebo“ pri negácii disjunkcie
3. Chyba v negovaní v právnej norme

¹² PIETARINEN, Ahti-Veikko a STANLEY, Donald E. The logic of medical reasoning: toward an integrated inductive, deductive, and abductive approach to clinical practices. *Philosophy, Ethics, and Humanities in Medicine*. 2025, vol. 20, no. 1, ISSN 17475341. s. 1

Kľúčom metodológie bolo, že sme v oboch prípadoch pracovali s identickými právnymi normami, čím sme zabezpečili porovnateľnosť výsledkov. Vždy išlo o tie isté tri ustanovenia práva, ktoré majú jasnú logickú štruktúru a v právnej praxi predstavujú časté problémové body. Pri každom ustanovení sme teda získali dve odpovede: jednu vyprodukovanú na základe odbornického promptu a druhú na základe laického promptu. Spolu sme tak získali šesť výstupov, ktoré boli následne predmetom našej vlastnej logickej analýzy.

Zvolený postup nám umožňuje sledovať dva dôležité aspekty. Po prvé, ako sa líši schopnosť modelu produkovať logicky konzistentné závery, keď je k tomu priamo vedený oproti situácii, keď je otázka formulovaná bežným používateľom. Po druhé, či sú rozdiely medzi odpoveďami natoľko výrazné, že môžu viesť k odlišným právnym záverom, čo má zásadný význam pre otázku právnej istoty.

Takto nastavená metodológia nám umožní nielen poukázať na limity modelu, ale aj na riziká spojené s jeho využívaním v praxi – od odbornej právnickej po bežnú laickú komunikáciu. V nasledujúcich častiach bližšie opíšeme jednotlivé typy chýb.

Chyba nesprávneho použitia pravidla *modus tollens* pri nutnej podmienke

Ako s prvou pracujeme s normou zo zákona č. 369/1990 Zb. o obecnom zriadení (vyhlásené znenie). Táto znie:

„Rokovania obecného zastupiteľstva sú zásadne verejné. (...) Vyhlásiť rokovanie obecného zastupiteľstva za neverejné možno iba vtedy, ak sa prerokúvajú veci, ktoré majú byť predmetom utajovania v štátnom záujme.“

Zaujímavá je pre nás druhá veta, ktorá obsahuje logickú spojku „...iba vtedy, ak...“, ktorá vyjadruje nutnú podmienku. Často krát, najmä v práve, dochádza k mylnému zamieňaniu tejto spojky s ekvivalentom.¹³ Samotný fakt, že „sa prerokúvajú veci, ktoré majú byť predmetom utajovania...“ ešte nespôsobuje, že rokovanie obecného zastupiteľstva môže byť vyhlásené za neverejné. Ak by sme chceli ustanovenie preformulovať a zaviesť dostatočnú podmienku, splnenie ktorej by už výsledok vyvolávalo, znela by nasledovne:

- **Ak** sa prerokúvajú veci, ktoré majú byť predmetom utajovania v štátnom záujme, **tak** možno vyhlásiť rokovanie obecného zastupiteľstva za neverejné.

Správny spôsob použitia pravidla *modus tollens* pre pôvodnú normu v tomto prípade vyzerá nasledovne:

$$\begin{array}{c} A \rightarrow B \\ \neg B \\ \hline \neg A \end{array}$$

¹³ GAHÉR, František. *Logika pre každého*. 4. dopl. vyd. Bratislava: Iris, 2013. s. 75

Pričom „A“ zastupuje časť „vyhlásiť rokovanie obecného zastupiteľstva za neverejné možno“

Implikátor vyjadruje spojku „...iba vtedy, ak...“

„B“ zastupuje časť „prerokujú sa veci, ktoré majú byť predmetom utajovania“.

Na druhom riadku vidíme negáciu časti „B“, ktorá teda znie „**ne**prerokujú sa veci, ktoré majú byť predmetom utajovania“.

Na treťom riadku vidíme negáciu časti „A“, ktorá znie takto: „...vyhlásiť rokovanie obecného zastupiteľstva za neverejné **nemožno**“

Teda slovné zjednodušenie môžeme toto pravidlo vyjadriť takto:

- 1) Vyhlásiť rokovanie obecného zastupiteľstva za neverejné možno iba vtedy, ak sa prerokujú veci, ktoré majú byť predmetom utajovania.
- 2) Neprerokujú sa veci, ktoré majú byť predmetom utajovania.
- 3) Nemožno vyhlásiť rokovanie obecného zastupiteľstva za neverejné.

Toto je správny spôsob usudzovania podľa pravidla modus tollens, pokiaľ norma obsahuje spojku, ktorá signalizuje nutnú podmienku. V prvom prípade teda budeme sledovať, či sa umelá inteligencia dopustí chyby a zmýli si implikátor s ekvivalentom.

Nesprávne použitie spojky „alebo“ pri negácii disjunkcie

Ďalšou chybou, s ktorou sa môžeme v písanom práve stretnúť je používanie spojky „alebo“ namiesto použitia spojky „ani“. Norma s ktorou pracujeme je ustanovená v § 137 ods. 2 zákona č. 40/1964 Zb. Občiansky zákonník a znie:

*„**Ak nie je** právnym predpisom ustanovené **alebo** účastníkmi (**nie je**) dohodnuté inak, (**tak**) sú podiely všetkých spoluvlastníkov rovnaké.“*

Právnu normu sme rekonštruovali doplnením slov v zátvorkách, pretože obsahuje výpustky. Na tomto mieste môže uvažovať, čo je cieľom tejto normy. Môžeme predpokladať, že cieľom je nastaviť základný režim pre určenie veľkosti podielov spoluvlastníkov, a to v prípade, keď **nie je** právnym predpisom ustanovené **a zároveň nie je** účastníkmi dohodnuté inak. V takom prípade, keď absentuje zákonné ustanovenie a absentuje aj dohoda, tak sú podiely všetkých rovnaké.

Naskytli sa nám teda dva možné zápisy vo formálnom logickom jazyku:

- 1) $\neg A \vee \neg B$
- 2) $\neg A \wedge \neg B$

Prvý zápis reflektuje na znenie uvedenej normy, pretože spojka „alebo“ vyjadruje disjunkt. Sledovaním cieľa predmetnej normy však tvrdíme, že zamýšľaný a správny by bol v tomto prípade záporný konjunkt, ktorý je v prirodzenom jazyku vyjadrený spojkou „ani“.

V druhom prípade teda sledujeme, či LLM porozumie cieľu normy, identifikuje túto chybu a bude pracovať so správnym logickým operátorom.

Chyba v negovaní v právnej norme

Niekedy dokážeme objaviť aj chybu, ktorej sa dopustil samotný zákonodarca. Napríklad v ustanovení § 39 ods. 6 zákona č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon), ktoré znie:

*„Zmluvou o vytvorení diela ani odovzdaním veci, ktorej prostredníctvom je dielo vyjadrené, **nenadobudne** objednávateľ právo použiť toto dielo, ak nie je uvedené inak, **len ak súčasne** so zmluvou o vytvorení diela alebo po tomto momente **uzatvorí** s autorom licenčnú zmluvu.“*

Cieľom tejto normy je zjavne to, aby objednávateľ **nenadobudol** právo použiť dielo v prípade, že **neuzavrie** s autorom licenčnú zmluvu. V uvedenom prípade sa však zrejme zákonodarca dopustil chyby. Spojka „..., len ak...“ opäť signalizuje nutnú podmienku. Podľa vyššie uvedeného pravidla modus tollens z chybnej normy vyplýva nasledovné:

- 1) Súčasne so zmluvou o vytvorení diela objednávateľ **neuzatvoril** s autorom licenčnú zmluvu.
- 2) Takže objednávateľ **nadobudne** právo použiť dielo.

Upravená norma, aby vyvolávala žiadaný výsledok by teda musela znieť:

*„Zmluvou o vytvorení diela ani odovzdaním veci, ktorej prostredníctvom je dielo vyjadrené, **nenadobudne** objednávateľ právo použiť toto dielo, ak nie je uvedené inak, **pokiaľ** súčasne so zmluvou o vytvorení diela alebo po tomto momente **neuzatvorí** s autorom licenčnú zmluvu.“*

V tomto príklade sledujeme, či LLM je schopný identifikovať túto chybu a reflektovať na ňu.

Diskusia k výsledkom

V prípade laických promptov sme doplnili ešte vždy ďalšiu otázku, aby sme potvrdili, či sa skutočne LLM mýli. Samozrejme berieme do úvahy problém, ktorý sa nazýva „sycophancy“ a vyjadríme sa k nemu v závere príspevku.

V prvom prípade sme testovali **nesprávne použitie pravidla modus tollens**.

Odbornícky prompt	Laický prompt
• LLM vykonal prepis do symbolickej podoby • Identifikoval, že sa v norme vyskytuje nutná podmienka • Správne použil pravidlo modus tollens	• Podal odpoveď ako učiteľ, nie ako právnik • Navrhoval skutočnosti, ktoré možno považovať za „utajené“ • Znovu zopakoval normu, bez určenia, čo z nej vyplýva

• Navyše uviedol, že tu dochádza k mylnému zavedeniu ekvivalencie	• Dopĺňujúcou otázkou potvrdil chybu v nesprávnom usudzovaní

Tabuľka č. 1
Zhrnutie č. 1

V druhom prípade sme sledovali **nesprávne použitie spojky „alebo“ pri negácii disjunkcie**.

Odbornícky prompt	Laický prompt
• LLM vykonal prepis do symbolickej podoby • Identifikoval, že musí ísť o negáciu celej disjunkcie • Neidentifikoval však chybu v zámene „ani“ za „alebo“ • Usúdil správny záver aj s vysvetlením	• Podal odpoveď ako učiteľ, nie ako právnik • Len z absentujúcej dohody medzi spoluvlastníkmi vyvodil, že podiely sú rovnaké • Normu opätovne nesprávne prepísal s chybou, ale nevysvetlil, čo z nej vyplýva • Dopĺňujúcou otázkou potvrdil chybu v nesprávnom usudzovaní

Tabuľka č. 2
Zhrnutie č. 2

V poslednom prípade sme pozorovali, či zvládne LLM identifikovať diskrepanciu v znení právnej normy a sledovaným cieľom. **Chyba v negovaní v právnej norme**.

Odbornícky prompt	Laický prompt
• LLM začal premýšľať pred generovaním odpovede (2m a 43s) • Normu prepísal do symbolickej podoby • Správne identifikoval chybu v právnej norme • Navrhol 2 úpravy právnej normy, ktoré sa však nezhodujú s tou našou	• Podal odpoveď ako učiteľ, nie ako právnik • Absolútne odignoroval chybu v právnej norme • Vysvetlil, čo je licenčná zmluva a na čo sa používa • Na dopĺňujúcu otázku, či sa mu zdá norma správna odpovedal kladne

Tabuľka č. 3
Zhrnutie č. 3

Záver

Prezentovanou analýzou šiestich konverzácií s umelou inteligenciou sme identifikovali jej nedostatky v prípade, že prompt nie je dostatočne konkrétny. Je potrebné však povedať, že výsledky získané použitím „odbornického“ promptu možno považovať za prekvapivé. LLM veľmi dôveryhodne napodobnil správnu logickú analýzu, hoci zrejme použitým slovám nerozumie.

Rozdiely vo výsledkoch medzi odpoveďou na odbornícky a laický prompt možno považovať za nekonzistentnosť v generovaní odpovedí. Zatiaľ čo norma bola v oboch prípadoch rovnaká, LLM generoval dve rôzne riešenia. Je dôležité teda upozorniť na dôležitosť dôkladného postupu pri vytváraní promptov, aby zadávateľ dostal čo najsprávnejší výsledok.

Vo svetle výsledkov by bolo ešte predčasné tvrdiť, že umelá inteligencia môže nahradiť napríklad osobu sudcu. Veľkými problémami sa javia byť „black box efekt“, medzi právnikmi diskutovaná zodpovednosť AI, ale aj nami prezentovaná logická nekonzistentnosť. Rápidny vývoj modelov umelej inteligencie však možno toto tvrdenie v dohľadnej dobe falzifikuje.

Limity zvoleného postupu

Prvým limitom, ktorý mohol ovplyvniť výsledky je tzv. „routing“¹⁴, ktorý ChatGPT 5 využíva. V snahe odľahčiť nápor na servery spoločnosti OpenAI sa LLM správa tak, že jednoduchšie typy otázok presúva na modely, ktoré generujú rýchlejšie a menej náročné odpovede. Počas nášho skúmania sme sa stretli s prípadom, kedy LLM deklaroval, že premýšľa. Pravdepodobne v tomto momente sme komunikovali s výkonnejším modelom, ktorý lepšie napodobňuje logické uvažovanie.

Ďalším limitom je „sycophancy“, ktorá sa mala možnosť prejavíť pri dodatočných otázkach v laickom promptovaní. Tento fenomén znamená, že modely AI sa snažia utvrdzovať používateľa v jeho názoroch, aby bol s výsledkami LLM spokojný. Tým môže dochádzať ku klamlivému potvrdzovaniu nepravdivých informácií. Napríklad pri položení sugestívnej otázky sa LLM bude snažiť kladne odpovedať.¹⁵

Poslednou zrejmovou limitáciou výskumu je fakt, že sme pracovali len s jedným modelom umelej inteligencie. Tento model, hoci najpoužívanejší, nám mohol priniesť iné výsledky ako ostatné modely (Gemini, Grok, DeepSeek, Llama). Argumentom však ostáva, že sme sa snažili simulovať čo najvernejšie komunikáciu bežného používateľa.

¹⁴ Deklarované samotnými vývojarmi. Online. Dostupné na: <https://openai.com/index/introducing-gpt-5/>. [cit. 2025-09-09].

¹⁵ SHARMA, Mrinank; TONG, Meg; KORBAK, Tomasz et. al. Towards Understanding Sycophancy in Language Models. In: *12th International Conference on Learning Representations, ICLR 2024*. Vienna, 2024, s. 1.

Zoznam použitej literatúry

1. GAHÉR, František. *Logika pre každého*. 4. dopl. vyd. Bratislava: Iris, 2013. 460 s., ISBN 978-80-89256-88-4.
2. ŠTĚPÁN, Jan. *Logika a právo*. 2., dopl. vyd., Praha: C.H. Beck, 2004. 128 s., ISBN 80-7179-872-X.
3. Pasetti, M., Santos, J.W., Corrêa, N.K. et al. Technical, legal, and ethical challenges of generative artificial intelligence: an analysis of the governance of training data and copyrights. In: *Discover Artificial Intelligence*, roč. 5, č. 1, 2025, 22 s. Dostupné z: <https://doi.org/10.1007/s44163-025-00379-6>. [cit. 2025-09-09].
4. BATHAEE, Yavar. The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*. 2018, roč. 31, č. 2, s. 890-938. ISSN 0897-3393. Dostupné z: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathae.pdf>. [cit. 2025-09-09].
5. MARCUS, Gary. *The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence*. Online. Eprint: arXiv:2002.06177. 2020, s. 59. Dostupné z: <https://doi.org/https://doi.org/10.48550/arXiv.2002.06177>. [cit. 2025-09-09].
6. SHARMA, Mrinank; TONG, Meg; KORBAK, Tomasz et al. Towards Understanding Sycophancy in Language Models. In: *12th International Conference on Learning Representations, ICLR 2024*. Vienna, 2024, 35 s. Dostupné z: <https://doi.org/10.48550/arXiv.2310.13548>. [cit. 2025-09-10].
7. PIETARINEN, Ahti-Veikko a STANLEY, Donald E. The logic of medical reasoning: toward an integrated inductive, deductive, and abductive approach to clinical practices. *Philosophy, Ethics, and Humanities in Medicine*. 2025, roč. 20, č. 1, 9 s. ISSN 17475341. Dostupné z: <https://doi.org/10.1186/s13010-025-00178-y>.
8. JUNNAN Liu, HONGWEI Liu, LINCHEN Xiao et al. *Are Your LLMs Capable of Stable Reasoning?*. In: *Findings of the Association for Computational Linguistics: ACL 2025*, Vienna, Austria, s. 17594–17632. Dostupné z: [10.18653/v1/2025.findings-acl.905](https://doi.org/10.18653/v1/2025.findings-acl.905). [cit. 2025-09-10].
9. NAVEED, Humza; ULLAH KHAN, Assad a QIU, Shi. A Comprehensive Overview of Large Language Models. *ACM Trans. Intell. Syst. Technol.* 2025, vol. 16, no. 5, 47 s. ISSN 2157-6904. Dostupné z: <https://doi.org/10.1145/3744746> [cit. 2025-09-10].
10. SHOJAEE, Parshin; MIRAZDEH, Iman; ALIZADEH, Keivan et al. *The Illusion of Thinking: Understanding the Strengths and Limitations of Reasoning Models via the Lens of Problem Complexity*. In: *NeurIPS*, 2025. 30 s. Dostupné z: <https://doi.org/10.48550/arXiv.2506.06941>. [cit. 2025-09-10].

Kontaktné údaje

Mgr. Marek Čiernik

marek.ciernik@flaw.uniba.sk

Univerzita Komenského v Bratislave

THE USE OF ARTIFICIAL INTELLIGENCE IN CONSUMER TRADE - AN OPTIMAL MODEL OF LEGAL REGULATIONS

Paweł Lewandowski¹

Abstract: The use of AI brings great benefits, and at the same time previously unknown threats. In response to these problems, appropriate regulations are being sought in the legal space. The research thesis of this study is that existing consumer law instruments do not fully address the challenges arising from the use of AI in economic transactions. The aim of the article is to search for the optimal legal framework in the field of consumer trade. In view of this a review of legal regulations regarding the use of AI in consumer trade was carried out. Above all, it was stated that the provisions are not transparent (they are extensive and general) and they impose obligations without providing clear sanctions for their violation. Attention is drawn to the need to establish precise legal rules for the use of AI by entrepreneurs. It is stated that only an appropriately regulated and sanctioned information obligation on the use of AI in any form and at any stage of contracting can prevent potential violations of consumer rights. Finally, *de lege ferenda* conclusions were formulated, indicating that AI requires quick and possibly comprehensive legal regulation.

Keywords: consumer, entrepreneur, consumer trade, AI

Introduction

It's clear that artificial intelligence (AI) has become a topic of interest in every field of science, including legal studies. This is no surprise, as AI is present at virtually every corner². Its presence raises numerous legal and ethical issues³.

¹University of Warmia and Mazury in Olsztyn, Faculty of Law And Administration, Department of Economic Public Law and Commercial Law

² See for example: REJMANIAK, Rafał: Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego, In: Roczniki Nauk Prawnych, Tom XXXI, nr 3, 2021, p. 95-113, DOI: <http://doi.org/10.18290/rnp21313.6>; JUŚCIŃSKI, Przemysław Piotr: Prawo autorskie w obliczu rozwoju sztucznej inteligencji, In: Zeszyty Naukowe Uniwersytetu Jagiellońskiego no. 1, 2019, p. 5-44.

³ It also brings benefits, e.g. see: GARG, Seema, MAHAJAN, Navita, GHOSH, Jayanta, Artificial Intelligence as an Emerging Technology in Global Trade: The Challenges and Possibilities, In: Vikas Garg, Richa Goel, Handbook of Research on Innovative Management Using AI in Industry 5.0, DOI: [10.4018/978-1-7998-8497-2.ch007](https://doi.org/10.4018/978-1-7998-8497-2.ch007), Publisher: IGI Global, 2022, p. 604 – 623, ISBN 978-166847461-7, 978-166847460-0.

Initially, from the legal point of view, the legal definition of AI posed a problem⁴. Although the term "artificial intelligence" for scientific discussion is attributed to John McCarthy as early as 1955⁵, its official meaning was first introduced by Article 3, Section 1, of the AI Act⁶. However, a common interpretation of this concept remains necessary. The legal subjectivity of AI is of equal interest in the legal literature⁷. Generally, there is no doubt that we are dealing with a systemic problem. Namely, AI is developing faster than the law; and legal systems, despite strenuous efforts, lack a uniform and clear regulatory regime.

Among the many issues encompassing AI, consumer law deserves special attention. The consumer became a special subject of civil law at the turn of the 21st century, when systemic inequality in consumer-business relations began to be recognized. Their separate treatment (as a special subject of civil law) is justified by the need to protect the weaker party in the legal relationship, prevent abuse, and ensure balance in economic transactions. The consumer, faced with AI – a tool that is fast, convincing, attractive to the user, and at the same time prone to errors – requires special protection.

⁴ Wider: RZYMOWSKI, Jakub: Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji, In: Przegląd Prawa Publicznego, no 11, 2024, p. 56-63, CHIAPPINI, Daniele: The Legal Definition of Artificial Intelligence: A Comparative Perspective, In: European Journal of Comparative Law and Governance, no. 11(3), 2024, p. 360-387, <https://doi.org/10.1163/22134514-bja10071>; MARTSENKO, Natalia: Influence of artificial intelligence on the legal system, In: Studia Prawnoustrojowe no. 54, 2021, p. 388- 395; see also NESSLER, Bernhard, WENDERHORS, Christiane: Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act, European Law Institute, Vienna, Austria 2024, ISBN: 978-3-9505495-3-9, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf; available on 14.09.2025.

⁵ McCARTHY, John, MINSKY, Marvin L., ROCHESTER, Nathaniel, SHANNON Claude E.: A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, <http://www-formal.stanford.edu/jmc/history/dartmouth.pdf> [data access: 6.02.2021].

⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) OJ L, 2024/1689, 12.7.2024, furthers as AI Act; The definition of an AI system in Article 3(1) of the AI Act is broad and reads as follows: 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

⁷ KOCOT, Wojciech Jerzy: Podmiotowość sztucznej inteligencji w nowym kodeksie cywilnym, In: Państwo i Prawo no 5, 2024, p. 108-134, NAGESH, Pal Singh; NIDHISH, Dev Lomash: Future of AI as Legal Personality, In: International Journal of Law Management & Humanities 4 (2021): 1116-[cvii].

This study is based on the assumptions of the dogmatic legal method, supplemented by references to EU law. The research thesis of this study is that existing consumer law instruments do not fully address the challenges arising from the use of AI in economic transactions, and therefore, it is necessary to adapt them to new technological realities. The aim of the study is to search for an optimal model of legal regulation in the field of consumer trade. The article contributes to the debate on whether and how civil law systems should adapt their legal frameworks regarding the relationships between consumers and professional entities using artificial intelligence systems.

Consumer trade

Established in national and EU legislation, as well as developed by legal doctrine, is the division of civil law trade into business trade (bilateral professional transactions), consumer trade, and general trade. The parties to bilateral professional transactions are exclusively entrepreneurs, which is why it is called business trade in the *strict sense*. Legal transactions between professional participants constitute commercial legal transactions, characterized by qualified action, repeatability, and a purpose. Within consumer trade (B2C, i.e., business-to-consumer), transactions are concluded between entrepreneurs and consumers. This category of trade is characterized by the subject structure of the legal relationship, where the recipient of the service is a non-professional entity (non-professional), while the provider conducts professional activities within the enterprise (which is characterized by the inequality of entities)⁸. For legal transactions to be considered as general trade, the qualification of the entities is irrelevant; it is sufficient that they can be subjects of a civil law relationship⁹. Therefore, the formal equality of the parties and the lack of a direct connection to the business activity being conducted are decisive¹⁰. Unlike to bilateral professional and consumer trade, in general trade none of its participants performs

⁸ For this reason, in the earlier literature on the subject, consumer trade was referred to as unilaterally commercial trade, currently there is no regulation similar to Article 498 § 1 of the Commercial Code (Journal of Laws 1934, 57, 502), which Act at one time defined commercial activities as legal acts of the merchant related to running his business, compare: ŁĘTOWSKA, Ewa: Kształtowanie się odrębności obrotu mieszanego, In: E. Łętowska (ed.), *Tendencje rozwoju prawa cywilnego*, Wrocław, Warszawa, Kraków, Gdańsk, Łódź, 1983, p. 372.

⁹ KATNER, Wojciech Jan, In: W.J. Katner (ed.), *Prawo cywilne i handlowe w zarysie*, Warsaw 2014, p. 31.

¹⁰ PECYNA, Marlena: *Kontrola wzorców umownych poza obrotem konsumenckim*, Kraków 2003, p. 26.

professionally any economic activity that would result in the provision of services or the offering of goods¹¹, and none of them has the status of a consumer.

Therefore, consumer trade is distinguished based on the subjective criterion¹². In the Polish legal system, a consumer is considered to be an individual who enters into a legal transaction with an entrepreneur that is not directly related to their business or professional activity (Article 22¹ of the Civil Code¹³). Polish jurisprudence and legal doctrine have emerged with both broad and narrow interpretations of the concept of consumer¹⁴. Using linguistic, systemic, and teleological interpretations, the concept of consumer is limited to the legal relationship between an individual and an entrepreneur. A pro-European legal interpretation considers the scope of the concept of consumer more broadly, recognizing as a consumer also a person who does not enter into a legal transaction with an entrepreneur¹⁵.

Using AI for the consumer

As noted, the consumer is a special subject in civil law trade. Primarily because he/she act in a relationship with an entrepreneur, which makes him the weaker party to the contract. Importantly, legal systems define the so-called average consumer model. This is considered to be a consumer who is reasonably well-informed and reasonably observant and circumspect, but whose characteristics make them particularly vulnerable to unfair commercial practices¹⁶. Both EU and Polish courts are obliged to make an objective assessment of the consumer model, taking into account that the consumer model is influenced by various factors, such as social, cultural and linguistic factors (such as age, physical or mental infirmity or credulity)¹⁷.

¹¹ Compare: KRUCZALAK, Kazimierz: Prawo obrotu gospodarczego. Część I. Zagadnienia ogólne. Prawo handlowe, Gdańsk 1990, p. 5.

¹² RUTKOWSKA-TOMASZEWSKA, Edyta: Wzorce umowne w obrocie konsumenckim, In: Zobowiązania w obrocie gospodarczym, A. Malarewicz-Jakubów (ed.), Warsaw 2025, p. 509.

¹³ Act of April 23, 1964, The Civil Code (consolidated text, Journal of Law of 2025, item 1071, as amended), hereinafter: Civil Code.

¹⁴ Wider: OSAJDA, Konrad: Granice statusu konsumenta w prawie cywilnym – perspektywa temporalna oraz kwestia niedokonania czynności prawnej, In: Przegląd Sądowy no 11-12, 2022, p. 41-53.

¹⁵ Ibidem p. 51.

¹⁶ See: assumptions (18) of the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ L, 149/23.

¹⁷ For example: judgment of the Administrative Court in Szczecin of May 18, 2022 r., I ACa 10/22, LEX nr 3433305; judgment of Administrative Court in Warsaw of February 10, 2022 r., I ACa 826/21, LEX nr

The consumer's position in trade is determined by many factors, not just their status and the resulting difficulties, for example, in assessing the validity of a contract or the risks associated with it. It should be noted that consumers are often provided with unclear information (underinformation), and standard contract forms are used (they are unable to individually negotiate contract terms). Importantly, it is also recognized that the use of AI technology can influence consumer trade, for example, by providing tools for manipulation, exploitation, and social control practices¹⁸. Currently, entrepreneurs massively using AI solutions in many ways. Chatbots¹⁹, recommendation systems, and marketing campaigns tailored to individual preferences are used in customer-consumer service²⁰. Client (consumer) service uses chatbots, recommendation systems, and marketing campaigns tailored to individual preferences²¹.

The use of AI in B2C relationships carries legal and ethical risks. Consumers are often unaware that they are speaking to a chatbot, not a human. Recommender systems can favor certain products/services over others, which can limit the consumer's right to make informed choices. Personalization of marketing content can be suggestive and violate the prohibition of unfair market practices. Above all, however, in the consumer-AI relationship, the first one stands "no chance". It's difficult to speak of a consumer's autonomy of will when they are negotiating with a system based on big data and advanced analytics, capable of predicting consumer behavior²².

Legal regulations regarding the use of AI in consumer trade

It can be stated at the beginning that the current legal system does not contain a single, comprehensive normative act that comprehensively addresses the use of AI

3324675, see also: PACHUCA-SMULSKA, Beata: The System of Consumer Protection in Poland, In: Consumer Protection Law in Poland from the Perspective of EU Law, B. Pachuca-Smulka (ed.), Warsaw 2017, p. 16-17.

¹⁸ JEDLIŃSKA-SABATOWSKA, Anna: Prawa konsumentów w erze AI: jak sztuczna inteligencja zmienia relacje w sferze B2C, In: Prawo Nowych Technologii no. 4, 2024, p. 53.

¹⁹ Comprehensive study focusing on protection of consumers against abuse of the scalper bots: SIWICKI, Maciej: Protection of consumers against abuse of artificial intelligence in electronic trade: the scalper bots case, In: Balcerzak Michał, Kapelańska-Pręgowska Julia (ed.), Artificial intelligence and international human rights law developing standards for a changing world, 2024, Cheltenham, UK | Northampton, MA, Edward Elgar Publishing, p. 231-249, ISBN 978-1-0353-3792-7.

²⁰ Ibidem, p. 52.

²¹ Ibidem.

²² More: VEALE, Michael, BORGESIU, Frederik z.,: Demystifying the Draft EU Artificial Intelligence Act. In: Computer Law Review International, no. 22(4), 2021, p. 97-112.

in consumer trade²³. However, individual acts (EU and national) contain regulations that provide legal solutions for certain situations involving the use of AI in consumer trade (they will be cited here). The analysis is of an outline nature, as it is objectively impossible to capture and discuss all the regulations relating to discussed matter.

First, it's worth noting the Artificial Intelligence Act²⁴. Besides providing a legal definition of an AI system (Article 3, Section 1), it prohibits certain AI practices (Article 5), such as the use of an AI system that deploys subliminal techniques beyond a person's consciousness or intentionally manipulative or deceptive techniques; and introduces transparency obligations (Article 50), such as informing a natural person that they are interacting with an AI system (like a chatbot, virtual assistant)²⁵. Next, it's worth noting the Unfair Commercial Practices Directive²⁶, which specifically regulates misleading commercial practices. All actions/omissions designated as misleading actions and aggressive commercial practices, although they don't explicitly indicate the use of AI, may also include situations involving the use of AI in consumer trade. For example, the use of dark patterns or the personalization of offers.

Another act of EU law that deserves attention is Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services²⁷. This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price (Article 3).

²³ More about: VUJICIC, Jelena: Analysis of Proposed Artificial Intelligence Regulations: Perspectives from the United States, China, and the European Union, In: In Nadia E. Nedzel, Samuel O. Idowu, Belén Díaz Díaz, Irene Guia Arraiano & René Schmidpeter (eds.), Global Corporate Governance: Proceedings of the 8th International Conference on CSR, Sustainability, Ethics and Governance, Baton Rouge, USA, June 2022. Cham: Springer Nature Switzerland, pp. 173-194, 2025, DOI: 10.1007/978-3-031-86330-1_10, ISSN 21967075.

²⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689, 12.7.2024

²⁵ See: NOWAK-BYRTEK, Dominika: Obowiązek zapewnienia transparentności przez dostawców i podmioty stosujące niektóre systemy AI, In: M. Gumularz, P. Kozik (ed.), *Ochrona danych osobowych w marketingu i sprzedaży*, Warsaw, 2025, p. 415 - 441.

²⁶ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), L 149/22.

²⁷ JO L 136 du 22.5.2019.

It seems that according to the use of AI in consumer trade also of some importance is Directive (EU) 2019/2161 the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules²⁸. The recitals of this document indicate that consumers should be clearly informed when the price presented to them is personalized on the basis of automated decision-making, so that they can take into account the potential risks in their purchasing decision (45).

Finally, the General Data Protection Regulation (GDPR)²⁹ states, among other things, that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22, point 1). The cited EU acts have had an impact on the Polish legal system. It can be noted, for example, that the Consumer Rights Act³⁰ regulates the obligation to inform consumers about the functionality of digital content (Article 12, Section 1, Item 19, where AI is considered a digital service). Subsequently, the Act of August 23, 2007, on Counteracting Unfair Market Practices³¹, prohibits misleading and aggressive practices that may involve the use of AI to manipulate consumer decisions (Articles 5 and 7). It is also worth noting the Act of May 10, 2018, on Personal Data Protection³², which implements the GDPR. Finally, it is worth adding traditional consumer protection instruments, namely abusive clauses contained in the Civil Code in consumer contracts (the possibility of examining, for example, provisions regarding the use of AI).

Without conducting a deeper analysis of the regulations mentioned (this requires a separate study), it can be stated that the provisions are not transparent (they are extensive and general), they impose obligations without providing clear sanctions for their violation, and finally, their verification may raise concerns (which entity is obliged to do so? What tools does it have? How effectively does it perform its obligations?).

²⁸ Official Journal of the European Union 18.12.2019 L 328/7.

²⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1.

³⁰ Act of May 30, 2014, Journal of Laws of 2024, item 1796 with amendments.

³¹ Journal of Laws of 2023, item 845, with amendments.

³² Journal of Laws of 2019, item 1781 with amendments.

Comprehensive legal regulation?

The fundamental question when analyzing the use of AI in consumer trade is whether comprehensive, detailed (case-by-case) legal regulation is possible and desirable. Such regulation could take the form of a separate legal act, such as an Act on the use of AI systems in consumer trade.

The law should undoubtedly include obligations for entrepreneurs and prohibited practices regarding the use of AI systems in consumer trade. These should be at least sufficiently specific, while remaining somewhat general. Next, the liability of entrepreneur for damage caused to consumers as a result of the operation of an AI system should be clearly regulated, which, as indicated at the beginning, is controversial. In an optimal regulatory model, it is desirable to grant consumers the right to request that actions be taken by a human, not solely by an AI system. Perhaps the consumer should not have a choice, but rather the option of having their matter resolved outside of AI.

It's worthwhile to work on drafting the proposed act on the use of AI systems in consumer trade. Its implementation and potential verification in practice could provide an opportunity to keep pace with technological progress and neutralize the resulting threats.

Conclusion

The analysis demonstrates that while AI has already become an inseparable element of consumer trade, the current legal framework – both at the EU and national level – remains fragmented and insufficiently transparent. Numerous regulations do not provide specific solutions. It also appears that, given the advancing technological advancements, they insufficiently protect consumers.

De lege lata, existing instruments are often general, imposing obligations without clear sanctions. It can be argued that they do not address current threats, such as the manipulation of consumer choices through recommendation systems and hidden patterns, violations of individual autonomy in decision-making processes, and uncertainty regarding liability for damage caused by AI systems.

De lege ferenda, it is justified to consider introducing a separate legal act regarding the use of AI in consumer trade. It is desirable to precisely define the consumer-AI relationship, establish clear obligations and responsibilities for entrepreneurs. A comprehensive law should provide a legal framework that is adapted to the pace of technological progress. The conclusions presented in this study are justified by the specific legal position of consumers as market participants.

Bibliography

1. CHIAPPINI, Daniele: The Legal Definition of Artificial Intelligence: A Comparative Perspective, In: European Journal of Comparative Law and Governance, no. 11(3), 2024, p. 360-387, <https://doi.org/10.1163/22134514-bja10071>.
2. GARG, Seema, MAHAJAN, Navita, GHOSH, Jayanta, Artificial Intelligence as an Emerging Technology in Global Trade: The Challenges and Possibilities, In: Vikas Garg, Richa Goel, Handbook of Research on Innovative Management Using AI in Industry 5.0, DOI: [10.4018/978-1-7998-8497-2.ch007](https://doi.org/10.4018/978-1-7998-8497-2.ch007), Publisher: IGI Global, 2022, p. 604 – 623, ISBN 978-166847461-7, 978-166847460-0.
3. JEDLIŃSKA-SABATOWSKA, Anna: Prawa konsumentów w erze AI: jak sztuczna inteligencja zmienia relacje w sferze B2C, In: Prawo Nowych Technologii no. 4, 2024, p. 53.
4. Judgment of Administrative Court in Warsaw of February 10, 2022 r., [I ACa 826/21](#), LEX nr 3324675.
5. Judgment of the Administrative Court in Szczecin of May 18, 2022 r., [I ACa 10/22](#), LEX nr 3433305.
6. JUŚCIŃSKI, Przemysław Piotr: Prawo autorskie w obliczu rozwoju sztucznej inteligencji, In: Zeszyty Naukowe Uniwersytetu Jagiellońskiego no. 1, 2019, p. 5-44.
7. KATNER, Wojciech Jan, In: W.J. Katner (ed.), Prawo cywilne i handlowe w zarysie, Warsaw 2021, p. 31, ISBN: 978-83-8246-547-1.
8. KOCOT, Wojciech Jerzy: Podmiotowość sztucznej inteligencji w nowym kodeksie cywilnym, In: Państwo i Prawo no 5, 2024, p. 108-134.
9. KRUCZALAK, Kazimierz: Prawo obrotu gospodarczego. Część I. Zagadnienia ogólne. Prawo handlowe, Gdańsk 1990, p. 5, ISBN: ISBN: 8370172717.
10. ŁĘTOWSKA, Ewa: Kształtowanie się odrębności obrotu mieszanego, In: E. Łętowska (ed.), Tendencje rozwoju prawa cywilnego, Wrocław, Warszawa, Kraków, Gdańsk, Łódź, 1983, p. 372. ISBN: 83-04-01467-x.
11. MARTSENKO, Natalia: Influence of artificial intelligence on the legal system, In: Studia Prawnoustrojowe no. 54, 2021, p. 388- 395.
12. MCCARTHY, John, MINSKY, Marvin L., ROCHESTER, Nathaniel, SHANNON Claude E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, <http://www-formal.stanford.edu/jmc/history/dartmouth.pdf> [data access: 6.02.2021].
13. NAGESH, Pal Singh; NIDHISH, Dev Lomash: Future of AI as Legal Personality, In: International Journal of Law Management & Humanities 4 (2021): 1116-[cvii].
14. NESSLER, Bernhard, WENDERHORS, Christiane: Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act, European Law Institute, Vienna, Austria 2024, ISBN: 978-3-9505495-3-9,

https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf; available on 14.09.2025.

15. NOWAK-BYRTEK, Dominika: Obowiązek zapewnienia transparentności przez dostawców i podmioty stosujące niektóre systemy AI, In: M. Gumularz, P. Kozik (ed.), *Ochrona danych osobowych w marketingu i sprzedaży*, Warsaw, 2025, p. 415 – 441, ISBN: 978-83-8356-877-5.
16. OSAJDA, Konrad: Granice statusu konsumenta w prawie cywilnym – perspektywa temporalna oraz kwestia niedokonania czynności prawnej, In: *Przegląd Sądowy* no 11-12, 2022, p. 41-53.
17. PACHUCA-SMULSKA, Beata: The System of Consumer Protection in Poland, In: *Consumer Protection Law in Poland from the Perspective of EU Law*, B. Pachuca-Smulska (ed.), Warsaw 2017, p. 16-17, ISBN: 978-83-255-9535-7.
18. PECYNA, Marlena: *Kontrola wzorców umownych poza obrotem konsumenckim*, Kraków 2003, p. 26, ISBN: 83-7333-183-2.
19. REJMANIAK, Rafał: Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego, In: *Roczniki Nauk Prawnych*, Tom XXXI, nr 3, 2021, p. 95-113, DOI: <http://doi.org/10.18290/rnp21313.6>.
20. RUTKOWSKA-TOMASZEWSKA, Edyta: Wzorce umowne w obrocie konsumenckim, In: *Zobowiązania w obrocie gospodarczym*, A. Malarewicz-Jakubów (ed.), Warsaw 2025, p. 509, ISBN: 978-83-8358-974-9.
21. RZYMOWSKI, Jakub: Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji, In: *Przegląd Prawa Publicznego*, no 11, 2024, p. 56-63.
22. SIWICKI, Maciej: Protection of consumers against abuse of artificial intelligence in electronic trade: the scalper bots case, In: [Balcerzak Michał, Kapelańska-Pręgowska Julia \(ed.\), Artificial intelligence and international human rights law developing standards for a changing world, 2024, Cheltenham, UK | Northampton, MA, Edward Elgar Publishing, p. 231-249, ISBN 978-1-0353-3792-Z.](#)
23. VEALE, Michael, BORGESIU, Frederik z.,: Demystifying the Draft EU Artificial Intelligence Act. In: *Computer Law Review International*, no. 22(4), 2021, p. 97–112.
24. VUJICIC, Jelena: Analysis of Proposed Artificial Intelligence Regulations: Perspectives from the United States, China, and the European Union, In: In Nadia E. Nedzel, Samuel O. Idowu, Belén Diaz Diaz, Irene Guia Arraiano & René Schmidpeter (eds.), [Global Corporate Governance: Proceedings of the 8th International Conference on CSR, Sustainability, Ethics and Governance, Baton Rouge, USA, June 2022.](#) Cham: Springer Nature Switzerland, pp. 173-194, 2025, DOI: 10.1007/978-3-031-86330-1_10, ISSN 21967075.

Contact details

Paweł Lewandowski, PhD

pawel.lewandowski@uwm.edu.pl

Univeristy of Warmia and Mazury in Olsztyn

Faculty of Law And Administration

Department of Economic Public Law and Commercial Law

VYUŽITIE DIGITÁLNYCH TECHNOLOGIÍ PRI VÝKONE ROZHODNUTIA VO VECIACH MALOLETÝCH: POMOCNÉ NÁSTROJE ALEBO HROZBY PRE NAJLEPŠÍ ZÁUJEM DIEŤAŤA?

THE USE OF DIGITAL TECHNOLOGIES IN DECISION-MAKING IN CASES INVOLVING MINORS: HELPFUL TOOLS OR THREATS TO THE BEST INTERESTS OF THE CHILD?

Tamara Čipková, Romana Smyčková¹

Abstrakt: Výkon rozhodnutia vo veciach maloletých musí reflektovať nielen osobitnú ochranu najlepšieho záujmu dieťaťa, ale súčasne kvalita jeho normatívneho rámca predstavuje výzvu pre zohľadnenie osobitostí procesného postupu, a to najmä s dôrazom na jeho efektivitu a právne limity ochrany rodinných hodnôt. Príspevok sa zameriava na analýzu a vyhodnotenie možnej miery zapojenia moderných technológií vo vykonávanom konaní s dôrazom na ochranu postavenia dieťaťa napr. formou monitoringu výkonu, virtuálnych stretnutí oprávneného subjektu s dieťaťom, či plánovaní stretnutí v rozsahu určenom v exekučnom titule.

Kľúčové slová: výkon rozhodnutia vo veciach maloletých, digitálne technológie, najlepší záujem dieťaťa, realizácia exekučného titulu

Abstract: The enforcement of decisions in matters concerning minors must reflect not only the special protection of the best interests of the child, but at the same time, the quality of its normative framework poses a challenge to take into account the specifics of the procedural process, with particular emphasis on its effectiveness and the legal limits of the protection of family values. The paper focuses on the analysis and evaluation of the possible extent of the involvement of modern technologies in enforcement proceedings, with an emphasis on protecting the status of the child, e.g., in the form of monitoring enforcement, virtual meetings between the authorized entity and the child, or planning meetings within the scope specified in the enforcement title.

¹ Právnická fakulta Univerzity Komenského v Bratislave, Katedra občianskeho práva

Key words: enforcement of decisions in matters of minors, digital technologies, best interests of the child, execution of an enforcement title

Úvod

Spoločnosť prechádzala a prechádza rôznymi vývojovými štádiami a je prirodzeným následkom, že svet okolo nás sa mení a život ovplyvňuje technologický progres a nové nároky sú kladené na rýchlu a pokiaľ možno aj „bezkontaktnú“ komunikáciu. Dnes sa bežne pohybujeme a komunikujeme v online priestore, dáta sa zberajú a ukladajú na rôznych druhoch nosičov, sú vytvárané systémy, ktoré ich môžu absorbovať v obrovskom množstve, do životov nám vstupujú fenomény ako umelá inteligencia, virtuálny priestor a pod.

Prirodzene sa uvedené premieta aj do platformy pre zdieľanie informácií a dát rôzneho typu a stieraním hraníc, čo vedie k problémom v rozpoznateľnosti medzi virtuálnou realitou a reálnym životom.

Hľadanie hraníc môže byť pre niektoré subjekty mimoriadne ťažké, až nemožné, prirodzene to tiež kladie nároky na riešenie nových otázok v spoločenskom styku, ale aj v právnej rovine. Sme nútení sa zamýšľať nad takými otázkami, ako je organizácia času a samotný faktor času, potlačenie bezprostredného reálneho kontaktu, ale aj otázkami bezpečnosti vo vzťahu k základným, zákonom chráneným hodnotám, akými sú ochrana súkromného a rodinného života, či ochrana osobných údajov.

Digitalizácia a elektronizácia sa jednoznačne prejavuje aj pri výkone súdnictva, ovplyvňuje nielen realizáciu procesných úkonov strán či účastníkov konania, ale aj úkony súdu vrátane spôsobov rozhodnutia a ich výkonu. Ak sme sa rozhodli analyzovať vplyv vývoja moderných technológií na špecifický druh súdneho konania, ktorým nepochybne je výkon rozhodnutia vo veciach maloletých (tzv. personálna exekúcia), je prirodzené, že v kontexte subjektov participujúcich na týchto procesných postupoch je namieste niekoľko zásadných a právne relevantných východísk a z nich plynúcich otázok. Za základné výskumné otázky pokladáme tieto:

- v akých fázach môžu moderné technológie vstupovať do konania?
- môžu moderné technológie zasahovať do výkonu rodičovských práv a povinností?
- kde je v prípadoch využívania digitálnych technológií v konaniach vo veciach starostlivosti súdu o maloletých hranica legitimacy a proporcionality zásahu?
- majú moderné technológie vôbec význam v právnej úprave rodinnoprávných vzťahov?

Vo vzťahu k výkonu rozhodnutia sa naskytá ďalšia výskumná otázka:

- môžu byť moderné technológie využité pri realizácii práva styku rodiča a dieťaťa?

Na základe uvedeného možno identifikovať hypotézu: *súčasná právna úprava výkonu rodičovských práv a povinností vrátane ich núteného výkonu pri personálnej exekúcii potvrdzuje možnosť ich realizácie s využitím moderných technológií s dôrazom na rešpektovanie ochrany najlepšieho záujmu dieťaťa*. Pri testovaní uvedenej hypotézy sme sa snažili zohľadniť ako najzásadnejšie oblasti: ochranu najlepšieho záujmu dieťaťa ako primárneho kritéria pre rešpektovanie jeho práv, podpory jeho zdravého psychického a emocionálneho vývinu, využitie moderných technológií pri náhrade fyzického, osobného kontaktu rodiča a dieťaťa, možnosti využitia moderných technológií pri plánovaní a monitoringu styku upraveného súdnym rozhodnutím a tiež pri komunikácii oprávneného a povinného subjektu.

Rodinnoprávne vzťahy, vzťah medzi rodičom a dieťaťom, najlepší záujem dieťaťa

Rodinnoprávne vzťahy predstavujú špecifický okruh vzťahov. Aj napriek existencii právnej regulácie sú penzom vzťahov limitovaných pomyslenými hranicami súkromia, autonómie vôle pri rozhodovaní v otázkach rodiny, výkonu rodičovských práv a povinností, či v širšom kontexte vo všetkom čo predstavuje súžitie v rodinnom spoločenstve. Právo na rodinný život je prirodzené právo spojené s osobnosťou človeka. Pod pojmom rodina pritom v súčasnej dobe možno rozumieť rôzne formy rodiny, ako napríklad nukleárna rodina, osamelý rodič a dieťa, širšia rodina, bezdetná rodina, rodina starých rodičov a pod. Medzi členmi rodiny je možné identifikovať emocionálne, ale aj materiálne väzby a rôznu dynamiku vzťahov.²

Právna úprava rodinnoprávných vzťahov s osobitným zreteľom na vzťah rodičov a detí vychádza z nosného princípu súkromného práva a to princípu rovnosti. Je ale prirodzené, že právna regulácia týchto vzťahov musí zohľadňovať ochranu slabšieho subjektu týchto vzťahov a tým je dieťa. Potreba dorovnávania nerovnovážne postavenia dieťaťa vyplýva z pozitívneho záväzku štátu chrániť rodinné vzťahy, právne postavenie dieťaťa, pri rešpektovaní súkromného a rodinného života a to aj pri nevyhnutnej intervencii do týchto vzťahov, kedy na základe spravidla vykonateľného rozhodnutia súdu dochádza k úprave výkonu rodičovských práv a povinností. Ak analyzujeme vzťahy, v ktorých dieťa vystupuje, je ho potrebné vnímať ako subjekt s ktorým sa viaže jeho legitímne oprávnenie realizovať sa v rodinnom prostredí a nie len prejavovať svoj názor, ale v širšom kontexte podieľať sa (participovať) na dotváraní rodinného spolužitia. S právnym postavením dieťaťa ako subjektu a nositeľa penza práv a povinností súvisí zachovanie a rešpektovanie miery ich uplatnenia. Práve v tomto význame je potrebné zamyslieť sa nad vplyvom vývoja moderných technológií, ktorých prienik do najintímnejších sfér rodinného

² LUPRICHOVÁ, Petronela. Rodina v 21. storočí. In: Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2022. Univerzita Komenského v Bratislave, Právnická fakulta, 2022. s. 26.

prostredia prináša výzvy smerujúce k naplneniu medzinárodných záväzkov vo vzťahu k ochrane záujmov dieťaťa. Uvedené je ešte väčšou výzvou pri rozhodovaní o autoritatívnom usmernení výkonu rodičovských oprávnení so zachovaním ochrany právneho postavenia dieťaťa. Nájdenie toho „správneho“ záujmu dieťaťa znamená v rozhodnutí, ak už k nemu musí dôjsť, ustáliť pre dieťa najvýhodnejšiu konšteláciu existujúcich potrieb dieťaťa a jeho životných podmienok. Analýzou právnej úpravy v hmotnoprávnej aj procesnej rovine³ a to ja s dôrazom na základné princípy, na ktorých je budovaná možno konštatovať, že rešpektuje zachovanie preferencie ochrany verejných záujmov smerujúcich k naplneniu najlepšieho záujmu dieťaťa, nediskriminácie, práve prezentovať svoj názor, právo na zachovanie kontaktu dieťaťa s rodičmi a rodinnými príslušníkmi na pravidelnej báze a ponechanie priestoru na základe legitimitu zásahu a intervencie len v odôvodnených prípadoch.

Zákon o rodine v ustanoveniach § 24, § 25 a § 36 len všeobecne uvádza, že súd upraví výkon rodičovských práv a povinností v rozsahu osobnej starostlivosti o dieťa, resp. upraví styk rodiča a maloletého dieťaťa. Rovnako všeobecne pristupuje zákon aj k úprave styku maloletého s blízkymi osobami. Nenormuje konkrétne formy realizácie styku s maloletým, preto je možné uvažovať aj o aplikácii digitálnych prostriedkov sprostredkovaného styku. Napokon, už aj Ústavný súd Slovenskej republiky sa vyjadril k otázke kolízie medzi digitálnym a osobným stykom počas pandémie Covid-19. Dospel pritom k záveru: *„ak sa osobný styk nahradí výlučne technickým stykom (videom), aj keď existovali možnosti udržania osobného styku za prípadnej asistencie, ide už o veľmi závažný zásah do základných práv, ktoré reprezentujú aj referenčné normy.“*⁴ Uvedené rozhodnutie nemožno vnímať ako absolútny zákaz úvah o nariadení styku prostredníctvom technických prostriedkov, práve naopak. Je zrejmé, že aj s touto formou realizácie styku možno v podmienkach Slovenskej republiky počítať, ale so zachovaním prísneho testu proporcionality jeho aplikácie najmä z pohľadu zachovania najlepšieho záujmu dieťaťa.

Výkon rozhodnutia vo veciach maloletých ako flexibilný mimosporový proces

Nie len legislatívne ukotvenie⁵, ale primárne doktrínalne východiská predurčujú a ovplyvňujú procesný postup v konaniach vo veciach maloletých a to tak v základnom, ako aj vo vykonávacom konaní. Uvedené úzko súvisí s už spomínaným pozitívnym záväzkom štátu chrániť rodinnoprávne vzťahy a intervenovať do týchto

³ Zákon č. 36/2005 Z. z. o rodine a o zmene a doplnení niektorých zákonov; zákon č. 161/2015 Z. z. Civilný mimosporový poriadok.

⁴ Nález Ústavného súdu Slovenskej republiky č. k. III. ÚS 38/2021 z 15. apríla 2021 zverejnený pod R ÚS 23/2021.

⁵ Zákon č. 161/2015 Z. z. civilný mimosporový poriadok, IV. Časť : Výkon rozhodnutia vo veciach maloletých.

vzťahov formou autoritatívneho rozhodnutia resp. jeho výkonu len v odôvodnených prípadoch a v nevyhnutnej miere. Povaha súdneho výkonu rozhodnutia vo veciach maloletých reflektuje nielen primárnu ochranu postavenia dieťaťa, ale aj zachovanie efektívneho postupu, smerujúceho k zachovaniu práv dieťaťa na kontakt s rodičmi, či inými oprávnenými osobami. To sa prejavuje nie len v možnosti začať konanie o výkon rozhodnutia *ex offio*, ale aj v možnosti využitia zákonných alternatív ovplyvňujúcich priebeh konania. Exekučné tituly v tomto type konaní smerujú k realizácii styku s dieťaťom, či iných ako peňažných povinností, vrátane rozhodnutí o týchto otázkach formou tzv. neodkladných opatrení.⁶ Procesný postup svojou právnou úpravou má priestor pre využitie alternatívnych „procesných nástrojov“, aby bol realizovaný aj prostredníctvom využitia moderných technológií. Použitie týchto sa prezumuje aj pri jeho samotnom priebehu (vytváranie zvukových a obrazových záznamov a ich uchovávanie na príslušných nosičoch), čo môže prispieť nie len k jeho efektívnemu uskutočneniu, ale aj prípadnej následnej kontrole, ak nastanú pochybnosti o legitimitě postupu v konaní.⁷ Využitie nových procesných nástrojov má svoje opodstatnenie aj s ohľadom na časový faktor, ktorý bezprostredne súvisí s eliminovaním nežiaducich konfliktov vyplývajúcich z výkonu rodičovských práv a povinností, tiež z pohľadu „zraniteľného“ dieťaťa, pre ktoré faktor času môže mať za následok oslabenie, či stratu väzieb a kontaktu s rodičom, čím môže dôjsť k nenapraviteľným stratám vo vzťahoch rozhodujúcich pri ovplyvňovaní vývinu dieťaťa.⁸ Človek sa sám definuje tým, aké má schopnosti, ale aj osobami, ku ktorým má vytvorené väzby. Súčasťou identity dospievajúcich detí sú ich blízke osoby a skupiny, ku ktorým patria.⁹ Výchovnou úlohou každého rodiča je podporovať vzťah dieťaťa s druhým rodičom a viesť ho k úcte a rešpektu k druhému rodičovi.¹⁰ Nie vždy si však túto úlohu rodičia riadne plnia, čo môže viesť k zhoršeniu vzájomných vzťahov v rodine. Práve preto považujeme za možné v racionálnej a kontrolovanej miere využiť alternatívnych foriem zachovania kontaktov v rodine (aj mimo rámca osobného kontaktu) v rozsahu judikovanom v exekučnom titule, ak už došlo k ich autoritatívnej úprave. Pritom je potrebné brať ohľad na zachovanie, nie

⁶ GEŠKOVÁ, Katarína. § 370. Exekučný titul. In: SMYČKOVÁ, R. a kol. Civilný mimosporový poriadok. 2. vydanie. Bratislava: C. H. Beck, 2024, s. 1131.

⁷ Vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 207/2016 Z. z. ktorou sa upravujú podrobnosti výkonu rozhodnutia vo veciach maloletých, Vyhláška MS SR č. 543/2005 Z. z. o Spravovacom a kancelárskom poriadku pre okresné sudy, krajské sudy, Špeciálny súd a vojenské sudy.

⁸ ZMEKOVÁ, Ivana. Úprava výkonu rodičovských práv a povinností k maloletým deťom. Praha: PRP Consulting, 2022. s. 187 – 188.

⁹ VÁGNEROVÁ, Marie – LISÁ, Lidka. Vývojová psychologie: dětství a dospívání. Praha: Karolinum, 2021. s. 451.

¹⁰ BÁNOS, Róbert - KOŠÚTOVÁ, Martina a. Zákon o rodine: veľký komentár. Bratislava: Eurokódex, 2023. s. 87.

deformovanie a vynútenie si vôle maloletého, čo by znamenalo zásah do rodinného života.¹¹

Digitálne nástroje v konaniach vo veciach starostlivosti súdu o maloletých

Konania vo veciach starostlivosti súdu o maloletých patria medzi najcitlivejšie oblasti civilného procesu. Pri rozhodovaní aj pri samotnom výkone súdnych rozhodnutí sa vždy musí klásť dôraz na rešpektovanie najlepšieho záujmu dieťaťa, ktoré je slabším subjektom rodinnoprávnych vzťahov. V posledných rokoch sa do popredia dostáva otázka, do akej miery možno do tejto špecifickej agendy zapájať moderné digitálne technológie. Tieto nástroje majú potenciál uľahčiť a zrýchliť konanie, zároveň však prinášajú aj otázky súvisiace s participáciou dieťaťa, legitimitou a proporcionalitou zásahu do rodinného života zúčastnených subjektov.

Civilný sporový poriadok v § 175 ods. 2 poskytuje možnosti účasti na pojednávaní prostredníctvom videokonferencie. Uvedené sa v súlade so zásadou subsidiarity (§ 2 ods. 1 CMP) aplikuje aj v mimosporových konaniach. Napriek prípustnosti využitia videokonferencie, slovenská právna úprava je v tomto smere stále pomerne konzervatívna, vzhľadom na to, že pojednávanie sa musí uskutočniť v pojednávacej miestnosti, ktorej bude sudca. Na diaľku môže v zmysle tohto zákonného ustanovenia vystupovať len strana/účastník konania. Uvedený reštriktívny prístup by však v mnohých prípadoch mohol znamenať napríklad zmarenia riadneho dokazovania (svedok je dlhodobo v zahraničí) a bol by v rozpore so zásadami rýchlosti a hospodárnosti konania, preto sa stotožňujeme s názorom, že prostredníctvom videokonferencie sa okrem strany sporu, môžu konania zúčastniť aj zástupca strany, svedok, znalec alebo tlmočník.¹²

Skúsenosti z Anglicka a Walesu, kde sa počas pandémie COVID-19 vo veľkej miere prešlo do digitálneho prostredia, ukazujú, že tento spôsob má viacero výhod.¹³ Pojednávania sa začínali načas a celkovo sa zvýšila efektivita ich priebehu. Účastníci, najmä tí, ktorí žijú vo väčšej vzdialenosti od súdu, sa dokázali zúčastniť bez zbytočných cestovných nákladov a problémov s logistikou, či dochvilnosťou. Ďalším pozitívom bolo, že obeť domáceho násillia, prípadne konfliktných vzťahov nemuseli čeliť priamemu kontaktu s druhou stranou, čo prispelo k väčšiemu pocitu bezpečia a emocionálnej stability. Viacerí účastníci uvádzali aj zníženie stresu, keďže nemuseli

¹¹ Nález Ústavného súdu Českej republiky z 13. októbra 2015, sp. zn. III.ÚS 3462/2014.

¹² ŠORL, Robert. § 175 Uskutočňovanie a zaznamenávanie priebehu pojednávania pomocou technických zariadení. In: ŠTEVČEK, Marek a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022, s. 701.

¹³ HARKER, Lucy – RYAN, Maggie: Remote hearings in family courts in England and Wales during Covid-19: Insights and lessons. In: Family Court Review, 60 (2) (2022), s. 212–213.

byť fyzicky prítomní v súdnej sieni, v ktorej často vládne napätie.¹⁴ Niektorí rodičia sa naopak cítili v domácom prostredí zraniteľnejší, keďže im chýbala emocionálna podpora zo strany ich právneho zástupcu alebo iného subjektu.¹⁵

V praxi sa ukázali aj limity a nevýhody tohto systému. Predovšetkým sa poukazovalo na to, že vzdialené vypočúvanie komplikuje hodnotenie neverbálnych prejavov účastníkov a sťažuje posúdenie dôveryhodnosti výpovedí. Najmenšiu podporu mali diaľkové formy konania pri tzv. „fact-finding hearings“, pri konečných rozhodnutiach a v sporoch o realizáciu styku či zverenie dieťaťa do starostlivosti, kde bola osobná prítomnosť považovaná za nenahraditeľnú. Značné problémy spôsobovali aj technické prekážky, nedostatočné pripojenie alebo nedostatok vhodných zariadení, ktoré obmedzovali plnohodnotnú účasť niektorých rodičov. Objavil sa aj pocit marginalizácie, keď sa účastníci cítili byť skôr pasívnymi pozorovateľmi ako aktívnou súčasťou konania.¹⁶ Z týchto zistení vyplýva, že hoci procesné úkony realizované prostredníctvom digitálnych prostriedkov majú v rodinnoprávnych konaniach v súčasnej dobe svoje miesto a prispievajú k efektívnosti systému, ich využitie by malo byť vždy posudzované individuálne, podľa povahy konkrétneho prípadu.

Je potrebné vziať do úvahy, že právny poriadok v § 24 ods. 4 zákona o rodine stanovuje ako podmienku pri rozhodovaní o úprave výkonu rodičovských práv a povinností rešpektovanie práva maloletého dieťaťa na zachovanie jeho vzťahu k obidvom rodičom¹⁷. Práve digitálne technológie môžu pomôcť tomu, aby dieťa nestratilo kontakt s jedným z rodičov, ktorý je napríklad dlhodobo služobne v zahraničí. Rovnako môžu digitálne technológie prispieť k tomu, aby sa neexistujúce alebo narušené vzťahové väzby, postupne, menej invazívnym spôsobom, vytvárali alebo reparaovali.

Aplikácie na plánovanie kontaktu s dieťaťom po rozchode rodičov

Jednou z novších foriem využitia digitálnych technológií v rodinných vzťahoch sú špecializované aplikácie určené pre rodičov po rozchode alebo rozvode. Ich základným cieľom je zlepšiť organizáciu a komunikáciu medzi rodičmi pri zabezpečovaní styku s dieťaťom, a tým prispieť k zníženiu konfliktov, ktoré sa často prenášajú priamo na dieťa. Medzi najčastejšie funkcie týchto aplikácií patrí zdieľaný

¹⁴ RYAN, Mary – ROTHERA, Sarah – ROE, Alice – REHILL, Jordan – HARKER, Lisa: Remote hearings in the family court post pandemic. In: Nuffield Family Justice Observatory Report, (2021), s. 12.

¹⁵ HARKER, Lucy – RYAN, Maggie: Remote hearings in family courts in England and Wales during Covid-19: Insights and lessons. In: Family Court Review, 60 (2) (2022), s. 214.

¹⁶ RYAN, Mary – ROTHERA, Sarah – ROE, Alice – REHILL, Jordan – HARKER, Lisa: Remote hearings in the family court post pandemic. In: Nuffield Family Justice Observatory Report, (2021), s. 13 – 14.

¹⁷ PAVELKOVÁ, Bronislava. Zákon o rodine a o zmene a doplnení niektorých zákonov. 3. vydanie. Bratislava: C. H. Beck, 2019, s. 148.

kalendár styku, zasielanie notifikácií a pripomienok, sledovanie výdavkov na dieťa, bezpečná komunikačná platforma alebo možnosť exportovať záznamy o priebehu kontaktov. V zmysle týchto funkcionalít môžu aplikácie slúžiť aj v súdnych konaniach ako plánovací a zároveň kontrolný mechanizmus, z ktorého súd môže čerpať dôkazný materiál pre svoje rozhodovanie.

Výskum realizovaný v Austrálii ukázal, že tieto aplikácie môžu mať pozitívny vplyv na transparentnosť dohôd a v niektorých prípadoch znižujú intenzitu konfliktných situácií.¹⁸ Rodičia oceňovali najmä možnosť evidovať dohodnuté termíny a rýchlo odkomunikovať praktické záležitosti bez potreby priamej interakcie. Aplikácie môžu byť prínosné pri znížení každodenných konfliktov a zabezpečení komunikácie. Zároveň je však potrebné zdôrazniť, že ich využitie nie je univerzálne a závisí od povahy prípadu. V situáciách, kde rodičia vykazujú vysokú mieru konfliktu, nedôveru alebo manipulatívne správanie, aplikácie neposkytujú očakávané výsledky a môžu dokonca prispieť k eskalácii sporov.¹⁹

Identifikované boli aj viaceré nevýhody, napríklad technického charakteru. Aplikácie nie sú jednotne vyvinuté, chýba konzistentnosť funkcií, ich používateľské rozhranie je neraz málo intuitívne a niektoré riešenia vykazujú problémy kompatibility medzi rôznymi zariadeniami.²⁰

Významnou témou je aj dobrovoľnosť používania týchto aplikácií. Súd by ich nemali nariaďovať autoritatívne, ale rodičom by mali byť ponúkané ako možnosť, s ktorou musia obaja súhlasiť. V opačnom prípade môže dôjsť k posilneniu mocenskej nerovnováhy medzi rodičmi alebo k pocitu, že technológia sa stáva ďalším nástrojom kontroly.²¹

Záznamy z aplikácií majú len obmedzenú dôkaznú hodnotu, pokiaľ nie sú overené, nemožno ich považovať za plnohodnotný podklad pre súdne rozhodovanie.²²

¹⁸ SMYTH, Bruce M. – PAYNE, Jason L. – IRVING, Michelle – HEARD, Genevieve: Popular post-separation parenting smartphone apps: An evaluation. In: *Family Court Review*, 61 (1) (2023), 563 – 568.

¹⁹ IRVING, Michelle A. – HEARD, Genevieve – SMYTH, Bruce M. – PAYNE, Jason L. – ALTHOR, Glenn: Post-separation parenting apps in the hands of family law practitioners: Expectations versus experience. In: *International Journal of Law, Policy and the Family*, 37 (1) (2023), ebad027, s. 18.

²⁰ SMYTH, Bruce M. – PAYNE, Jason L. – IRVING, Michelle – HEARD, Genevieve: Popular post-separation parenting smartphone apps: An evaluation. In: *Family Court Review*, 61 (1) (2023), 580 – 581.

²¹ SMYTH, Bruce M. – PAYNE, Jason L. – IRVING, Michelle – HEARD, Genevieve: Popular post-separation parenting smartphone apps: An evaluation. In: *Family Court Review*, 61 (1) (2023), 581.

²² HEARD, G. M., IRVING, M. A., SMYTH, B. M., PAYNE, J. L., & ALTHOR, G. (2023). Risks and benefits of post-separation parenting apps: perceptions of family law professionals in Australia and New Zealand. *Journal of Social Welfare and Family Law*, 45 (2), s. 144–145.

Aplikácie môžu byť účinným pomocníkom pri plánovaní a evidencii styku, ale len vtedy, ak ich rodičia používajú dobrovoľne a s podporou odborníkov. Pri povinnom nariadení ich používania alebo v prostredí vysoko konfliktných vzťahov sa ich efektivita znižuje. Z pohľadu súdnej praxe je preto vhodné chápať tieto technológie ako podporný, nie primárny nástroj realizácie povinností vyplývajúcich z rozhodnutí, pričom ich uplatnenie má byť vždy posudzované v kontexte najlepšieho záujmu dieťaťa.²³

Z pohľadu slovenského právneho poriadku by takéto aplikácie mohli nájsť svoje uplatnenie najmä ako doplnkový nástroj po právoplatnosti súdneho rozhodnutia, napríklad pri plánovaní styku alebo evidencii jeho realizácie. Ich využitie by však muselo byť sprevádzané jasnými pravidlami ochrany osobných údajov a primeraným metodickým usmernením zo strany štátu alebo súdov. Následne by informácie z týchto aplikácií mohli slúžiť ako dôkazný materiál aj v rámci vykonávacieho konania. Najmä, ak by išlo o aplikáciu, ktorá by zabezpečovala aj dostatočnú dôveryhodnosť dát. Predpokladom pre ich úspešné nasadenie by zároveň bola aj dostupnosť v slovenskom jazyku²⁴, intuitívnosť pre rodičov s rôznou mierou digitálnej gramotnosti a možnosť jednoduchého overenia správnosti dát.

Aplikácie na plánovanie kontaktu predstavujú zaujímavý príklad toho, ako môže digitalizácia prispieť k posilneniu právnej istoty a zníženiu zbytočných konfliktov. Ich potenciál však nemožno absolutizovať, musia byť vnímané ako podporný nástroj, nie ako univerzálne riešenie, a ich využitie by malo vždy rešpektovať princíp najlepšieho záujmu dieťaťa, ako aj individuálny charakter každej rodinnoprávnej veci.

Záver

Digitálna transformácia je nepochybne jedným z krokov k zlepšeniu prístupu k spravodlivosti, ako aj efektívnosti, kvalite a transparentnosti justičných systémov, súdneho procesu vrátane výkonu rodičovských práv a povinností a to aj pri prípadnej intervencii štátu formou ich vynútenia. Tento vývoj a s ním súvisiace zmeny *nemôžu rezignovať na dodržiavanie základných práv a hodnôt*, a to najmä tým, že sa v oblasti justície umožní účinne riešiť všetky výzvy, ktoré by mohli z dôvodu ich virtuálnej povahy vzniknúť počas konaní a pri realizovaní procesných postupov a úkonov uskutočňovaných prostredníctvom využitia moderných technológií. Uvedené je

²³ IRVING, Michelle A. – HEARD, Genevieve – SMYTH, Bruce M. – PAYNE, Jason L. – ALTHOR, Glenn: Post-separation parenting apps in the hands of family law practitioners: Expectations versus experience. In: International Journal of Law, Policy and the Family, 37 (1) (2023), ebado27, s. 18.

²⁴ V čase písania tohto článku sa nám nepodarilo nájsť aplikáciu, ktorá by takéto funkcionality v slovenskom jazyku ponúkala. V anglickom jazyku je takýchto aplikácií niekoľko a sú voľne dostupné pre užívateľov na stiahnutie. V záujme nepreferovania žiadnej z nich neuvádzame konkrétne príklady, ale ich vyhľadávanie je v obchodoch s mobilnými aplikáciami zjednodušené napríklad použitím kľúčového slova „co-parent“.

potrebné zdôrazniť o to viac, že v nami analyzovaných právnych vzťahoch je jedným zo subjektov dieťa. Ochrana jeho záujmov v kontexte ostatných, štátom uznaných hodnôt, musí byť konfrontovaná s mierou možného prieniku moderných technológií a to s dôrazom na osobitný charakter rodinnoprávných vzťahov. Ťažiskom ústavného systému musí byť a zostať jednotlivец (osoba, človek vo všetkých fázach jeho vývinu) *a jeho práva*, ktoré sú s ním neodmysliteľne späté a ktoré tvoria pomyselnú hranicu limitov, s ktorými by mali byť konfrontované novodobé technológie pri výkone súdnictva.

Na základe vykonanej analýzy možno potvrdiť základnú výskumnú hypotézu, podľa ktorej súčasná právna úprava výkonu rodičovských práv a povinností, vrátane ich núteného výkonu pri personálnej exekúcii, nebráni využívaniu moderných digitálnych technológií. Civilný sporový poriadok výslovne počíta s možnosťou využitia technických prostriedkov pri pojednávaní (najmä formou videokonferencie), pričom sa týmto spôsobom neobchádza požiadavka na osobnú prítomnosť účastníkov, ale vytvára sa flexibilný rámec pre efektívnejší a bezpečný priebeh konania. V mimosporových konaniach, ktoré sa uplatňujú v konaniach vo veciach starostlivosti súdu o maloletých, ako aj pri výkone rozhodnutí vo veciach maloletých, je možné tieto ustanovenia primerane aplikovať, a to vždy s dôrazom na rešpektovanie princípu najlepšieho záujmu dieťaťa.

Moderné technológie často vstupujú do konania už vo fáze pred jeho začatím (elektronické podanie), počas samotného konania (účasť na pojednávaní prostredníctvom videokonferencie, elektronická komunikácia účastníkov so súdom), pri rozhodovaní (forma výkonu styku upravená prostredníctvom videostretnutí) a vo fáze výkonu rozhodnutia (digitálne plánovanie styku, záznamy o realizovaní, či nerealizovaní styku). Využitie digitálnych nástrojov pri realizácii styku dieťaťa s rodičom je možné, ak sú prostriedkom na zabezpečenie alebo podporu osobného styku, nie jeho absolútnou náhradou. Digitálne nástroje môžu pomôcť pri zachovaní kontaktu (napr. videohovory v situáciách, keď osobný kontakt nie je vhodný alebo možný – zdravotný stav, vzdialenosť, potreba znovuobnovenia kontaktu a pod.), avšak nemôžu trvalo a úplne nahradiť podstatu osobného styku rodiča a dieťaťa.

Do rozhodovacieho procesu môžu digitálne technológie zasahovať len nepriamo. Napríklad môžu súdu sprostredkovať relevantné informácie (o neplnení povinností prostredníctvom zdieľaných aplikácií, ktoré by mohli predstavovať jeden z dôkazov pre zmenu rozhodnutia alebo uskutočnenie výkonu rozhodnutia a pod.). Samotný rozhodovací proces však zostáva výlučne v kompetencii súdu. Moderné technológie môžu byť pomocným nástrojom, ale nie absolútnou náhradou za vlastné hodnotenie dôkazov a na ich základe vydané autoritatívne rozhodnutie zo strany sudcu.

Záverom možno uviesť, že moderné technológie majú aj v rámci úpravy rodinnoprávných vzťahov svoj význam. Musia však byť využívané efektívne a citlivo, s ohľadom na ochranu najlepšieho záujmu dieťaťa.

Zoznam použitej literatúry

1. BÁNOS, Róbert - KOŠÚTOVÁ, Martina. Zákon o rodine: veľký komentár. Bratislava: Eurokódex, 2023. 540 s. ISBN 978-80-8155-119-2
2. GEŠKOVÁ, Katarína. § 370. Exekučný titul. In: SMYČKOVÁ, Romana a kol. Civilný mimosporový poriadok. 2. vydanie. Bratislava: C. H. Beck, 2024, 1240 s. ISBN 978-80-8232-049-0.
3. HARKER, Lucy – RYAN, Maggie: Remote hearings in family courts in England and Wales during Covid-19: Insights and lessons. In: Family Court Review, 60 (2) (2022), s. 207–219. <https://doi.org/10.1111/fcre.12638>
4. HEARD, G. M., IRVING, M. A., SMYTH, B. M., PAYNE, J. L., & ALTHOR, G.. Risks and benefits of post-separation parenting apps: perceptions of family law professionals in Australia and New Zealand. Journal of Social Welfare and Family Law, 45(2) (2023), s. 143–164. <https://doi.org/10.1080/09649069.2023.2206225>
5. IRVING, Michelle A. – HEARD, Genevieve M. – SMYTH, Bruce M. – PAYNE, Jason L. – ALTHOR, Glenn. Post-separation parenting apps in the hands of family law practitioners: Expectations versus experience. In: International Journal of Law, Policy and the Family, 37, 1 (2023), ebad027. <https://doi.org/10.1093/lawfam/ebad027>
6. LUPRICOVÁ, Petronela. Rodina v 21. storočí. In: Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2022. Univerzita Komenského v Bratislave, Právnická fakulta, 2022. s. 24 - 28. ISBN 978-80-7160-665-9.
7. PAVELKOVÁ, Bronislava. Zákon o rodine a o zmene a doplnení niektorých zákonov. 3. vydanie. Bratislava: C. H. Beck, 2019, 688 s. ISBN 978-80-89603-72-5.
8. RYAN, Mary – ROTHERA, Sarah – ROE, Alice – REHILL, Jordan – HARKER, Lisa: Remote hearings in the family court post pandemic. In: Nuffield Family Justice Observatory Report, (2021), s. 1–48.
9. SMYTH, Bruce M. – PAYNE, Jason L. – IRVING, Michelle – HEARD, Genevieve M.: Popular post-separation parenting smartphone apps: An evaluation. In: Family Court Review, 61 (3) (2023), s. 563 - 585. <https://doi.org/10.1111/fcre.12738>
10. ŠORL, Robert. § 175 Uskutočňovanie a zaznamenávanie priebehu pojednávania pomocou technických zariadení. In: ŠTEVČEK, Marek a kol. Civilný sporový poriadok. 2. vydanie. Praha: C. H. Beck, 2022, 1752 s. ISBN: 978-80-7400-909-9.
11. VÁGNEROVÁ, Marie – LISÁ, Lidka. Vývojová psychologie: dětství a dospívání. Praha: Karolinum, 2021. 544 s. ISBN 978-80-246-4961-0.
12. ZMEKOVÁ, Ivana. Úprava výkonu rodičovských práv a povinností k maloletým deťom. Praha: PRP Consulting, 2022. 310 s. ISBN 978-80-974-2010-9.

Kontaktné údaje

Mgr. Tamara Čipková, PhD.

tamara.cipkova@flaw.uniba.sk

prof. JUDr. Romana Smyčková, PhD.

romana.smyckova@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

ZRUŠENIE ROZHODCOVSKÉHO ROZSUDKU – NIEKOĽKO ÚVAH O (NE)DOSTATOČNOSTI PLATNEJ PRÁVNEJ ÚPRAVY

ANNULMENT OF AN ARBITRAL AWARD – SOME THOUGHTS ON THE (IN)ADEQUACY OF THE CURRENT LEGAL FRAMEWORK

Radoslav Hnilica¹

Abstrakt: Príspevok sa zaoberá problematikou žaloby na zrušenie tuzemského rozhodcovského rozsudku ako osobitného právneho inštitútu predstavujúceho výnimočný prostriedok kontroly rozhodcovských konaní všeobecnými súdmi. Cieľom je identifikovať nedostatky platnej právnej úpravy obsiahnutej v zákone č. 244/2002 Z.z. o rozhodcovskom konaní a formulovať úvahy o jej doplnení či spresnení. Autor vychádza z analýzy pozitívnoprávnej úpravy, jej výkladu v doktríne a rozhodovacej praxi všeobecných súdov, pričom osobitnú pozornosť venuje otázke preskúmateľnosti odôvodnenia rozhodcovského rozsudku ako potenciálneho dôvodu pre jeho zrušenie. Metodologicky sa príspevok opiera o komparatívny prístup, ktorý zohľadňuje zahraničné legislatívne modely, ako aj judikatúru najvyšších súdnych autorít v Slovenskej republike. Dosiahnuté závery poukazujú na medzerovitú úpravu požiadaviek na riadne odôvodnenie rozhodcovského rozsudku, na nedostatočne precizované pravidlá o príslušnosti všeobecných súdov po jeho zrušení a na absenciu právneho rámca digitalizácie rozhodcovských procesov. Vedeckým prínosom príspevku je konceptuálne uchopenie uvedených problémov a návrh možného legislatívneho riešenia. Praktický prínos spočíva v poskytovaní interpretačných východísk pre rozhodovaciu prax súdov a v podnete pre ďalšiu diskusiu o optimalizácii právnej úpravy rozhodcovského konania v podmienkach Slovenskej republiky.

Kľúčové slová: (rozhodcovské konanie, rozhodcovský rozsudok, rozhodca, preskúmanie rozhodcovského rozsudku, zrušenie rozhodcovského rozsudku)

Abstract: The article deals with the issue of actions for the annulment of domestic arbitral awards as a special legal institute representing an exceptional means of review of arbitral proceedings by general courts. The aim is to identify the shortcomings of the current legal regulation contained in the Arbitration Act No. 244/2002 Coll. and to formulate considerations for its supplementation

¹ Univerzita Komenského v Bratislave, Právnická fakulta

or clarification. The author draws on an analysis of positive law, its interpretation in doctrine and the decision-making practice of general courts, paying particular attention to the issue of the reviewability of the reasoning behind an arbitral award as a potential ground for its annulment. Methodologically, the article is based on a comparative approach that takes into account foreign legislative models as well as the case law of the highest judicial authorities in the Slovak Republic. The conclusions reached point to gaps in the regulation of the requirements for the reasoning of an arbitral award, insufficiently precise rules on the jurisdiction of general courts after its annulment, and the absence of a legal framework for the digitization of arbitration proceedings. The scientific contribution of the paper lies in its conceptual approach to the above-mentioned problems and its proposal for a possible legislative solution. The practical contribution lies in providing interpretative guidelines for the decision-making practice of courts and in stimulating further discussion on the optimization of the legal regulation of arbitration proceedings in the Slovak Republic.

Key words: (arbitration, arbitral award, arbitrator, review of an arbitral award, annulment of an arbitral award)

Úvod

Rozhodcovské konanie je v súčasnosti už etablované ako efektívna a pomerne využívaná alternatíva k riešeniu sporov pred všeobecnými súdmi. Ide pritom o inštitút, ktorý má v našich právnych podmienkach dlhodobú tradíciu v podobe alternatívneho riešenia predovšetkým obchodno-právnych sporov.² V rozhodcovskom konaní je garantovaná možnosť dosiahnuť vydanie záväzného rozhodnutia a rovnako aj možnosť jeho vynútenia štátnou mocou. Eventualitu vzniku rôznych procesných pochybení a väd rozhodcovských rozhodnutí nemožno ani v tomto druhu procesu nikdy celkom vylúčiť. Jednou z mála možností nápravy vadných a nesprávnych rozhodcovských rozhodnutí je žaloba na zrušenie tuzemského rozhodcovského rozsudku.

Podľa odbornej literatúry sú rozhodnutia rozhodcov spravidla konečné a záväzné. „Neexistujú žiadne alebo len veľmi obmedzené dôvody, na základe ktorých sa možno

² KUBÍČEK, Pavol: Niekoľko poznámok k vývoju právnej úpravy rozhodcovského konania v Slovenskej republike. In: Právo, obchod, ekonomika. Košice: Univerzita P. J. Šafárika v Košiciach, 2024. s. 251. ISBN 978-80-574-0389-0.

proti rozhodnutiam rozhodcov odvolať na súd z dôvodu, že závery rozhodcov sú nesprávne.“.³

Všeobecné súdy vo vzťahu ku rozhodcovským súdom vykonávajú niektoré pomocné ako aj kontrolné funkcie napr. rozhodujú o ustanovení rozhodcu, námietke proti rozhodcovi, námietke nedostatku právomoci, rozhodujú o žalobách na zrušenie tuzemského rozhodcovského rozsudku. Ministerstvo spravodlivosti SR síce nedisponuje štatistikami o počte nápadu sporov na rozhodcovské súdy v tom ktorom roku, avšak disponuje štatistikami o počte žalôb podaných na všeobecné súdy podľa zákona č. 244/2002 Z. z. o rozhodcovskom konaní v znení neskorších predpisov (ďalej len „ZRK“), ktoré sú evidované v súdnom registri Cr. Podľa štatistík Ministerstva spravodlivosti SR od roku 2021 každoročne opätovne narastá početnosť nápadu týchto vecí na všeobecné súdy (r. 2018 – 181 vecí; r. 2019 – 106 vecí; r. 2020 – 59 vecí; r. 2021 – 47 vecí; r. 2022 – 68 vecí; r. 2023 – 69 vecí; r. 2024 – 84 vecí).⁴ Z hľadiska budovania dôvery v rozhodcovské súdnictvo je táto znovu narastajúca tendencia podávania žalôb na všeobecné súdy pomerne znepokojujúca. Hoci v kontexte nápadu sporov v iných súdnych agendách nejde o veľký nápad vecí, po odznení pandemických opatrení ich početnosť začína postupne opätovne narastať. I tieto relatívne čísla tak naznačujú, že aj rozhodcovské konanie má stále svoje problémové miesta, na ktoré je potrebné reflektovať.

Žaloba na zrušenie tuzemského rozhodcovského rozsudku

Vo všeobecnosti je rozhodcovské konanie zásadne jednoinštančné (nemožno ho preskúmať opravným prostriedkom so suspenzívnym účinkom). Na dvojinštančnosti – preskúmaní rozhodcovského rozsudku iným rozhodcom resp. rozhodcami sa zmluvné strany musia vopred dohodnúť v rozhodcovskej zmluve; inak je také preskúmanie vylúčené. Žiadosť o preskúmanie rozhodcovského rozsudku iným rozhodcom je pritom jediným univerzálnym opravným prostriedkom umožňujúcim preskúmanie rozhodcovského rozsudku ako z procesných, tak i hmotnoprávných dôvodov. V prípade, že sa zmluvné strany rozhodcovskej zmluvy nedohodli na preskúmateľnosti rozhodcovského rozsudku iným rozhodcom (dvojinštančnom konaní), strana ktorá nie je s rozhodnutím rozhodcovského súdu spokojná nemá veľa možností ako napadnúť takéto rozhodnutie a zvrátiť pre ňu nepriaznivú právnu situáciu. Jednou z možností ako napadnúť rozhodnutie zaťažené procesnými vadami je žaloba na príslušný všeobecný súd o zrušenie tuzemského rozhodcovského rozsudku. „Vnútroštátne súdy v mieste rozhodcovského konania sú zvyčajne príslušné (a výlučne príslušné) na prerokovanie žalôb o zrušenie rozhodcovského

³ LEW, Julian, MISTELIS, Loukas, KROLL, Stefan: Comparative International Commercial Arbitration. Haag: Kluwer Law International, 2003. s. 7. ISBN 90-411-1568-4.

⁴ Zdroj: <https://www.justice.gov.sk/ministerstvo/analyticke-centrum/>.

rozsudku. Rozsah tohto súdneho prieskumu je primárne záležitosťou vnútroštátneho práva, ktoré sa v jednotlivých krajinách líši. V mnohých rozvinutých národných rozhodcovských úpravách je rozhodcovský rozsudok predmetom malého alebo žiadneho meritórneho (vecného) prieskumu a malého prieskumu procesného postupu rozhodcovského súdu. Naproti tomu niektoré štáty povoľujú relatívne rozsiahle preskúvanie rozhodcovského rozsudku vo veci samej a procesného postupu v arbitráži, či už explicitne alebo vo forme rozsiahleho prieskumu verejných záujmov.“⁵

Inštitút kontroly a preskúmateľnosti rozhodcovského rozsudku všeobecným súdom je determinovaný povinnosťou štátu zabezpečiť základné právo na súdnu ochranu. Žalobu na zrušenie tuzemského rozhodcovského rozsudku však môže podať účastník konania len z taxatívne vymedzených dôvodov⁶, ak:

a) účastník rozhodcovského konania preukáže, že

1. nemal spôsobilosť uzavrieť rozhodcovskú zmluvu, rozhodcovská zmluva nebola uzavretá v súlade s právnym poriadkom, podľa ktorého sa na základe dohody zmluvných strán mala rozhodcovská zmluva uzavrieť, alebo že takáto dohoda nebola uzavretá, podľa právneho poriadku Slovenskej republiky,
2. nebol riadne upovedomený o ustanovení rozhodcu, o rozhodcovskom konaní alebo že mu nebolo umožnené sa zúčastniť na rozhodcovskom konaní,
3. rozhodcovským rozsudkom sa rozhodol spor, pre ktorý nebola uzatvorená rozhodcovská zmluva, alebo ktorý nie je v medziach rozhodcovskej doložky, alebo že rozsudok prekračuje dosah dohovoru o rozhodcovi alebo dosah rozhodcovskej doložky; ak ale môžu byť časti rozhodcovského rozsudku vo veciach podrobených rozhodcovskému konaniu oddelené od častí rozsudku pojednávajúcich o veciach, ktoré nie sú mu podrobené, súd zruší rozhodcovský rozsudok len v dotknutej časti,
4. rozhodcovský súd nebol ustanovený, rozhodcovské konanie neprebiehalo spôsobom dohodnutým účastníkmi rozhodcovského konania alebo že sa táto dohoda neuzavrela, ak ustanovenie rozhodcovského súdu alebo priebeh rozhodcovského konania bol v rozpore s ustanoveniami tohto zákona, ak tieto skutočnosti mohli mať vplyv na rozhodnutie vo veci samej alebo

⁵ BORN, Gary: International Commercial Arbitration. Volume I. Alphen aan den Rijn: Kluwer Law International, 2009. s. 1680-1681. ISBN 978-90-411-2759-4.

⁶ § 40 ods. 1 ZRK.

b) súd zistí, že sú dôvody, pre ktoré by boli odopreté uznanie a výkon cudzieho rozhodcovského rozsudku aj bez návrhu účastníka podľa [§ 50 ods. 2](#) tohto zákona⁷.

Určítym filtrom prípustnosti žalôb a limitom uplatnenia dôvodov podľa § 40 ods. 1 písm. a) ZRK (vady, ktoré všeobecný súd skúma len na námietku strany) je skutočnosť, že uplatňovaný dôvod (vady) musel účastník rozhodcovského konania namietat už v konaní pred rozhodcovským súdom, inak všeobecný súd na takýto dôvod žaloby neprihliadne (§ 40 ods. 4 ZRK). Možno konštatovať, že vo vzťahu k týmto vadám platí zásada *vigilantibus iura scripta sunt*.⁸ Tiež sa žiada dodať, že procesné pochybenia rozhodcovského súdu v konaní budú môcť byť dôvodom pre zrušenie, len ak mohli mať vplyv na rozhodnutie o veci samej.

Nie je účelom tohto článku podrobnejšie rozoberať a komentovať vyššie uvedené dôvody prípustnosti žaloby na zrušenie rozhodcovského rozsudku. Preto sústredíme pozornosť len na otázky, pri ktorých vidíme priestor na vylepšenie právneho rámca ZRK.

V prvom rade je potrebné zdôrazniť, že z uvedeného taxatívneho výpočtu zákonných dôvodov vyplýva, že tuzemský rozhodcovský rozsudok možno na návrh účastníka zrušiť na všeobecnom súde len z „procesných“ dôvodov napr. pre nedostatky v subjektívnej alebo objektívnej arbitrabilite, procesnej nespravodlivosti spočívajúcej v porušení procesných pravidiel. Znamená to, že všeobecný súd v zásade nemôže rozhodcovský rozsudok podrobiť vecnému (meritórnemu) prieskumu.

Vynára sa však podstatná otázka, či môže byť rozsudok rozhodcovského súdu zrušený všeobecným súdom aj z dôvodu nedostatkov jeho odôvodnenia - nepreskúmateľnosť rozhodcovského rozsudku pre nezrozumiteľnosť alebo nedostatok dôvodov?

Odôvodnenie rozhodnutia je dôležitou náležitosťou každého rozhodovacieho aktu, či už vydaného orgánom verejnej moci alebo súkromným subjektom. ZRK pritom neupravuje žiadne obsahové náležitosti odôvodnenia rozhodcovského rozsudku. V rámci odôvodňovania rozhodcovského rozhodnutia je preto potrebné prihliadnuť

⁷ Ide o prípady, keď podľa právneho poriadku Slovenskej republiky nemožno predmet sporu riešiť v rozhodcovskom konaní alebo by jeho uznanie a výkon boli v rozpore s verejným poriadkom. Tieto dôvody skúma všeobecný súd *ex offio*.

⁸ „Najvyšší súd dáva do pozornosti zásadu, ktorá platila už v rímskom práve, podľa ktorej „*vigilantibus iura scripta sunt*“ t. j. „práva patria len bdelým“ (pozorným, ostražitým, opatrným, starostlivým), teda tým, ktorí sa aktívne zaujímajú o ochranu a výkon svojich práv a ktorí svoje procesné oprávnenia uplatňujú včas a s dostatočnou starostlivosťou a predvídavosťou. V slobodnej spoločnosti je totiž predovšetkým vecou nositeľov práv, aby svoje práva bránili a starali sa o ne, inak ich podcenením či zanedbaním môžu strácať svoje práva majetkové, osobné, satisfakčné a pod.. To platí obdobne aj o využívaní zákonných procesných ustanovení včítane využitia možnosti podania opravných prostriedkov.“ - rozsudok Najvyššieho súdu SR sp. zn. 5Sžf 65/2011 zo dňa 19.07.2012.

na ustanovenie § 51 ods. 3 ZRK, ktoré odkazuje na subsidiárne použitie Civilného sporového poriadku. Takúto právnu úpravu nepovažujeme za dostatočnú.⁹

V súvislosti s nedostatočným odôvodnením rozhodcovského rozsudku je potrebné uviesť, že nepreskúmateľnosť rozhodcovského rozsudku pre nezrozumiteľnosť alebo nedostatok dôvodov, nie je *expressis verbis* zákonným dôvodom na preskúmanie a zrušenie tuzemského rozhodcovského rozsudku všeobecným súdom.

Po tzv. „veľkej novele“ právnej úpravy ZRK od 01.01.2015 sa k možnosti preskúmania rozhodcovského rozsudku pre nedostatky v jeho odôvodnení najskôr priklonila v odbornej spisbe právna doktrína.¹⁰ Rozhodovacia prax súdov však bola v tejto otázke omnoho zdržanlivejšia a prvé rozhodnutia súdov naopak zaujali negatívny postoj.¹¹

Preskúmateľnosť odôvodnenia rozhodcovského rozsudku všeobecným súdom nakoniec odvodila aj judikatúra najvyšších súdnych autorít tak, že ju subsumovala pod zásadu rovnosti účastníkov rozhodcovského konania¹². Najvyšší súd SR k tomu konštatuje, že *„všeobecný súd rozhodujúci o žalobe o zrušenie tuzemského rozhodcovského rozsudku môže preskúmať odôvodnenie tohto rozsudku na základe vznesenej námietky jeho nepreskúmateľnosti len ako namietaný procesný postup rozhodcovského súdu, teda bez toho, aby sa zaoberal skutkovými zisteniami a právnymi*

⁹ V súlade s aktuálnymi právnymi závermi rozhodovacej praxe Najvyššieho súdu SR sme názoru, že systematika odôvodnenia rozhodcovského rozsudku by v zásade mala byť obdobná s odôvodnením rozsudku všeobecného súdu, avšak rozsah, podrobnosť a kvalita zdôvodnenia výroku rozhodcovského súdu môže byť vyjadrená podstatne jednoduchšie a koncíznejšie. Zároveň uvádzame, že pre vylúčenie pochybností a rôznych výkladov v aplikačnej praxi by preto bolo vhodné priamo do ZRK explicitne zakotviť minimálny štandard formálnych požiadaviek riadneho odôvodnenia rozhodcovského rozsudku.

Pozri bližšie: HNILICA, Radoslav: Rozhodcovský rozsudok v kontexte jeho osobitostí. In: Mílniky práva v stredoeurópskom priestore 2025. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025. s. 890. ISBN (e-verzia) 978-80-7160-758-8.

¹⁰ Pozri napr. GYÁRFÁŠ, Juraj: § 40 [Dôvody na podanie žaloby]. In: GYÁRFÁŠ, Juraj, ŠTEVČEK, Marek a kol. Zákon o rozhodcovskom konaní. 1. vydanie. Praha: C. H. Beck, 2016. s. 518-593. ISBN 978-80-7400-636-4.

¹¹ „... nedostatočné odôvodnenie rozhodcovského rozsudku – však nemožno považovať za porušenie zásady rovnosti účastníkov rozhodcovského konania v zmysle § 17 ZoRK“ - uznesenie Najvyššieho súdu SR sp. zn. 3Obdo/18/2018 z 12.06.2018.

„... argumenty žalobcu, ktoré sa obmedzili na jeho snahu preskúmať vec z hmotnoprávnej stránky a v ktorých namietal nedostatok odôvodnenia rozhodcovského rozsudku, sú vzhľadom na právnu úpravu obsiahnutú v ustanovení § 40 ZoRK neprípustné“ - rozsudok Krajského súdu v Bratislave sp. zn. 2Cob/119/2016 z 03.10.2017.

¹² Podľa § 17 ZRK „Účastníci rozhodcovského konania majú v rozhodcovskom konaní rovné postavenie. Každému účastníkovi rozhodcovského konania sa má poskytnúť rovnaká možnosť na uplatnenie jeho práv a na ich ochranu.“.

závermi rozhodcovského súdu z hľadiska vecnej správnosti rozhodnutia.“.¹³ Je však potrebné zdôrazniť, že porušenie zásady rovnosti účastníkov konania by muselo znamenať extrémny zásah do práva na spravodlivý proces, spočívajúci v úplnej absencii odôvodnenia rozhodcovského rozsudku, alebo celkom chýbajúcim zaoberaním sa pre vec zásadnými skutkovými a právnymi námietkami účastníka rozhodcovského konania.

Odôvodnenie písomného vyhotovenia rozhodcovského rozsudku je pritom potrebné považovať za súčasť procesného postupu rozhodcovského súdu v rozhodcovskom konaní. Nedostatočné odôvodnenie rozhodcovského rozsudku je tak procesnou vadou, ktorá môže založiť prípustnosť žaloby o zrušenie tuzemského rozhodcovského rozsudku v zmysle ustanovenia § 40 ods. 1 písm. a) bod 4 ZRK ako „*priebeh rozhodcovského konania v rozpore s ustanoveniami ZRK*“.

Možno konštatovať, že závery o prípustnosti preskúmania odôvodnenia rozhodcovského rozsudku majú legitímny právny základ. Absencia riadneho odôvodnenia rozhodcovského rozsudku je ako dôvod na jeho zrušenie priamo upravená napríklad v brazílskej právnej úprave rozhodcovského konania.¹⁴ Vzhľadom na skutočnosť, že ide o osobitný dôvod prípustnosti preskúmania rozhodcovského rozsudku iným orgánom - všeobecným súdom, zastávame názor, že tento dôvod preskúmateľnosti rozhodcovského rozsudku by bolo vhodné (po už realizovanej pozitívnej aprobácii rozhodovacou činnosťou Najvyššieho súdu SR i odbornou spisbou právnej doktríny) explicitne zakotviť aj do právnej úpravy ZRK.

Samotná žaloba smeruje proti druhému účastníkovi rozhodcovského konania a obsahuje rovnaké formálne náležitosti ako žaloba podľa § 132 Civilného sporového poriadku. Rozhodcovia nie sú účastníkmi konania o žalobe na zrušenie rozhodcovského rozsudku, nakoľko neboli ani účastníkmi právneho vzťahu, ktorý bol predmetom rozhodcovského konania.¹⁵ Je potrebné zdôrazniť, že po podaní žaloby na zrušenie rozhodcovského rozsudku na príslušnom súde, napadnutý rozhodcovský rozsudok zostáva právoplatný.

Práve pri prejednávaní žalôb na zrušenie rozhodcovského rozsudku civilným súdom sa prejavuje kontrolná funkcia všeobecných súdov vo vzťahu k rozhodcovským súdom. Z tohto dôvodu sú ustanovenia týkajúce sa zrušenia rozhodcovského rozsudku podľa § 42 ZRK kogentnými ustanoveniami, ktoré nemôžu účastníci v rozhodcovskej zmluve vylúčiť. V odbornej spisbe sa môžeme stretnúť tiež

¹³ Pozri bližšie: uznesenie Najvyššieho súdu SR sp. zn. sp. zn. 5Obdo/52/2021 z 27.04.2022 (publikované v zbierke stanovísk Najvyššieho súdu a rozhodnutí súdov Slovenskej republiky pod č. R 8/2023).

¹⁴ WALD, Arnaldo, BORJA, Ana: The New Brazilian Arbitration Law. In: Inter-American Law Review. University of Miami, Roč. 47, 2015, s. 21–52.

¹⁵ BĚLOHLÁVEK, A.: Zákon o rozhodčím řízení a o výkonu rozhodčích nálezů. Komentář. 1. vydání. Praha: C. H. Beck, 2004. s. 233. ISBN 80-7179-629-8.

s názorom, že strany rozhodcovskej zmluvy si nemôžu dohodnúť ani rozšírenie dôvodov na zrušenie rozhodcovského rozsudku nad rámec právnej úpravy stanovenej zákonom.¹⁶ Tiež sa žiada pre úplnosť dodať, že v medzinárodnej obchodnej arbitráži bola nastolená i otázka, či je možné vymáhať rozhodcovský nález podľa New Yorského dohovoru o uznaní a výkone cudzích rozhodcovských rozhodnutí z roku 1959 i napriek tomu, že nález bol zrušený vnútroštátnym súdom v mieste konania arbitráže.¹⁷

Všeobecný súd rozhodne o podanej žalobe tak, že buď žalobu zamietne (ak je nedôvodná) alebo napadnutý rozhodcovský rozsudok zruší, a to i v časti. Postup po zrušení rozhodcovského rozsudku následne závisí od dôvodu, z ktorého všeobecný súd rozhodcovský rozsudok zrušil¹⁸:

1. Ak všeobecný súd zruší rozhodcovský rozsudok z dôvodov neplatnosti rozhodcovskej zmluvy alebo nemožnosti riešiť predmet sporu v rozhodcovskom konaní pokračuje v konaní vo veci v rozsahu uvedenom v žalobe alebo vzájomnej žalobe všeobecný súd, pretože rozhodcovská zmluva sa stala bezpredmetnou. Teda vo veci samej rozhodne nakoniec práve všeobecný súd. Tu nastáva problém, pretože konkrétnu príslušnosť súdu na konanie vo veci samej platná právna úprava ZRK však už neurčuje. Na mieste je preto otázka, ktorý všeobecný súd bude po zrušení rozhodcovského rozsudku príslušný na meritórne rozhodnutie? Výkladom príslušných ustanovení CSP možno dospieť ku dvom rôznym riešeniam, v zmysle ktorých bude príslušným buď (i.) všeobecný súd, ktorý rozhodcovský rozsudok zrušil alebo (ii.) všeobecný súd, ktorý by bol príslušný na prejednanie veci samej. V prvom prípade by sme príslušnosť súdu, ktorý rozhodcovský rozsudok zrušil mohli vyvodiť gramatickým výkladom § 43 ods. 1 ZRK a na základe ustanovenia § 36 ods. 2 CSP normujúci zásadu *perpetuatio fori*. V zmysle uvedenej zásady platí, že ak v čase začatia konania

¹⁶ TAJAJ, Flutura – CINARI, Silvana: Annulment of Arbitral Awards Rendered in Albania: Trends and Challenges. In: Alternative Dispute Resolution in the Western Balkans. Trends and Challenges. European Union and its Neighbours in a Globalized World 20. Springer, 2025. s. 87–104. ISBN 978-3-031-76345-8 (eBook).

¹⁷ K tomu pozri napr.: PETROCHILLOS, Georgios: Enforcing awards annulled in their state of origin under the New York Convention. In: International & Comparative Law Quarterly, Roč. 48, č. 4 (1999), s. 856–888; SEYADI, Reyadh: Enforcement of arbitral awards annulled by the court of the seat. In: Arbitration, Roč. 84, č. 2 (2018), s. 128–141.

¹⁸ Podľa § 43 ods. 1 a 2 ZRK „(1) Ak súd zruší rozhodcovský rozsudok z dôvodov neplatnosti rozhodcovskej zmluvy alebo nemožnosti riešiť predmet sporu v rozhodcovskom konaní, pokračuje v konaní vo veci v rozsahu uvedenom v žalobe alebo v rozsahu uvedenom vo vzájomnej žalobe. (2) Ak súd zruší rozhodcovský rozsudok z iného dôvodu, ako je uvedený v odseku 1, rozhodcovská zmluva zostáva v platnosti. Rozhodcovia zúčastnení na zrušenom rozhodcovskom rozsudku sú z nového prerokovania a rozhodnutia veci vylúčení. Ak sa účastníci konania nedohodnú inak, budú noví rozhodcovia ustanovení podľa § 8.“.

o žalobe na zrušenie rozhodcovského rozsudku bol príslušný konkrétny všeobecný súd, ktorý rozhodcovský rozsudok zrušil, mala by jeho príslušnosť ďalej trvať aj na pokračovanie v konaní vo veci samej. Tento záver by však nezohľadňoval skutočnosť, že zrušením rozhodcovského rozsudku sa predmet konania o žalobe na zrušenie rozhodcovského rozsudku vyčerpal a konanie sa už skončilo právoplatným rozhodnutím. Dotknutá právna úprava § 43 ZRK sa teda týka pokračovania (pôvodne rozhodcovského konania) o žalobe vo veci samej, a nie pokračovania konania o zrušení rozhodcovského rozsudku. Príslušnosť na pokračovanie vo veci samej súdu, ktorý zrušil rozhodcovský rozsudok, by preto zrejme nemohla procesne obstáť. Ako druhá alternatíva príslušnosti prejednať vec samu sa javí súd, ktorý by bol príslušný na prejednanie veci samej nebyť rozhodcovskej zmluvy. V takom prípade by jeho príslušnosť bola založená podľa § 13 CSP „*Na konanie v prvej inštancii je miestne príslušný všeobecný súd žalovaného, ak nie je ustanovené inak.*“. Treba tiež poznamenať, že i v prípade pokračujúceho konania podľa § 43 ods. 1 ZRK platí právna úprava kauzálnej príslušnosti obsiahnutá v § 22 a nasl. CSP, ktorú by bolo potrebné zohľadniť podľa povahy nároku. V súlade s recentnou rozhodovacou praxou¹⁹ sme názoru, že na pokračovanie v konaní vo veci samej po zrušení rozhodcovského rozsudku bude súd príslušný podľa CSP, ktorý by vec samu prejednával a rozhodoval, nebyť rozhodcovskej zmluvy. Aj v tomto ohľade by preto bolo potrebné precizovať platnú právnu úpravu ZRK.

2. Ak všeobecný súd zruší rozhodcovský rozsudok z iných dôvodov, ako sú uvedené v predchádzajúcom ods. 1, rozhodcovská zmluva zostáva naďalej v platnosti. Rozhodcovia zúčastnení na zrušenom rozsudku sú z nového prerokovania a rozhodnutia veci vylúčení. Ak sa účastníci nedohodnú inak, budú noví rozhodcovia ustanovení podľa rovnakých zásad ako pôvodní rozhodcovia. V tomto prípade vo veci samej rozhodne opäť rozhodcovský súd, ale v inom zložení. V tejto súvislosti je vhodné upozorniť na ďalší nedostatok platnej právnej úpravy ZRK, ktorá v intenciách tohto procesného postupu opomenula záväzne upraviť problematiku postúpenia veci (spisu) novým rozhodcom. V praxi tak môže nastať situácia síce výnimočná, ale so závažnými dôsledkami, keď po zrušení rozsudku vylúčený rozhodca (rozhodcovia) nepostúpia vec novému

¹⁹ „Ustanovenie § 43 ods. 1 Zákona o rozhodcovskom konaní nezakladá osobitnú príslušnosť súdu na meritórne konanie nasledujúce po zrušení (časti) rozhodcovského rozsudku. Príslušným bude súd podľa Civilného sporového poriadku, ktorý by vec samu (spor) riešil, nebyť rozhodcovskej zmluvy. Pre príslušnosť súdu na rozhodovanie o veci samej (spore) po právoplatnosti rozsudku o žalobe o zrušenie (časti) rozhodcovského rozsudku, je určujúca povaha nároku, pôvodne uplatneného žalobou (vzájomnou žalobou) na rozhodcovskom súde, ktorý je predmetom konania pokračujúceho po zrušení (časti) rozhodcovského rozsudku.“ – uznesenie Najvyššieho súdu SR sp. zn. 5Ndob/30/2024 z 27. novembra 2024.

rozhodcovi (rozhodcom). Efektívnym riešením by bolo jednoduché zakomponovanie tejto povinnosti vylúčených rozhodcov do ZRK.

Digitalizácia rozhodcovského konania

Vo všeobecnosti možno konštatovať, že nositeľom inovácií a pokroku vo všetkých sférach života je zvyčajne súkromný sektor. Je zrejme paradoxom, že práve v rozhodcovskom konaní ako konaní pred súkromným orgánom, sa tento progres neprejavuje v plnej miere. Samozrejme je treba rozlišovať situáciu pri *ad hoc* arbitráži, kedy ide o príležitostné vykonávanie právomoci rozhodcami a pri inštitucionálnej arbitráži, kedy sú stále rozhodcovské súdy predstaviteľmi tradičného rozhodovania sporov a sú zvyčajne späté so zázemím a podporou príslušnej komory (zvyčajne obchodnej, resp. stavovskej).

V rozhodcovskom konaní nie sú zavedené elektronické formuláre na realizovanie podaní, elektronické doručovanie do dátových schránok, elektronický súdny spis a ani možnosť vydania rozsudku v elektronickej podobe. Výnimočne sa možno stretnúť s dištančným pojednávaním prostredníctvom prostriedkov komunikačnej technológie. Na tomto mieste treba tiež poznamenať, že digitalizácia rozhodcovského konania v našom domácom prostredí výrazne zaostáva za situáciou v súdnom konaní pred všeobecnými súdmi. V rokovacích poriadkoch etablovaných rozhodcovských súdov napr. Rozhodcovského súdu SOPK²⁰, Rozhodcovského súdu SAK²¹ je upravená iba ústna a písomná forma konania, pričom absentuje napr. úprava on-line konania, kde celý proces prejednávania a rozhodovania súdnej veci prebieha v elektronickom prostredí.

Naviac, podľa platnej právnej úpravy ZRK sa rozhodcovský rozsudok vyhotovuje písomne v listinnej forme²², a teda musí byť vždy vyhotovený výhradne ako fyzická listina. Takáto požiadavka pritom priamo nevyplýva ani z modelového zákona UNCITRAL Model Law on International Commercial Arbitration v znení zmeny z roku 2006 a ani z Dohovoru o uznaní a výkone cudzích rozhodcovských rozhodnutí tzv. Newyorský dohovor, publikovaný vo vyhláske ministra zahraničných vecí č. 74/1959 Zb. Určitou osobitosťou právnej úpravy rozhodcovského konania preto je, že na rozdiel od rozsudku všeobecného súdu, nemôže byť rozhodcovský rozsudok vyhotovený v elektronickej podobe. Takáto úprava je zrejme reliktom snahy o obmedzenie negatívnych dôsledkov spojených s umožnením vzniku veľkého množstva stálych rozhodcovských súdov, ktoré pôvodne mohla zriaďovať akákoľvek právnická osoba. Táto koncepcia vytvorila podhubie pre zneužitie rozhodcovského

²⁰ https://www.sopk.sk/rs/rokovaci_poriadok/.

²¹ https://info.sak.sk/sud/rokovaci_poriadok/.

²² § 34 ods. 1 ZRK.

konania na nekalé praktiky²³, pričom nedostatočná kontrola nad nimi spôsobovala, že konanie mnohých sa výrazne odchyľovalo od profesionálnych a etických štandardov zavedených medzinárodných inštitúcií²⁴. Je však potrebné pre úplnosť dodať, že v prípade vydania rozhodcovského rozhodnutia v elektronickej podobe do cudziny by mohol vzniknúť problém s uznaním a vykonateľnosťou rozsudku podľa Newyorského dohovoru pri jeho vymáhaní v cudzine.

V súčasnej dobe je elektronický výkon spravodlivosti v oblasti rozhodcovského konania zrejme ešte len otázkou budúcnosti. Primárnou úlohou bude vytvorenie zodpovedajúceho právneho rámca a premostenie s platnou legislatívou, ktorá bude umožňovať bezpečné a spoľahlivé rozhodovanie sporov rozhodcovskými orgánmi v elektronickej podobe. Rozhodcovské konanie tak v našich domácich podmienkach ešte len stojí pred výzvou zásadnejšej digitalizácie rozhodovacích procesov smerom k ešte rýchlejšiemu a efektívnejšiemu rozhodovaniu.

Záver

Rozhodcovské konanie ako etablovaná forma alternatívneho riešenia sporov predstavuje významný prvok právneho systému, ktorého účelom je zabezpečiť efektívne a flexibilné rozhodovanie sporových agend. Zároveň však nemožno opomenúť potrebu primeranej kontroly nad činnosťou rozhodcovských súdov, ktorej podstatným nástrojom je žaloba na zrušenie rozhodcovského rozsudku. Analýza platnej právnej úpravy ZRK poukazuje na skutočnosť, že súčasný rámec umožňuje zásah všeobecných súdov iba z taxatívne vymedzených procesných dôvodov, čím je vylúčený meritórny prieskum veci. Tento prístup chráni zásadu konečnosti rozhodcovských rozsudkov, no zároveň vyvoláva otázky o dostatočnej ochrane práv účastníkov, najmä v prípadoch, keď absentuje riadne a presvedčivé odôvodnenie rozhodnutia.

Osobitne sa ukazuje potreba legislatívneho spresnenia povinností rozhodcov pri vyhotovení písomného odôvodnenia a výslovného zakotvenia možnosti jeho preskúmania v konaní o žalobe na zrušenie rozhodcovského rozsudku do právnej úpravy ZRK. Rovnako tak vyvstáva požiadavka doplnenia pravidiel o príslušnosti všeobecných súdov po zrušení rozhodcovského rozsudku a explicitnej úpravy procesných následkov postúpenia veci novým rozhodcom. Tieto aspekty majú

²³ Pozri bližšie: KUBÍČEK, Pavol: Niekoľko poznámok k vývoju právnej úpravy rozhodcovského konania v Slovenskej republike. In: Právo, obchod, ekonomika. Košice: Univerzita P. J. Šafárika v Košiciach, 2024. s. 251. ISBN 978-80-574-0389-0.

²⁴ COLE, Tony, BANTEKAS, Ilias, FERRETTI, Federico, RIEFA, Christine, WARWAS, Barbara, ORTOLANI, Pietro: Legal Instruments and Practice of Arbitration in the EU. In: Study for the JURI Committee. Brusel: European Parliament, 2014. s. 163. ISBN 978-92-8236254-9.

zásadný význam pre posilnenie právnej istoty účastníkov a predvídateľnosti procesných postupov.

Nezanedbateľným rozmerom skúmanej problematiky je aj absencia systematickej digitalizácie rozhodcovského konania, ktorá výrazne zaostáva za všeobecným súdnictvom. Vytvorenie právneho rámca umožňujúceho využívanie elektronických podaní, elektronického spisu a vydávanie rozhodnutí v elektronickej forme predstavuje nevyhnutný krok k zvýšeniu efektívnosti a konkurencieschopnosti arbitráže v prostredí moderného práva.

Zhrnutím možno konštatovať, že žaloba na zrušenie rozhodcovského rozsudku plní nezastupiteľnú kontrolnú funkciu, no platná právna úprava vykazuje nedostatky, ktoré si vyžadujú legislatívnu reflexiu. Ich odstránenie by prispelo k rovnováhe medzi rýchlosťou a efektívnosťou rozhodcovského konania na jednej strane a ochranou základných procesných práv účastníkov na strane druhej.

Zoznam použitej literatúry

1. BĚLOHLÁVEK, A.: Zákon o rozhodčím řízení a o výkonu rozhodčích nálezů. Komentář. 1. vydání. Praha: C. H. Beck, 2004. 701 s. ISBN 80-7179-629-8.
2. BORN, G.: International Commercial Arbitration. Volume I. Alphen aan den Rijn: Kluwer Law International, 2009. s. 3303. ISBN 978-90-411-2759-4.
3. COLE, T. – BANTEKAS, I. – FERRETTI, F. – RIEFA, C. – WARWAS, B. – ORTOLANI, P.: Legal Instruments and Practice of Arbitration in the EU. In: Study for the JURI Committee. Brusel: European Parliament, 2014. s. 308. ISBN 978-92-8236254-9.
4. GYÁRFÁŠ, J., ŠTEVČEK, M. a kol.: Zákon o rozhodcovskom konaní. 1. vydanie. Praha: C. H. Beck, 2016. 744 s. ISBN 978-80-7400-636-4.
5. HNILICA, R.: Rozhodcovský rozsudok v kontexte jeho osobitostí. In: Míľniky práva v stredoeurópskom priestore 2025. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025. s. 885-893. ISBN (e-verzia) 978-80-7160-758-8.
6. HUČKOVÁ, R., TREŠČÁKOVÁ, D.: Zákon o rozhodcovskom konaní. Komentár. Bratislava: Wolters Kluwer SR s.r.o., 2018. 192 s. ISBN 978-80-8168-922-2.
7. KUBÍČEK, P.: Niekoľko poznámok k vývoju právnej úpravy rozhodcovského konania v Slovenskej republike. In: Právo, obchod, ekonomika. Košice: Univerzita P. J. Šafárika v Košiciach, 2024. s. 248-254. ISBN 978-80-574-0389-0.
8. LEW, J. – MISTELIS, L. – KROLL, S.: Comparative International Commercial Arbitration. Haag: Kluwer Law International, 2003. s. 953. ISBN 90-411-1568-4.
9. PETROCHILOS, G.: Enforcing awards annulled in their state of origin under the New York Convention. In: International & Comparative Law Quarterly, Roč. 48, č. 4 (1999), s. 856–888.

10. SEYADI, R.: Enforcement of arbitral awards annulled by the court of the seat. In: Arbitration, Roč. 84, č. 2 (2018), s. 128–141.
11. TAJAJ, F. – CINARI, S.: Annulment of Arbitral Awards Rendered in Albania: Trends and Challenges. In: Alternative Dispute Resolution in the Western Balkans. Trends and Challenges. European Union and its Neighbours in a Globalized World 20. Springer, 2025. s. 87–104. ISBN 978-3-031-76345-8 (eBook).
12. WALD, Arnoldo, BORJA, Ana: The New Brazilian Arbitration Law. In: Inter-American Law Review. University of Miami, Roč. 47, 2015, s. 21–52.
13. Zákona č. 244/2002 Z. z. o rozhodcovskom konaní v znení neskorších predpisov.
14. Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov.
15. <https://www.justice.gov.sk/ministerstvo/analyticke-centrum/>.
16. rozsudok Najvyššieho súdu SR sp. zn. 5Sžf 65/2011 zo dňa 19.07.2012.
17. uznesenie Najvyššieho súdu SR sp. zn. 3Obdo/18/2018 z 12.06.2018.
18. rozsudok Krajského súdu v Bratislave sp. zn. 2Cob/119/2016 z 03.10.2017.
19. uznesenie Najvyššieho súdu SR sp. zn. sp. zn. 5Obdo/52/2021 z 27.04.2022.
20. uznesenie Najvyššieho súdu SR sp. zn. 5Ndob/30/2024 z 27.11.2024.

Kontaktné údaje

JUDr. Radoslav Hnilica, PhD.

radoslav.hnilica@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

NAJLEPŠÍ ZÁUJEM DIEŤAŤA A UMEĽÁ INTELIGENCIA: KAM MÔŽE VIESŤ OPTIMALIZÁCIA V RODINNOM PRÁVE?

THE BEST INTERESTS OF THE CHILD AND ARTIFICIAL INTELLIGENCE: WHERE CAN OPTIMIZATION LEAD IN FAMILY LAW?

Petronela Luprichová Cvengrošová¹

Abstrakt: Príspevok analyzuje princíp najlepšieho záujmu dieťaťa v kontexte narastajúceho využívania umelej inteligencie v rodinnom práve. Vychádza z medzinárodných dokumentov, slovenského právneho rámca a psychologických poznatkov o rozhodovaní. Osobitná pozornosť je venovaná heuristikám, ktoré ovplyvňujú ľudské rozhodovanie, a možnostiam ich kalibrácie pomocou algoritmických nástrojov. Prípadová štúdia z Allegheny County (USA) ilustruje výhody aj riziká prediktívnych modelov v ochrane detí. Článok navrhuje multidisciplinárny model kalibrácie rozhodovania, ktorý kombinuje právne, psychologické a technologické aspekty s cieľom chrániť dôstojnosť a individuálne potreby dieťaťa. Diskusia prináša odporúčania pre legislatívu, odbornú prax a výskum.

Kľúčové slová: nejlepší zájem dieťaťa, umelá inteligencia, rodinné právo, AFST

Abstract: The article analyzes the principle of the best interests of the child in the context of the increasing use of artificial intelligence in family law. It is based on international documents, the Slovak legal framework and psychological knowledge about decision-making. Special attention is paid to heuristics that influence human decision-making and the possibilities of their calibration using algorithmic tools. A case study from Allegheny County (USA) illustrates both the benefits and risks of predictive models in child protection. The article proposes a multidisciplinary model of decision-making calibration that combines legal, psychological and technological aspects in order to protect the dignity and individual needs of the child. The discussion brings recommendations for legislation, professional practice and research.

Key words: best interest of the child, artificial intelligence, family law, AFST

¹ Univerzita Komenského v Bratislave, Právnická fakulta

Úvod

Princíp najlepšieho záujmu dieťaťa predstavuje základný pilier rodinného práva, ktorý sa uplatňuje pri všetkých rozhodnutiach týkajúcich sa maloletých. Tento princíp je zakotvený v medzinárodných dokumentoch, národných právnych predpisoch a judikatúre, pričom jeho aplikácia si vyžaduje komplexné posúdenie individuálnych potrieb dieťaťa, jeho vzťahového prostredia, emocionálnej stability, ako aj schopnosti rodičov zabezpečiť jeho harmonický vývin. V posledných rokoch sa do rozhodovacích procesov v rodinnom práve začína dostávať umelá inteligencia (AI), ktorá má potenciál zefektívniť administratívne úkony, podporiť konzistentnosť rozhodnutí a predikovať rizikové situácie. Napriek týmto výhodám sa objavujú zásadné otázky týkajúce sa etiky, transparentnosti, právnej zodpovednosti a rizika dehumanizácie rozhodovania. AI totiž operuje na základe historických dát, ktoré môžu obsahovať systémové nerovnosti, predsudky alebo neúplné informácie. Cieľom tohto článku je analyzovať, kam môže viesť optimalizácia rozhodovania v rodinnom práve pomocou AI, aké riziká prináša algoritmické rozhodovanie, ako sa prejavujú heuristiky v ľudskom rozhodovaní, a aké korekčné mechanizmy je možné zaviesť. Osobitná pozornosť bude venovaná prípadovej štúdii z okresu Allegheny County v USA, kde bol zavedený prediktívny algoritmus na identifikáciu rizikových rodín. Na základe tejto analýzy bude navrhnutý model kalibrácie rozhodovania, ktorý kombinuje právne, psychologické a technologické aspekty s cieľom chrániť najlepší záujem dieťaťa.

Právny rámec najlepšieho záujmu dieťaťa

Najlepší záujem dieťaťa je zakotvený v článku 3 ods. 1 Dohovoru o právach dieťaťa (OSN, 1989), ktorý stanovuje, že *„záujem dieťaťa musí byť prvoradým hľadiskom pri akýchkoľvek postupoch týkajúcich sa detí, či už vykonávaných súkromnými zariadeniami sociálnej starostlivosti, súdmi, správnymi alebo zákonodarnými orgánmi“*. Tento princíp bol ďalej rozpracovaný vo Všeobecnom komentári č. 14 Výboru OSN pre práva dieťaťa (2013), ktorý definuje najlepší záujem ako trojrozmerný koncept: hmotnoprávny princíp, výkladové pravidlo a procesné právo. Komentár zdôrazňuje potrebu individuálneho posúdenia každého prípadu, zohľadnenie názoru dieťaťa, jeho identity, rodinného prostredia, zdravia, bezpečnosti a stability.

V slovenskom právnom poriadku je princíp najlepšieho záujmu dieťaťa zakotvený v Zákone č. 36/2005 Z. z. o rodine, konkrétne v čl. 5, ktorý stanovuje, že *„záujem maloletého dieťaťa je prvoradým hľadiskom vo všetkých veciach, ktoré sa ho týkajú“*. Tento princíp sa uplatňuje pri rozhodovaní o zverení dieťaťa do starostlivosti, výživnom, styku s rodičmi, ako aj pri ochrane pred násilím, zanedbávaním či zneužívaním. Ústavný súd SR vo viacerých nálezochoch zdôraznil, že najlepší záujem dieťaťa nie je abstraktný pojem, ale konkrétny právny štandard, ktorý musí byť

posudzovaný individuálne a ide o samovykonateľnú právnu normu. Aplikácii vo vnútroštátnom práve najlepšie vyhovujú také normy medzinárodného práva, ktorých znenie, účel a samotný obsah umožňuje, aby priamo zaväzovali štátne orgány, fyzické a právnické osoby bez toho, aby bol k tomu potrebný aplikačný zásah prostredníctvom normy práva vnútroštátneho. Norma medzinárodného práva, spĺňajúca uvedené predpoklady, sa nazýva „**samovykonateľnou**“ (**self-executing**) **normou**.² Podľa nášho názoru, znenie článku 3 ods. 1 Dohovoru o právach dieťaťa spĺňa všetky uvedené atribúty a je preto vhodná na priamu aplikáciu. K rovnakému stanovisku dospel aj Ústavný súd ČR, ktorý vo svojom náleze uviedol: „ V čl. 3 ods. 1 Dohovor o právach dieťaťa ustanovuje, že záujem dieťaťa musí byť prvoradým hľadiskom pri akejkoľvek činnosti týkajúcej sa detí... Toto ustanovenie má povahu normy vnútroštátne bezprostredne použiteľnej („self – executing“). Uvedená norma je na priame použitie spôsobilá vzhľadom na svoju dikciu (...záujem dieťaťa...pri akejkoľvek činnosti), ktorá je dostatočne a do takej miery jasná, aby povinné subjekty, ktorým je adresovaná (vnútroštátne subjekty), boli schopné zodpovedajúcim spôsobom upraviť svoje správanie.“³ Stotožňujeme sa s názorom, že najlepší záujem dieťaťa **musí byť posudzovaný s ohľadom na ďalšie práva dieťaťa**, ako napr. na právo dieťaťa na rodinný a súkromný život a zákaz diskriminácie, ktoré mu poskytuje Dohovor o ochrane ľudských práv a základných slobôd v čl. 8 a 14, v nadväznosti na právo na starostlivosť oboch rodičov, garantované čl. 7 a 9 Dohovoru o právach dieťaťa a rovnako participačného práva dieťaťa, vyplývajúceho z čl. 12 Dohovoru o právach dieťaťa.⁴

Definícia a typológia AI v právnom kontexte

Umelá inteligencia (AI) v právnom prostredí označuje systémy schopné analyzovať dáta, predikovať výsledky, navrhovať rozhodnutia alebo automatizovať procesy, ktoré si tradične vyžadovali ľudský úsudok. V rodinnom práve sa AI najčastejšie využíva v týchto oblastiach:

- **Výpočet výživného:** algoritmy, ktoré na základe príjmov, výdavkov a počtu detí navrhujú výšku výživného.
- **Online mediácia:** digitálne platformy, ktoré pomáhajú rodičom dosiahnuť dohodu bez zásahu súdu.
- **Prediktívne modely:** systémy, ktoré identifikujú rizikové rodiny na základe historických dát.

² VEČEŘA, M. a kol.: Teória práva. 2. vyd. Bratislava: Euro Kódex, 2008. 146 s.

³ Nález Ústavného súdu ČR z 9. Apríla 1997, sp. zn. PL. ÚS 31/96

⁴ KRÁLÍČKOVÁ, Z.: Lidskoprávní dimenze českého rodinného práva. Brno: Masarykova univerzita, 2009.

- **Podpora rozhodovania:** nástroje, ktoré poskytujú odporúčania sudcom alebo pracovníkom sociálnych služieb.

Tieto aplikácie sa líšia mierou autonómie – od čisto podporných nástrojov až po systémy, ktoré generujú návrhy rozhodnutí.

Výhody využitia AI v rodinnom práve

- **Efektivita:** zrýchlenie administratívnych procesov, zníženie zaťaženia súdov
- **Konzistentnosť:** algoritmy môžu zabezpečiť rovnaké rozhodovanie pri rovnakých vstupoch
- **Predikcia rizika:** identifikácia ohrozených detí na základe dátových vzorcov
- **Podpora odborníkov:** AI môže slúžiť ako nástroj na overenie hypotéz, návrh riešení alebo kontrolu rozhodnutí⁵

Kritika a riziká AI v rodinnom práve

- **Netransparentnosť algoritmov:** mnohé AI systémy fungujú ako „čierne skrinky“, ktorých logika nie je zrozumiteľná ani kontrolovateľná
- **Diskriminácia:** algoritmy môžu reprodukovать systémové nerovnosti, ak sú trénované na historických dátach
- **Absencia kontextu:** AI nedokáže zohľadniť emocionálne väzby, dôstojnosť, individuálne potreby dieťaťa
- **Zodpovednosť:** nie je jasné, kto nesie právnu zodpovednosť za rozhodnutie generované algoritmom
- **Etické dilemy:** napr. či je prípustné, aby algoritmus rozhodoval o odobratí dieťaťa z rodiny⁶

Prípadová štúdia – Allegheny county (USA)

Allegheny County v štáte Pennsylvania sa stal medzinárodne známym vďaka implementácii prediktívneho algoritmu **Allegheny Family Screening Tool (AFST)**, ktorý bol zavedený v roku 2016 ako podporný nástroj pre pracovníkov call centra v oblasti ochrany detí. Cieľom algoritmu bolo pomôcť rozhodnúť, či má byť rodina vyšetrovaná kvôli podozreniu na zanedbávanie alebo týranie dieťaťa. AFST funguje na základe analýzy historických dát z oddelení sociálnych služieb, zdravotníctva, školstva, trestných registrov a ďalších verejných databáz. Na základe týchto údajov generuje rizikové skóre, ktoré má pomôcť pracovníkom identifikovať prípady, kde je vyššia pravdepodobnosť zásahu do rodičovských práv a povinností. Dôležité je

⁵ COUTURE, R.J.: The impact of artificial intelligence on law firms' business models. Harvard Law School Center on the legal Profession, 2025. [online] dostupné: <https://clp.law.harvard.edu/knowledge-hub/insights/the-impact-of-artificial-intelligence-on-law-law-firms-business-models/>

⁶ WILLIAMSON, J.: "The rise of AI in legal practice: Opportunities, challenges, & ethical considerations". In: Colorado Technology Law Journal, 2025. [online] dostupné: <https://ctlj.colorado.edu/?p=1297>

zdôrazniť, že algoritmus nerozhoduje autonómne – slúži ako odporúčanie, pričom konečné rozhodnutie robí človek.⁷

Podľa správy zverejnenej 31. mája 2024 na portáli Allegheny Analytics, AFST priniesol niekoľko pozitívnych výsledkov:

- **Zvýšenie presnosti rozhodovania:** algoritmus pomohol identifikovať prípady, ktoré by inak neboli vyšetrené, čím sa znížilo riziko zanedbania.
- **Zníženie rasovej nerovnosti:**
 - Rozdiel v miere vyšetrovania medzi čiernymi a bielymi rodinami sa znížil o 83 % pri najrizikovejších prípadoch
 - Rozdiel v miere odobratia detí sa znížil o 73 %.
- **Podpora odborníkov:** pracovníci vnímali algoritmus ako užitočný nástroj, ktorý im pomáha pri rozhodovaní, najmä v nejasných prípadoch⁸

Tieto výsledky môžu naznačovať, že správne kalibrovaný algoritmus môže prispieť k spravodlivejšiemu rozhodovaniu, ak je používaný ako doplnok, nie náhrada ľudského úsudku.

Kritika a zásah Ministerstva spravodlivosti USA

Napriek pozitívnym výsledkom sa však AFST stal predmetom vyšetrovania Ministerstva spravodlivosti USA, ktoré v roku 2023 začalo preverovať, či algoritmus neporušuje občianske práva zraniteľných skupín. Konkrétne sa objavili podozrenia, že systém diskriminuje rodiny s mentálnym postihnutím, psychickými poruchami alebo nízkym socioekonomickým statusom.

Kritika AFST vychádza najmä z týchto oblastí:

- **Netransparentnosť algoritmu:** rodiny nevedia, na základe akých dát boli označené ako rizikové
- **Predsudky a historická nespravodlivosť:** algoritmus bol trénovaný na historických dátach, ktoré odrážajú systémové chyby – napr. vyššiu mieru zásahov voči chudobným alebo menšinám
- **Absencia právneho rámca:** neexistuje jasná legislatíva, ktorá by upravovala používanie AI v ochrane detí
- **Etické dilemy:** otázka, či je prípustné, aby algoritmus ovplyvňoval rozhodnutia o zásahu do rodinného života
- **Riziko na základe asociácie:** nástroj zaraďuje rodiny do skupín a na základe údajov o jednom členovi rodiny priraduje vysoké rizikové skóre celej rodine

⁷ Allegheny County. Evaluation Findings on the Use of Predictive Risk Model in Child Welfare, 2024. [online] Dostupné na: [https:// Allegheny Family Screening Tool - Allegheny County, PA](https://AlleghenyFamilyScreeningTool-AlleghenyCounty,PA)

⁸ Summarizing Recent Research on Predictive Risk Models in Child Welfare, 2024. [online] dostupné: <24-ACDHS-04-Predictive-Risk-Algorithms.pdf>

Dopady na zraniteľné skupiny

Zraniteľné skupiny – najmä rodiny s mentálnym postihnutím, psychickými problémami, nízkym príjmom alebo inou marginalizáciou sú najviac ohrozené nesprávnym označením algoritmom. Takéto označenie má vážne dôsledky medzi ktoré patrí stres a stigmatizácia, zásah do práva na rodinný život, zníženie dôvery voči inštitúciám a najzávažnejšie je riziko odobratia dieťaťa bez dostatočného dôvodu. Prípady Allegheny County ukazujú, že AI môže byť užitočným nástrojom, ak je správne navrhnutá, transparentná a pod ľudským dohľadom. Zároveň však upozorňuje na potrebu právneho a etického rámca, ktorý zabezpečí ochranu práv detí a rodín. Na základe toho sa domnievame, že AI nesmie rozhodovať autonómne o zásahu do rodiny, algoritmus musí byť vysvetliteľný a kontrolovateľný, zraniteľné skupiny musia byť chránené pred diskrimináciou a musí existovať možnosť korekcie rozhodnutia. Každé rozhodnutie týkajúce sa dieťaťa musí rešpektovať jeho dôstojnosť, autonómiu a právo na individuálne posúdenie. Rozhodovanie pomocou AI prináša riziko, že dôstojnosť dieťaťa bude redukovaná na dátové skóre. Ak algoritmus vyhodnotí situáciu bez zohľadnenia emocionálneho vývinu, vzťahových väzieb či názoru dieťaťa, môže dôjsť k zásahu, ktorý je formálne správny, ale ľudsky neprimeraný. Ďalším rizikom je rozhodne možnosť dehumanizácie, ktorá môže nastať vtedy, keď sa rozhodovanie stane technickým procesom bez zohľadnenia ľudského kontextu. V rodinnom práve je to obzvlášť nebezpečné, pretože ide o najintímnejšie aspekty života – vzťahy, starostlivosť, lásku, bezpečie. AI systémy, ktoré operujú na základe štatistiky, nemajú schopnosť empatie, intuície ani morálneho úsudku. Ich výstupy môžu byť presné, ale bezcitné. Napríklad algoritmus môže odporučiť odobratie dieťaťa na základe rizikového skóre, hoci rodič prejavuje úprimnú snahu o zlepšenie podmienok. Dehumanizácia sa však môže prejaviť aj v tom, že odborníci začnú slepo dôverovať algoritmu a prestanú klásť otázky, reflektovať a pochybovať. To vedie k strate profesionálnej zodpovednosti. Pri rozhodovaní v rodinnoprávnej agende je zároveň dôležitá aj potreba empatie a emocionálnej citlivosti, ktoré môžeme charakterizovať ako schopnosť vcítiť sa do situácie druhého človeka, pochopiť jeho pocity, potreby a motivácie. V rozhodovaní o deťoch je empatia nevyhnutná – umožňuje odborníkovi vnímať nielen fakty, ale aj emocionálnu realitu. Mnohé výskumy ukazujú, že deti potrebujú stabilné vzťahy, pocit bezpečia a predvídateľnosti. Rozhodnutia, ktoré ignorujú tieto potreby, môžu viesť k traumatizácii, narušeniu vývinu a strate dôvery. AI nemá schopnosť empatie. Preto musí byť vždy doplnená ľudským pohľadom, ktorý zohľadňuje emocionálny vývin dieťaťa, jeho vzťahové väzby a subjektívne prežívanie.

Algoritmus umelej inteligencie vs. ľudský algoritmus

Na základe získaných informácií sme dospeli k záveru, že algoritmus umelej inteligencie nie je schopný cítiť a využívať empatiu pri posudzovaní najlepšieho záujmu dieťaťa a z toho dôvodu by nemal byť v súčasnosti používaný bez tzv. ľudského dozoru. Položili sme si však aj otázku, aký je rozdiel medzi algoritmom umelej inteligencie a ľudským algoritmom, nakoľko ľudia, podľa nášho názoru, pri svojom rozhodovaní tiež používajú algoritmy a dospeli sme k záveru, že tieto algoritmy sú pomerne podobné s tým rozdielom, že ľudský algoritmus je menej transparentný a je veľmi ťažké určiť, či nie je ovplyvňovaný heuristikami (mentálnymi skratkami), predsudkami a naučenými vzorcami správania. Aj ľudský algoritmus preto často potrebuje istú kalibráciu, ak chceme zabezpečiť, že rozhodnutie je v najlepšom záujme dieťaťa. Možno práve v tejto oblasti môže byť budúcnosť využívania umelej inteligencie v rodinnoprávnej agende.

Model kalibrácie rozhodovania

Rozhodovanie v rodinnom práve je komplexný proces, ktorý zahŕňa právne, psychologické, sociálne a etické dimenzie. Či už ide o rozhodnutie sudcu, posudok psychológa alebo výstup algoritmu, každý krok môže byť ovplyvnený heuristikami, predsudkami alebo neúplnými informáciami. Kalibrácia predstavuje systematický spôsob, ako tieto rozhodnutia korigovať, overiť a zlepšiť ich kvalitu. Kalibrácia je bežná v technických oblastiach (napr. meranie, strojové učenie), no v právnom kontexte sa uplatňuje menej často. V rodinnom práve by mala slúžiť na zabezpečenie toho, že rozhodnutie je v súlade s najlepším záujmom dieťaťa, nie s rutinou, predsudkom alebo technickým výstupom.

Na základe našich zistení navrhujeme šesťfázový model kalibrácie, ktorý môže byť aplikovaný na ľudské aj algoritmické rozhodovanie:

1. Zber údajov

- Získanie relevantných informácií o dieťati, rodičoch, vzťahoch, zdravotnom stave, školskom prostredí, názore dieťaťa
- V prípade AI: vstupné dáta musia byť aktuálne, úplné a eticky získané

2. Predbežné rozhodnutie

- Odborník (sudca, psychológ, sociálny pracovník,...) alebo algoritmus navrhne riešenie na základe dostupných údajov
- Toto rozhodnutie je považované za hypotézu, nie finálny verdikt

3. Kalibračná kontrola

- Overenie rozhodnutia pomocou štandardizovaných nástrojov (napr. posudky, škály, konzultácie)
- V prípade AI: testovanie výstupu na vzorke, porovnanie s ľudským úsudkom

4. Spätná väzba

- Získanie názoru ďalších odborníkov, prípadne samotného dieťaťa (ak je to možné)
- Reflexia rozhodnutia z viacerých uhlov – právneho, psychologického, sociálneho

5. Finálne rozhodnutie

- Po kalibrácii sa rozhodnutie upraví, potvrdí alebo zamietne
- Musí byť odôvodnené, transparentné a zdokumentované

6. Monitoring a korekcia

- Po vykonaní rozhodnutia sa sleduje jeho dopad na dieťa
- V prípade negatívnych dôsledkov sa rozhodnutie bezodkladne reviduje

Záver

Analýza právneho rámca, rozhodovania v najlepšom záujme dieťaťa, využitia AI a prípadovej štúdie Allegheny County ukazuje, že rozhodovanie o najlepšom záujme dieťaťa je multidimenzionálny proces, ktorý si vyžaduje kombináciu právnej presnosti, psychologickej citlivosti a technologickej opatrnosti. AI môže byť užitočným nástrojom, ale nesmie nahradiť ľudský úsudok, empatiu ani etické zvažovanie.

Heuristiky sú nevyhnutnou súčasťou ľudského rozhodovania, no bez kalibrácie môžu viesť k systematickým chybám. AI môže pomôcť tieto chyby identifikovať, ale zároveň môže sama generovať nové riziká, ak nie je správne navrhnutá, testovaná a kontrolovaná.

Zároveň sa nám, pri našej analýze načrtlo niekoľko otázok, ktoré by mali byť predmetom ďalšieho skúmania problematiky využitia modelov umelej inteligencie v rodinnoprávnej agende:

- **Autonómia vs. automatizácia:** Kde je hranica medzi podporou rozhodovania a jeho nahradením?
- **Presnosť vs. dôstojnosť:** Môže byť technicky správne rozhodnutie zároveň ľudsky necitlivé?
- **Efektivita vs. spravodlivosť:** Je rýchle rozhodovanie vždy v najlepšom záujme dieťaťa?
- **Zodpovednosť vs. delegácia:** Kto nesie právnu a morálnu zodpovednosť za rozhodnutie ovplyvnené AI?

Princíp najlepšieho záujmu dieťaťa je komplexný, dynamický a citlivý na kontext. V digitálnej dobe čelí novým výzvam, ktoré si vyžadujú premyslené odpovede. Umelá inteligencia môže byť užitočným nástrojom, ak je správne navrhnutá, eticky kalibrovaná a pod ľudským dohľadom. Optimalizácia rozhodovania v rodinnom práve nesmie viesť k strate dôstojnosti, empatie ani individuálneho posúdenia. Budúcnosť

patri hybridným modelom, ktoré spájajú technológiu s ľudskosťou, presnosť s citlivosťou, efektívnosť s spravodlivosťou. Ochrana najlepšieho záujmu dieťaťa musí zostať prvoradým hľadiskom – bez ohľadu na to, kto rozhoduje.

Zoznam použitej literatúry

1. VEČEŘA, M. a kol.: Teória práva. 2. vyd. Bratislava: Euro Kódex, 2008. I SBN 978-80-89363-21-6
2. Nález Ústavného súdu ČR z 9. apríla 1997, sp. zn. PL. ÚS 31/96
3. COUTURE, R.J.: The impact of artificial intelligence on law firms' business models. Harvard Law School Center on the legal Profession, 2025. [online] dostupné: <https://clp.law.harvard.edu/knowledge-hub/insights/the-impact-of-artificial-intelligence-on-law-law-firms-business-models/>
4. WILLIAMSON, J.: The Rise of AI in Legal Practice: Opportunities, Challenges, & Ethical considerations". In: Colorado Technology Law Journal, 2025. [online] dostupné: <https://ctlj.colorado.edu/?p=1297>
5. LINNA, E. and LINNA, T.: Judicial Requirements for Generative AI in Legal Reasoning. *ArXiv* abs/2508.18880 (2025)
6. Summarizing Recent Research on Predictive Risk Models in Child Welfare, 2024. [online] dostupné: [24-ACDHS-04-Predictive-Risk-Algorithms.pdf](#)
7. Allegheny County. Evaluation Findings on the Use of Predictive Risk Model in Child Welfare, 2024. [online] Dostupné na: [https:// Allegheny Family Screening Tool - Allegheny County, PA](https://AlleghenyFamilyScreeningTool-AlleghenyCounty,PA)
8. Dohovor o právach dieťaťa
9. Výbor OSN pre práva dieťaťa. Všeobecný komentár č. 14 (2013) k článku 3 ods. 1 Dohovoru o právach dieťaťa
10. Zákon č. 36/2005 Z. z. o rodine a o zmene a doplnení niektorých zákonov
11. LANSDOWN, G., "The evolving capacities of the child", Innocenti Research Centre, UNICEF/Save the Children, Florence (2005)
12. KRÁLIČKOVÁ, Z.: Lidskoprávní dimenze českého rodinného práva. Brno: Masarykova univerzita, 2009. 75 s. ISBN 978-80-210-5053-2

Kontaktné údaje

Mgr. Petronela Luprichová Cvengrošová
petronela.luprichova@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta

Sekcia finančného práva

Právo finančného trhu a daňové právo v kontexte
digitalizácie a kybernetickej bezpečnosti

DAŇOVÉ EXEKUČNÉ KONANIE V PODMIENKACH DIGITALIZÁCIE: PERSPEKTÍVY DO BUDÚCNOSTI

TAX ENFORCEMENT PROCEEDINGS IN THE CONTEXT OF DIGITALIZATION: FUTURE PERSPECTIVES

Tímea Jančiová¹

Abstrakt: Prezintovaný článok sa zaoberá problematikou daňového exekučného konania v Slovenskej republike so zreteľom na jeho digitalizáciu a perspektívy ďalšieho vývoja. Cieľom je zmapovať aktuálny stav tohto procesu, identifikovať prvky digitalizácie už zavedené do praxe a poukázať na možnosti jeho modernizácie v kontexte európskych a medzinárodných trendov. Výskumný rámec je založený na kombinácii analytickej, komparatívnej, syntetickej a deskriptívnej metódy, ktoré umožnili zhodnotiť právnu úpravu, aplikačnú prax a skúsenosti zo zahraničia. Výsledky poukazujú na to, že hoci v posledných rokoch došlo k určitému pokroku, napríklad zavedením povinnej elektronickej komunikácie, QR kódov či prípravou predvyplnených daňových priznaní, digitalizácia daňového exekučného konania má zatiaľ prevažne čiastkový charakter. Elektronické dražby a širšie využitie inteligentných digitálnych nástrojov neboli dosiaľ implementované, čo naznačuje potrebu legislatívnych, technologických a organizačných reforiem. Prínos práce spočíva v zmapovaní stavu digitalizácie daňového exekučného konania, identifikácii medzier v právnej úprave a praxi, ako aj v načrtnutí perspektív jeho budúceho rozvoja. Výsledky sú využiteľné pre tvorcov právnych predpisov, orgány finančnej správy a odbornú verejnosť, keďže poskytujú podklady pre diskusiu o možnostiach implementácie moderných digitálnych riešení, vrátane umelej inteligencie, s cieľom zvýšiť efektívnosť, transparentnosť a právnu istotu daňových subjektov.

Kľúčové slová: daňové exekučné konanie, daňová exekúcia, digitalizácia, daňové právo

Abstract: The presented article addresses the issue of tax enforcement proceedings in the Slovak Republic, with particular emphasis on their digitalization and future perspectives. The objective is to map the current state

¹ Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Katedra finančného práva, daňového práva a ekonómie

of this process, to identify elements of digitalization already introduced into practice, and to highlight opportunities for its modernization in the context of European and international trends. The research framework is based on a combination of analytical, comparative, synthetic, and descriptive methods, which enabled the assessment of the legal framework, practical application, and foreign experience. The results indicate that although certain progress has been achieved in recent years, such as the introduction of mandatory electronic communication, QR codes, and the preparation of pre-filled tax returns, the digitalization of tax enforcement proceedings has thus far remained largely partial in nature. Electronic auctions and the broader use of intelligent digital tools have not yet been implemented, which suggests the necessity of legislative, technological, and organizational reforms. The contribution of this study lies in mapping the state of digitalization of tax enforcement proceedings, identifying gaps in the legal framework and practice, and outlining perspectives for their future development. The results are relevant for lawmakers, tax administration authorities, and the professional community, as they provide a basis for discussion on the implementation of modern digital solutions, including artificial intelligence, with the aim of increasing efficiency, transparency, and legal certainty for taxpayers.

Key words: tax enforcement proceedings, tax execution, digitalization, tax law

Úvod

Daňové exekučné konanie predstavuje kľúčový nástroj pri vymáhaní daňových nedoplatkov, čím priamo prispieva k efektívnej činnosti daňovej správy a k stabilnému zabezpečeniu príjmov štátneho rozpočtu. Daňové exekučné konanie je jedným z exekučných konaní, s ktorými sa môžeme stretnúť v našom právnom poriadku. Prijatím zákona č. 219/1999 Z. z. bol s účinnosťou od 1. septembra 1999 zavedený inštitút daňového exekučného konania.²

V dnešnej dobe rýchleho rozvoja moderných technológií sa otvárajú nové príležitosti a možnosti zefektívnenia tohto procesu a samotného inštitútu daňového exekučného konania, resp. daňovej exekúcie v podmienkach Slovenskej republiky. V posledných rokoch sa otázka digitalizácie dostáva do popredia v mnohých vedných odboroch či vedeckých disciplínach a právo, ktoré jestvovalo odnepamäti, prirodzene nie je výnimkou.

Digitalizácia v spojení s oblasťou daňového práva, konkrétne s inštitútom daňového exekučného konania, znamená potenciálny vysoko pozitívny prínos a početné

² BABČÁK, Vladimír. *Daňové právo procesné*. Košice: ATOM computers, 2000. s. 334.

benefity, či už ide o otázku efektívnosti či transparentnosti vymáhania daňových nedoplatkov, plynulejšieho toku finančných prostriedkov do verejných rozpočtov, či samotnej dôvery dotknutých subjektov voči autoritám stojacim nad nimi.

Digitalizácia všeobecne predstavuje jednu z kľúčových výziev súčasnosti a zároveň otvára dvere novým možnostiam, ako novými modernými technológiami zefektívniť a celkovo vylepšiť tradičné právne procesy. Daňové právo a konkrétne daňové exekučné konanie sa nachádza na v prelomovom bode transformácie.

Trendy v oblasti digitalizácie daňovej správy možno pritom sledovať v širšom medzinárodnom kontexte, ktoré postupne prichádzajú aj k nám. V Európskej únii je kladený dôraz na elektronizáciu procesov a zefektívnenie cezhraničnej spolupráce, o čom svedčí Smernica o administratívnej spolupráci v oblasti daní (*DAC – Directive on Administrative cooperation*)³, ktorá upravuje elektronickú výmenu informácií medzi krajinami. V spojení s digitalizáciou v rámci EÚ možno spomenúť balík opatrení týkajúci sa DPH v digitálnom veku – z tlačovej správy z 5. novembra 2024 vyplýva, že Rada Európskej únie „dosiahla dohodu o nových opatreniach, ktorými sa EÚ prispôsobuje digitálnemu veku. Vďaka novým pravidlám pre elektronické faktúry a oznamovanie údajov v reálnom čase, ako aj pre podnikanie prostredníctvom digitálnych platforiem umožní tento balík právnych predpisov bojovať proti daňovým podvodom, podporiť podniky a presadiť digitalizáciu.“⁴

Okrem toho možno spomenúť správu OECD „*Tax Administration Digitalisation and Digital Transformation Initiatives*“, ktorá sumarizuje dáta z *Inventory of Tax Technology Initiatives (ITTI)*. Jej obsahom je bohatý repertoár informácií z viac ako 100 jurisdikcií týkajúcich sa využitia technológií daňovými správami a jej hlavným cieľom je napomôcť daňovým správam pri riešení a zvažovaní možných „domácich“ reforiem, ako aj napomôcť identifikácii budúcich spoluprác medzi daňovými správami.⁵ V uvedenom dokumente nájdeme témy ako využívanie digitálnych identít, automatické predvypĺňanie údajov v systémoch či dokonca využívanie umelej inteligencie, ktorú využíva viac ako 70% daňových správ. Mnohé daňové správy začali s identifikáciou a mapovaním potrebných schopností pre „digitálnu

³ SMERNICA RADY 2011/16/EÚ 77/799/EHS z 15. februára 2011 o administratívnej spolupráci v oblasti daní a zrušení smernice (DAC – Directive on Administrative cooperation). Dostupné na : https://taxation-customs.ec.europa.eu/taxation/tax-transparency-cooperation/administrative-co-operation-and-mutual-assistance/directive-administrative-cooperation-dac_en

⁴ Tlačová správa Rady Európskej únie z 15. novembra 2024. „Zdaňovanie: Rada sa dohodla na balíku opatrení týkajúcich sa DPH v digitálnom veku“. Dostupné na : <https://www.consilium.europa.eu/en/press/press-releases/2024/11/05/taxation-council-agrees-on-vat-in-the-digital-age-package/>

⁵ OECD. *Tax Administration Digitalisation and Digital Transformation Initiatives*, OECD Publishing, Paris. 2025. Dostupné na : <https://doi.org/10.1787/co76d776-en>.

transformáciu“ a dokonca 80% správ vyvinulo stratégiu pre „digitálnu transformáciu“. ⁶

Ako posledný z príkladov uvádzame tzv. Tax Administration 3.0, konkrétne dokument nedávno publikovaný OECD Forum on Tax Administration s názvom „*Tax Administration 3.0: From Vision to Strategy*“⁷. Predmetný dokument prezentuje rôzne odporúčania a myšlienky, potencionálne benefity, otázky automatizácie, AI a pod., či samotnú otázku prečo je vôbec potrebné rozvinúť stratégiu digitálnej transformácie. Digitalizácia citeľne prebieha vo všetkých oblastiach života, daňové právo – daňové správy a jednotlivé relevantné inštitúty nie sú výnimkou. Inštitút daňového exekučného konania do určitej miery prešiel modernizáciou, podstatné kroky k jeho modernej zdigitalizovanej podobe však má stále pred sebou.

Cieľom tohto článku je vymedziť problematiku daňového exekučného konania. Pozornosť bude zameraná na analýzu súčasného stavu daňového exekučného konania v kontexte prebiehajúcej digitalizácie. Parciálnym cieľom je načrtnutie perspektívy jeho ďalšieho vývoja, možnosti implementácie moderných digitálnych prvkov, ako aj vypočítanie potenciálnych benefitov či rizík do budúcnosti.

Pokiaľ ide o metodológiu, pri spracovaní príspevku bola použitá kombinácia viacerých vedeckovýskumných metód typických pre právnu vedu. Základ tvorila analytická metóda, ktorá sa uplatnila pri skúmaní súčasného právneho rámca daňového exekučného konania v Slovenskej republike, so zreteľom na zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a jeho novelizácie, ako aj na relevantné strategické dokumenty Ministerstva financií SR a Finančnej správy SR, vrátane Národného programu reforiem (2023,2024) a Výročnej správy o pokroku 2025. Súčasťou metodologického postupu bola aj komparatívna metóda, prostredníctvom ktorej sa skúmal stav digitalizácie daňovej správy resp. daňového exekučného konania s Českou republikou. Výsledky týchto analýz boli následne spracované syntetickou metódou, ktorá umožnila formulovať závery a odporúčania vychádzajúce zo zistení analytického skúmania. Napokon bola využitá aj deskriptívna metóda, ktorá sa uplatnila pri popise trendov digitalizácie v oblasti daňového práva. Kombinácia uvedených metodologických prístupov umožnila nielen analyzovať aktuálny stav právnej úpravy a jej fungovanie v praxi, ale aj poukázať na budúce výzvy.

Súčasný stav poznania

⁶ OECD. *Tax Administration Digitalisation and Digital Transformation Initiatives*, OECD Publishing, Paris. 2025. Dostupné na : <https://doi.org/10.1787/co76d776-en>.

⁷ OECD Forum on Tax Administration. *Tax Administration 3.0: From Vision to Strategy*. 2025. Dostupné na : <https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/tax-administration-3-o-from-vision-to-strategy.pdf>

Vo všeobecnosti sa exekúciou chápe zákonom ustanovený postup, ktorým štátny orgán vynucuje plnenie uložené rozhodnutím, ktoré nebolo splnené dobrovoľne - takýto postup je realizovaný v rámci osobitného druhu právneho procesu, ktorý sa v odbornej literatúre zvykne označovať všeobecným pomenovaním exekučné konanie. V súčasnosti je exekučné konanie samostatne upravené najmä pre konanie trestné, občianske súdne, správne a daňové.⁸ Vymáhanie daní (resp. daňových nedoplatkov) sa týka situácií, kedy daňový subjekt dobrovoľne neuhradí daňový nedoplatok, ktorý je splatnou daňovou pohľadávkou.⁹

Daňové exekučné konanie, upravené v zákone č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov, konkrétne v ustanovení § 88 a nasl., je *konanie, v ktorom správca dane z úradnej moci vymáha daňový nedoplatok, iné peňažné plnenie uložené rozhodnutím, exekučné náklady a hotové výdavky*¹⁰. Splnomocňuje správcu dane - daňový úrad a colný úrad - vykonávať všetky právne úkony v mene štátu. Pokiaľ ide o správcu dane – obec - ďalej môže okrem výkonu exekúcie podľa ustanovení tohto zákona postupovať aj tak, že požiada o výkon exekúcie súdneho exekútora.¹¹

Toto konanie predstavuje špecifickú a významnú súčasť daňového práva, ktorá priamo súvisí s vymáhaním daňových nedoplatkov a ich efektívnym výberom. Tento inštitút bol zavedený s účinnosťou od 1. septembra 1999 a súčasne nahradil dovtedajší právny režim vymáhania daňových nedoplatkov ktoré bolo považované za procesnú etapu, respektíve štádium daňového konania.¹² Zákonodarca jasne a jednoznačne rozlišuje medzi daňovým konaním a daňovým exekučným konaním, dôkazom je aj ich samostatné legálne vymedzenie – sú to dve relatívne samostatné časti výkonu správy daní, ich vzájomný pomer vyplýva z rôznych úloh a cieľov, ktoré sledujú.¹³

Napriek jeho nespornému zásadnému významu, vedecká komunita v Slovenskej republike tejto problematike nevenuje náležitú pozornosť. Publikačné výstupy sa zväčša sústreďujú na všeobecné otázky daňového práva, pričom oblasť daňového exekučného konania a výkonu daňových exekúcií zostáva spracovaná iba v obmedzenom, nepatrnom rozsahu.

⁸ BABČÁK, Vladimír. *Slovenské daňové právo*. [1. vyd.]. Bratislava: Epos, 2012. s. 598.

⁹ GROSSOVÁ, Marie Emilie : „*Daňová exekuce*“. In : *Znalosti pro tržní praxi 2015: ženy - podnikatelky v minulosti a současnosti: sborník z mezinárodní vědecké konference : 10. a 11. září 2015 v Olomouci*. Olomouc: Societas Scientiarum Olomucensis II, 2015. s. 135.

¹⁰ § 88 ods. 1 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov

¹¹ KUBINCOVÁ, Soňa. *Daňový poriadok: komentár*. 2. vydanie. Beckova edícia komentované zákony. Praha: C.H. Beck, 2024. s. 746.

¹² BABČÁK, Vladimír. *Dane a daňové právo na Slovensku: (teória a legislatíva)*. Ružomberok: Epos, 2022. s. 747.

¹³ BABČÁK, Vladimír. *Daňové (exekučné) konanie*. Bratislava: Veda, 2005. s. 252-253.

Pokiaľ ide o problematiku daňového exekučného konania, z dostupných relevantných slovenských zdrojov možno spomenúť monografiu prof. Babčáka „*Daňové (exekučné) konanie*“ publikovanú v roku 2005¹⁴. Na tomto mieste je potrebné zdôrazniť, že dodnes nebola vydaná iná publikácia – monografia, ktorá by sa venovala len daňovému exekučnému konaniu v tomto rozsahu.

Daňové exekučné konanie býva spravidla stručne, rámcovo a v rozsahu platnej právnej úpravy súčasťou literatúry týkajúcej sa daňového práva ako celku, či napr. oblasti daňového práva procesného¹⁵. Ak by sme chceli nájsť odborné a vedecké články na túto tému, ďaleko by sme sa nedopracovali.

Na vedeckej úrovni je tejto téme venovaná nedostatočná pozornosť, počet článkov, ktoré by sme našli nepresiahne hranicu jednociferného čísla, nehovoriac o tom, že ide o príspevky značne zastaralé a neaktuálne – nezachytávajú nové výzvy spojené s implementáciou moderných technológií. Pokiaľ by sme chceli nájsť slovenské vedecké príspevky týkajúce sa daňového exekučného konania v spojení s jeho digitalizáciou, naša cesta by skončila skôr než začala.

V zahraničí však nájdeme mnoho autorov z rôznych krajín, ktorí sa venujú daňovému právu a pohľadu naň optikou digitalizácie a jej prínosom či hrozbám. Napr. v oblasti daňového práva či práva obchodných spoločností, niektoré štúdie naznačujú, že digitalizácia prispieva k znižovaniu daňových únikov, čo môže pomôcť orgánom verejnej moci vnímať digitalizáciu ako silný nástroj na predchádzanie finančnej kriminalite. (Bogdan-Florian Amzuică, Roxana-Adriana Mititelu, Ileana Nişulescu)¹⁶, či napríklad využitie digitálnych technológií v rámci daňovej kontroly (daňového auditu) v Rusku, ktoré sa podľa štúdií javí ako značne pozitívne vďaka automatizácii kontroly dokumentov v rámci tohto procesu (Imeda A. Tsindeliani, Tatyana A. Guseva, Anton V. Izotov)¹⁷.

Z hľadiska súčasného výskumu možno identifikovať významnú výskumnú medzeru, a to práve vo vzťahu medzi problematikou digitalizácie a daňovým exekučným konaním. Tento príspevok je zhmotnením ambície vyplniť uvedenú výskumnú medzeru, resp. vykonať postupné kroky k tomuto cieľu. Máme za to, že vzhľadom na charakter daňového exekučného konania je nevyhnutné začať mu venovať zvýšenú pozornosť. Je nevyhnutné poukázať na aktuálnosť daňového exekučného konania,

¹⁴BABČÁK, Vladimír. *Daňové (exekučné) konanie*. Bratislava: Veda, 2005. ISBN 8022408441.

¹⁵Príkladmo: BABČÁK, Vladimír. *Dane a daňové právo na Slovensku: (teória a legislatíva)*. Ružomberok: Epos, 2022. ISBN 9788056203392, BABČÁK, Vladimír. *Slovenské daňové právo*. [1. vyd.]. Bratislava: Epos, 2012. ISBN 9788080579715 a i.

¹⁶AMZUICĂ, Bogdan-Florian – MITITELU, Roxana-Adriana – NIŞULESCU, Ileana. "Digitalization of Business – Implications on Tax Evasion Dimensions". In: *Proceedings of the International Conference on Business Excellence* The Bucharest University of Economic Studies, 17, no. 1. 2023. s. 1888.

¹⁷TSINDELIANI, Imeda A. – GUSEVA, Tatyana A. – IZOTOV, Anton V. „The improvement of tax control in the conditions of digitalization. *Law Enforcement Review*“. 6(1), 2022 s. 77.

resp. daňových exekúcií. Tento inštitút je v našich podmienkach využívaný v značnej miere. V tomto roku (2025) za prvých 6 mesiacov bolo vydaných 20 887 rozhodnutí o začatí daňového exekučného konania, za rok 2024 ich bolo 36 953. Nedoplatky odstúpené na vymáhania za prvé 4 mesiace tohto roka presahujú sumu 440 miliónov eur.¹⁸ Z uvedených číselných údajov je naozaj citelná vážnosť inštitútu daňového exekučného konania a jeho význam pre plynutie finančných prostriedkov do verejných rozpočtov a v konečnom dôsledku fungovanie našej krajiny ako takej. Je preto nevyhnutné spracovať príspevok mapujúci súčasný stav daňového exekučného konania so zohľadnením aktuálnych trendov v digitalizácii.

Digitalizácia procesov

Fenoménom 21. storočia sa stáva digitalizácia, ktorá preniká do všetkých oblastí spoločenského života.¹⁹ Digitalizácia je v zmysle dostupných internetových zdrojov akýsi „proces prechodu z analógových formátov na formáty digitálne“²⁰. Či už ide o digitalizáciu rôznych dokumentov, hudby, alebo digitalizáciu prebiehajúcu v oblastiach ako je právo, stretávame sa s ňou čoraz častejšie.

Digitalizáciu v právnej oblasti možno aj ako reakciu zákonodarcu na spoločenské zmeny prirodzene plynúce z nových možností, ktoré so sebou prinášajú rozvoj digitálnych technológií. Hovoriť možno o širokom diapazóne využívania digitálnych technológií : umožnenie elektronickej komunikácie so súdmi, zriaďovaní elektronických schránok a pod.²¹

V odbornej literatúre sa často stretneme s pojmom „štvrtá priemyselná revolúcia“. Štvrtá priemyselná (t. j. digitálna) revolúcia sa stala hlavnou témou na výročnom zasadnutí Svetového ekonomického fóra v Davose.²²

Predchádzajúce priemyselné revolúcie oslobodili ľudstvo od zvieracej sily, umožnili masovú výrobu a priniesli digitálne schopnosti miliardám ľudí. Štvrtá priemyselná revolúcia je zásadne odlišná. Je charakterizovaná radom nových technológií, ktoré

¹⁸Open Data portál Ministerstva financií Slovenskej republiky. Dostupné na : <https://opendata.financnasprava.sk/opendata/category/145-vymahanie-a-exekucie>

¹⁹ SIMIČ, S., ČAKOCI, K., 2022. K vybraným otázkam zdaňovania digitálnej ekonomiky. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.) Právo obchodu ekonomika. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 29.

²⁰Digitalizácia. Internetový zdroj : <https://www.ui42.sk/uickovska-abeceda/digitalizacia#:~:text=%C4%8Co%20to%20znamen%C3%A1%20Digitaliz%C3%A1cia%20je%20proces%20prechodu,%C4%8D%C3%ADm%20sa%20zvy%C5%A1uje%20ich%20dostupnos%C5%A5%20a%20vyu%C5%BEite%C4%BEnos%C5%A5.>

²¹ SOKOL, Michal. *Digitalizácia a umelá inteligencia v obchodných spoločnostiach*. Beckova edícia právne inštitúty. Bratislava: C.H. Beck, 2024. s. 3.

²² KAČALJAK, Matej. *Vybrané trendy vo výbere daní a možnosti ich právnej reflexie na Slovensku*. Monografie. Bratislava: Wolters Kluwer. 2017. s. 43.

spájajú fyzický, digitálny a biologický svet, ovplyvňujú všetky disciplíny, ekonomiky a odvetvia a dokonca spochybňujú predstavy o tom, čo znamená byť človekom.²³

Tento fenomén so sebou prináša množstvo benefitov, bez ohľadu na oblasť ktorej sa digitalizácia týka možno spomenúť zrýchlenie či zvýšenie efektivity procesov, jednoduchší prístup k informáciám a s tým spojený transparentnosť, skvalitnenie služieb a zvýšenie komfortu cieľových subjektov či iné. Samozrejme, každý fenomén má dve stránky – pozitívnu a negatívnu – možné negatívne dopady a potencionálne hrozby.

V oblasti podnikania, transformácia podnikania nie je výhodou iba pre samotné podniky, ktoré týmto procesom prechádzajú, ale aj pre samotného spotrebiteľa, ktorý získava produkty a služby rýchlejšie a môže si ich zabezpečiť pohodlnejšie. Toto všetko je však vykúpené istým narušením integrity jeho súkromia a základných práv – v súvislosti s využívaním elektronickej komunikácie totiž dochádza napr. k masívnemu zhromažďovaniu údajov o spotrebiteľoch, ich súkromí a správaní.²⁴

Bez ohľadu na to, aké potencionálne benefity či naopak hrozby digitalizácia prináša, nemožno oponovať faktu, že sa jedná o prirodzene vyvíjajúci sa proces prenikajúci do všetkých sfér života. Slovenské daňové právo nie je výnimkou.

Digitalizácia slovenského daňového práva v praxi

V praxi daňového práva sa môžeme stretnúť s viacerými prvkami, ktoré možno vnímať ako výsledok digitalizácie a elektronizácie.

Praktické príklady z praxe možno spomenúť inštitúty zakomponované na webovej stránke Finančnej správy Slovenskej republiky²⁵. Mottom modernej proklientskej finančnej správy je „menej administratívy, viac výkonu“. ²⁶ Na tomto mieste možno spomenúť predvyplnené daňové priznania k dani z motorových vozidiel či informatívne upozornenia pre klientov finančnej správy. Z digitálnych projektov je na mieste spomenúť projekt „Elektronická komunikácia“ (zavedenie povinnosti vybraných subjektov doručovať podania elektronicke), projekt „eKasa“ (povinný systém pre podnikateľov, napojenie pokladníc na portál FS; projekt je súčasťou

²³ HUČKOVÁ, Regina - SOKOL, Pavol - RÓZENFELDOVÁ, Laura: „4th Industrial Revolution and Challenges for European Law (with Special Attention to the Concept of Digital Single Market)“. In: *EU and Comparative Law Issues and Challenges Series (ECLIC)*, Vol. 2, (2018). s. 202. Dostupné na : <https://doi.org/10.25234/eclic/7107>.

²⁴ TREŠČÁKOVÁ, Diana. „Individuals and their rights in the middle of digitalization and technological progress of the society“. In : *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7. 2023. s. 322. Dostupné na : <https://doi.org/10.25234/eclic/27453>

²⁵ Internetová stránka Finančnej správy Slovenskej republiky. Dostupné na : <https://www.financnasprava.sk/sk/titulna-stranka>

²⁶ Digitalizácia procesov. Internetová stránka Finančnej správy Slovenskej republiky. Dostupné na : <https://www.financnasprava.sk/sk/financna-sprava/digitalizacia-procesov>.

opatrení na boj proti daňovým podvodom - vďaka nim sa podarilo znížiť daňovú medzeru zo 41% na 26% a do štátnej pokladnice priniesli viac o približne 3,7 mld. eur), projekt „Call centrum a sociálne siete“ (o. i. prevádzka Facebook stránky) a projekt „TAXANA“ (automatizovaný chatbot, ktorého úlohou je automatická komunikácia medzi verejnosťou a inštitúciou, čím môže finančná správa vybaviť väčšie množstvo dopytov a odbremeniť zamestnancov call centra).²⁷

Digitalizácia daňového exekučného konania v Slovenskej republike

Digitalizácia sa do istej miery dotkla aj daňového exekučného konania v Slovenskej republike, čo predstavuje významný krok smerom k modernizácii štátnej správy a jej jednotlivých inštitúcií, inštitútov a procesov. Výsledkom digitalizácie sú napr. elektronické služby poskytované Finančnou správou Slovenskej republiky či (povinná) elektronická komunikácia, čo znamená značné urýchlenie a zjednodušenie. Napriek malému množstvu prvkov zavedených na účely digitalizácie daňového exekučného konania je však stále prítomná jeho nemoderná a neaktuálna povaha, čo potvrdzuje aj vyjadrenie Ministerstva financií SR ešte z roku 2023²⁸.

V Národnom programe reforiem 2023 vydanom Ministerstvom financií Slovenskej republiky²⁹ nájdeme opatrenie s názvom „Zefektívniť procesy vymáhania daňových nedoplatkov“, obsahom ktorého mala byť novela Daňového poriadku v časti upravujúcej vymáhanie nedoplatkov (najmä elektronizácia dražieb, zefektívnenie iných spôsobov výkonu daňovej exekúcie, odstránenie obsolentných ustanovení), zabezpečenie technickej podpory pre daňových exekútorov (rýchly prístup k majetkovým a iným registrom) a i. V Národnom programe reforiem 2024³⁰ sa pri predmetnom opatrení uvádza, že „Daňový poriadok sa novelizuje s cieľom zvýšenia objemu vymožených a uhradených nedoplatkov, zníženia celkového objemu evidovaných nedoplatkov, zvýšenia efektivity vymáhania a zabezpečenia rozvoja IT

²⁷ Digitalizácia procesov. Internetová stránka Finančnej správy Slovenskej republiky. Dostupné na : <https://www.financnasprava.sk/sk/financna-sprava/digitalizacia-procesov>.

²⁸ „Cieľom pripravovanej novely daňového poriadku je zreformovať daňové exekučné konanie, zaviesť nové efektívne formy daňovej exekúcie a existujúce upraviť tak, aby reflektovali aktuálnu prax, moderné trendy digitalizácie a elektronizácie výkonu štátnej správy a čerpali z osvedčených medzinárodných postupov. (...) obsahuje niektoré v súčasnosti už nerelevantné inštitúty. Efektivita výkonu daňovej exekúcie tak dosiahla limity zákonnej úpravy, ktorá však nereflektuje moderné trendy výkonu rozhodnutí.“ Dostupné na : TASR : „Daňové exekučné konanie by sa malo zreformovať“. Dostupné online : <https://www.vssr.sk/clanok-z-titulky/danove-exekucne-konanie-by-sa-malo-zreformovat-spravodajstvo-7-2023.htm>.

²⁹ Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/narodny-program-reforiem/narodny-program-reforiem-2023.pdf>

³⁰ Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/narodny-program-reforiem/npr-2024.pdf>

podpory exekútorov. Aktuálne prebiehajú práce na finalizácii textu návrhu legislatívnej úpravy (implementácia prebieha)".

Z Výročnej správy o pokroku 2025³¹ sa dozvieme, že doposiaľ došlo k skvalitneniu elektronických služieb finančnej správy a to „zavedením QR kódov v dokumentoch štátnych inštitúcií s cieľom zjednodušiť platby, eliminovať manuálne zadávanie údajov, znížiť chybovosť a zvýšiť spokojnosť používateľov. V júni 2024 boli spustené všetky tri fázy zavádzania QR kódov do dokumentov exekútorov, kontrolórov a správcov. V oblasti spotrebných daní boli QR kódy skompletizované v apríli 2025. QR kódy pre dovozné platby budú zavedené v roku 2026“³². QR kódy boli úspešne zavedené, aktuálne je táto informácia zverejnená na oficiálnej webovej stránke Finančnej správy SR.³³ Ďalším novým prvkom má byť „predvyplnenie daňových priznaní, ktoré má byť realizované pomocou asistenta na základe spracovania údajov z potvrdenia o zdaniteľných príjmoch. V priebehu roku 2025 je plánované vykonanie analýzy predvyplnenia daňových priznaní pomocou asistenta, s predpokladaným zavedením na daňových priznaniach podaných v roku 2026 za zdaňovacie obdobie roku 2025". Aktuálny stav opatrenia s názvom „Zefektívniť procesy vymáhania daňových nedoplatkov" je nasledovný : „prebieha komunikácia medzi FR SR a MF SR k zneniu legislatívnej úpravy, ktorá už prešla predbežným pripomienkovým konaním so súhlasným stanoviskom komisie. Súčasne sa pokračuje v aplikácii nelegislatívnych opatrení na zefektívnenie vymáhania nedoplatkov a predchádzania ich vzniku.“³⁴.

Je na mieste zdôrazniť, že napriek zavedeniu QR kódov a pripravovaných predvyplnených daňových priznaní, zavedenie elektronických dražieb v rámci daňového exekučného konania ostáva doposiaľ nedotknutým teritórium.

Perspektívy do budúcnosti

Digitalizácia daňového exekučného konania v Slovenskej republike predstavuje postupne rozvíjajúci sa proces. Hoci boli doposiaľ dosiahnuté určité pozitívne výsledky, najmä v oblasti elektronizácie komunikácie, zavedenie a využívanie QR kódov v praxi či plánovaných predvyplnených daňových priznaní, stále možno hovoriť o pomerne roztrieštenom uplatňovaní digitálnych nástrojov. Zavedené opatrenia a digitálne nástroje môžeme vnímať skôr ako čiastkové drobné riešenia – k celkovej

³¹ Výročná správa o pokroku Slovenskej republiky 2025. Ministerstvo Financií Slovenskej republiky. Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/vyroczna-sprava-pokroku/vyroczna-sprava-pokroku-sr-2025.pdf>

³² Výročná správa o pokroku Slovenskej republiky 2025. Ministerstvo Financií Slovenskej republiky. str. 20. Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/vyroczna-sprava-pokroku/vyroczna-sprava-pokroku-sr-2025.pdf>

³³ Notifikačná služba ku QR platbám. Dostupné na : <https://www.info-qrplatby.sk/>

³⁴ Výročná správa o pokroku Slovenskej republiky 2025. Ministerstvo Financií Slovenskej republiky. str. 29. Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/vyroczna-sprava-pokroku/vyroczna-sprava-pokroku-sr-2025.pdf>

digitálnej transformácii daňového exekučného konania ako takého doposiaľ nedošlo, čo vytvára priestor pre zavedenie ďalších čiastkových opatrení, ktoré v konečnom dôsledku vytvoria modernú aktualizovanú podobu tohto konania.

Pokiaľ ide o perspektívy do budúcnosti a ďalší potencionálny vývoj daňového exekučného konania, je na mieste zaviesť inštitút už spomínaných elektronických dražieb. Ako inšpiráciu pre legislatívnu úpravu a prax možno využiť príklad z Českej republiky, kde je inštitút elektronických dražieb realizovaných v rámci daňových exekúcií plne zakomponovaný do ich právneho poriadku. Finanční správa ČR prevádzkuje webovú aplikáciu APED (Aplikace elektronických dražeb)³⁵, ktorá úspešne funguje a umožňuje komukoľvek zapojiť sa do dražby rôznych predmetov, čo značne rozširuje okruh potencionálnych vydražiteľov a v konečnom dôsledku úspešnosť vymáhania daňových nedoplatkov a uzatvorenie daňových exekučných konaní.

Do budúcnosti je nevyhnutné, aby digitalizácia a stav daňového exekučného konania či daňovej správy ako takej, prešiel od jednoduchých nástrojov na úroveň inteligentných riešení, ktoré budú založené na analýze dát, automatizácii procesov či plnom využívaní umelej inteligencie. Aktuálny trend využívania umelej inteligencie v mnohých oblastiach života sa javí ako žiaduci aj v oblasti daňového práva – daňového exekučného konania.

Tento proces zakomponovania nových digitálnych nástrojov prirodzene nie je jednoduchou jedno-krokovou záležitosťou. Budúcnosť digitalizácie daňového exekučného konania závisí od viacerých rovín. Jednak ide o rovinu legislatívnu – potreba novelizácie Daňového poriadku, zavedenie nových inštitútov, ktoré by obsahovali, resp. reflektovali moderné trendy. Ďalej rovina technická / technologická, nakoľko zavedenie nových inštitútov a podôb daňového exekučného konania bude vyžadovať technickú IT podporu. V neposlednom rade možno spomenúť organizačnú rovinu a s ňou súvisiacu procesnú rovinu, nakoľko bude potrebné prispôbiť dotknuté orgány – Finančnú správu, daňové úrady či priamo daňových exekútorov – novým podobám realizácie daňového exekučného konania. Ak máme mať v Slovenskej republike plne funkčné zdigitalizované systémy, je potrebné neustále pozorovať a hodnotiť medzery v právnej úprave a nedostatky v praxi. To umožní pružne reagovať na výzvy, pred ktorými inštitút daňového exekučného konania stojí.

Záver

Digitalizácia predstavuje jednu z najvýraznejších premien súčasnej spoločnosti. Nejde iba o zavádzanie nových technológií, ale o zásadnú transformáciu spôsobu fungovania štátnej správy, podnikateľského prostredia i celkového každodenného

³⁵ Dostupné na : <https://drazby.fs.gov.cz/client/main>

života jednotlivcov. V právnom poriadku sa digitalizácia čoraz viditeľnejšie prejavuje v oblasti daňového práva, pričom daňové exekučné konanie ako nástroj vymáhania daňových nedoplatkov a zabezpečenia príjmov verejných rozpočtov nemožno z tohto procesu vyňať.

Aktuálny stav daňového exekučného konania v Slovenskej republike do istej miery svedčí o prebiehajúcej digitalizácii, či už sa pozrieme na nedávne zavedenie QR kódov, pripravované predvyplnenie daňových priznaní či elektronizáciu Finančnej správy ako takej. Napriek určitým pozitívnym krokom stále ostávajú nevyplnené medzery a neprekonané výzvy. Slovenská republika stojí pred výzvou, aby digitalizáciu nevnímala iba ako akúsi technickú inováciu, ale ako dlhodobú stratégiu transformácie daňovej správy.

V blízkej budúcnosti tak bude potrebné zamerať pozornosť na implementáciu moderných technológií (umelej inteligencie, elektronizácie dražieb a i.), legislatívne prispôsobenie Daňového poriadku digitálnym procesom či budovanie technického vybavenia. Úspešné zvládnutie tohto procesu by znamenalo posun od tradičného, administratívne náročného modelu k modernému, transparentnému a efektívnemu mechanizmu, ktorý bude zodpovedať požiadavkám 21. storočia.

Zoznam použitej literatúry

1. AMZUICĂ, Bogdan-Florian – MITITELU, Roxana-Adriana – NIȘULESCU, Ileana. "Digitalization of Business – Implications on Tax Evasion Dimensions". In : *Proceedings of the International Conference on Business Excellence* The Bucharest University of Economic Studies, 17, no. 1. 2023. s. 1888-1896. Dostupné na : <https://doi.org/10.2478/picbe-2023-0166>
2. Aplikace elektronických dražeb. Finanční správa ČR. Dostupné na : <https://drazby.fs.gov.cz/client/main>
3. BABČÁK, Vladimír. *Dane a daňové právo na Slovensku: (teória a legislatíva)*. Ružomberok: Epos, 2022. 829 s. ISBN 9788056203392.
4. BABČÁK, Vladimír. *Daňové (exekučné) konanie*. Bratislava: Veda, 2005. 305 s. ISBN 8022408441.
5. BABČÁK, Vladimír. *Daňové právo procesné*. Košice: ATOM computers, 2000. 398 s. ISBN 8096840916.
6. BABČÁK, Vladimír. *Slovenské daňové právo*. 1. vyd. Bratislava: Epos, 2012. 670 s. ISBN 9788080579715.
7. Digitalizácia procesov. Internetová stránka Finančnej správy Slovenskej republiky. Dostupné na : <https://www.financnasprava.sk/sk/financna-sprava/digitalizacia-procesov>.
8. Digitalizácia. Internetový zdroj : <https://www.ui42.sk/uickovska-abeceda/digitalizacia#:~:text=%C4%8Co%20to%20znamen%C3%A1%20Digit>

[aliz%C3%A1cia%20je%20proces%20prechodu,%C4%8D%C3%ADm%20sa%20zvy%C5%A1uje%20ich%20dostupnos%C5%A5%20a%20vyu%C5%BEite%C4%BEnos%C5%A5](#)

9. GROSSOVÁ, Marie Emilie : „Daňová exekuce“. In : *Znalosti pro tržní praxi 2015: ženy - podnikatelky v minulosti a současnosti: sborník z mezinárodní vědecké konference : 10. a 11. září 2015 v Olomouci*. Olomouc: Societas Scientiarum Olomucensis II, 2015. 1149 s. ISBN 9788087533123.
10. HUČKOVÁ, Regina - SOKOL, Pavol - RÓZENFELDOVÁ, Laura: „4th Industrial Revolution and Challenges for European Law (with Special Attention to the Concept of Digital Single Market)“. In: *EU and Comparative Law Issues and Challenges Series (ECLIC)*, Vol. 2, (2018). s. 201–215. ISSN 2459-9425. Dostupné na : <https://doi.org/10.25234/eclic/7107>.
11. Internetová stránka Finančnej správy Slovenskej republiky. Dostupné na : <https://www.financnasprava.sk/sk/titulna-stranka>
12. KAČALJAK, Matej. *Vybrané trendy vo výbere daní a možnosti ich právnej reflexie na Slovensku*. Monografie. Bratislava: Wolters Kluwer. 2017. 89 s. ISBN 9788081686436.
13. KUBINCOVÁ, Soňa. *Daňový poriadok: komentár*. 2. vydanie. Beckova edícia komentované zákony. Praha: C.H. Beck, 2024. 1112 s. ISBN 9788074009822.
14. Národný program reforiem Slovenskej republiky 2023. Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/narodny-program-reforiem/narodny-program-reforiem-2023.pdf>
15. Národný program reforiem Slovenskej republiky 2024. Dostupné online : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/narodny-program-reforiem/npr-2024.pdf>
16. OECD (2025), *Tax Administration Digitalisation and Digital Transformation Initiatives*, OECD Publishing, Paris. Dostupné na : <https://doi.org/10.1787/c076d776-en>.
17. OECD Forum on Tax Administration. *Tax Administration 3.0: From Vision to Strategy*. 2025. Dostupné na : <https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/tax-administration-3-0-from-vision-to-strategy.pdf>
18. Open Data portál Ministerstva financií Slovenskej republiky. Dostupné online : <https://opendata.financnasprava.sk/opendata/category/145-vymahanie-a-exekucie>
19. SIMIČ, Soňa - ČAKOČI, Karin. 2022. K vybraným otázkam zdaňovania digitálnej ekonomiky. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.) *Právo obchod ekonomika*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 29-43. ISBN 9788057401544.

20. SMERNICA RADY 2011/16/EÚ 77/799/EHS z 15. februára 2011 o administratívnej spolupráci v oblasti daní a zrušení smernice (DAC – Directive on Administrative cooperation). Dostupné na : https://taxation-customs.ec.europa.eu/taxation/tax-transparency-cooperation/administrative-co-operation-and-mutual-assistance/directive-administrative-cooperation-dac_en.
21. SOKOL, Michal. *Digitalizácia a umelá inteligencia v obchodných spoločnostiach*. Beckova edícia právne inštitúty. Bratislava: C.H. Beck, 2024. 117 s. ISBN 9788082320506.
22. Tlačová správa Rady Európskej únie z 15. novembra 2024. „Zdaňovanie: Rada sa dohodla na balíku opatrení týkajúcich sa DPH v digitálnom veku“. Dostupné na : <https://www.consilium.europa.eu/en/press/press-releases/2024/11/05/taxation-council-agrees-on-vat-in-the-digital-age-package/>.
23. TREŠČÁKOVÁ, Diana. „Individuals and their rights in the middle of digitalization and technological progress of the society“. In : *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7. 2023. 315-333. Dostupné na : <https://doi.org/10.25234/eclic/27453>
24. TSINDELIANI, Imeda A. – GUSEVA, Tatyana A. – IZOTOV, Anton V. „The improvement of tax control in the conditions of digitalization. *Law Enforcement Review*“. 2022 ; 6(1):77-87. ISSN 2658-4050. Dostupné na: [https://doi.org/10.52468/2542-1514.2022.6\(1\).77-87](https://doi.org/10.52468/2542-1514.2022.6(1).77-87)
25. Výročná správa o pokroku Slovenskej republiky 2025. Ministerstvo financií Slovenskej republiky. Dostupné na : <https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/vyroczna-sprava-pokroku/vyroczna-sprava-pokroku-sr-2025.pdf>
26. Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov

Kontaktné údaje

Mgr. Tímea Jančiová

timea.janciova@student.upjs.sk

Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Katedra finančného práva, daňového práva a ekonómie

MIESTNE DANE A POPLATKY NA SLOVENSKU – AKTUÁLNE TRENDY¹

LOCAL TAXES AND FEES IN SLOVAKIA – CURRENT TRENDS

Erika Neubauerová², Tomáš Černěňko³

Abstrakt: Od naštartovania fiškálnej decentralizácie na Slovensku ubehlo dvadsať rokov. Počas tohto obdobia došlo v systéme miestnych daní a poplatkov k viacerým zmenám a úpravám legislatívy. Zavedený bol poplatok za rozvoj, zmenilo sa rozpočtové určenie dane z motorových vozidiel, viackrát došlo k zmenám v prerozdeľovaní dane z príjmov fyzických osôb medzi štát a územnú samosprávu. V ostatnom období sa čoraz častejšie diskutuje o efektívnosti a spravodlivosti zdanenia nehnuteľností, o tom, či súčasný finančný systém samospráv je vhodne nastavený aj vo vzťahu k rozsahu kompetencií, ktorými samospráva disponuje. Pozornosť je preto v príspevku venovaná miestnym daniam, najmä dani z nehnuteľností, ktorá zaznamenala v priebehu svojej existencie viacero legislatívnych zmien, stále sa však očakáva systémové riešenie úpravy jej daňového základu. Miestnym poplatkom s osobitným zreteľom na poplatok za rozvoj a najvýznamnejším zmenám v prerozdeľovaní výnosu dane z príjmov územnej samosprávy sa venujú ďalšie časti príspevku. Zámerom autorov je ponúknuť stručný prehľad doterajších zmien v systéme miestnych daní a poplatkov na Slovensku v kontexte daňového práva na úrovni územnej samosprávy.

Kľúčové slová: miestne dane, miestne poplatky, podielové dane, fiškálna decentralizácia

Abstract: Twenty years have passed since the beginning of fiscal decentralization in Slovakia. During this period, several changes and amendments to the legislation in the system of local taxes and fees have occurred. A development fee was introduced, the budgetary allocation of the motor vehicle tax was changed, and there have been several changes in the

¹ Príspevok je spracovaný v rámci projektu APVV – 22 – 0482 „Financovanie územnej samosprávy – potenciál funkčných mikroregiónov“.

² Ústav ekonomických vied, Právnická fakulta, Univerzita Komenského v Bratislave

³ Katedra verejnej správy a regionálneho rozvoja, Národohospodárska fakulta, Ekonomická univerzita v Bratislave

redistribution of personal income tax between the state and local governments.

Recently, there has been increasing discussion about the effectiveness and fairness of property taxation and whether the current financial system of local governments is appropriately set up in relation to the scope of powers available to local governments. This article therefore focuses on local taxes, in particular property tax, which has undergone several legislative changes during its existence, but a systemic solution to adjust its tax base is still awaited. Other sections of the paper deal with local fees, with particular emphasis on the development fee, and the most significant changes in the redistribution of income tax revenue to local governments. The authors' intention is to provide a brief overview of the changes to date and current trends in the development of the system of local taxes and fees in Slovakia in the context of tax law at the local government level.

Key words: local taxes, local fees, shared taxes, fiscal decentralization

Úvod

Decentralizácia verejnej správy je proces, v ktorom centrálna vláda presúva kompetenciu samostatne rozhodovať o istých záležitostiach alebo sa dokonca vzdáva určitých kompetencií v prospech nižších úrovní riadenia.⁴ V širšom zmysle slova mení decentralizácia vzájomné vzťahy medzi centrálnym (federálnym resp. štátnym rozpočtom) a rozpočtami nižších vládnych úrovní, čo sa odráža nie len v prerozdelení kompetencií, ale aj v primeranom nastavení daňovo-transferového mechanizmu, ktorého cieľom je posilniť použitie zdrojov v mieste ich vzniku a obmedzenie prerozdeľovacích procesov. Aj preto sa častejšie používa pomenovanie tohto procesu pojmom fiškálna decentralizácia. Jej zámerom je spravidla posilnenie finančnej nezávislosti a zodpovednosti nižších vládnych úrovní pri poskytovaní služieb občanom. Fiškálna decentralizácia môže viesť k efektívnejšiemu poskytovaniu miestnych verejných statkov a služieb a podporovať lepšie zosúladenie politík s preferenciami občanov⁵. Kľúčovými zámermi fiškálnej decentralizácie na Slovensku bolo: zvýšiť právomoc územnej samosprávy najnižšieho stupňa pri sadzbách dane z nehnuteľností a tým umožniť rast príjmov z tohto zdroja, transformovať miestne poplatky na miestne dane, zmeniť daňové určenie cestnej

⁴ KLIMOVSKÝ, Daniel: Základy verejnej správy. Košice: UPJŠ v Košiciach, 2008, s. 200.. ISBN 978-80-7097-713-2.

⁵ BARTOLINI David, STOSSBERG Sibylle, BLÖCHLIGER Hansjörg: Fiscal Decentralisation and Regional Disparities. OECD Economics Department Working Papers No. 1330, 2016. <https://dx.doi.org/10.1787/5jlpq7v3j237-en>

dane (dane z motorových vozidiel) v prospech rozpočtov vyšších územných celkov, zásadne zmeniť systém prerozdelenia výnosu dane z príjmov.⁶ V ďalšom texte príspevku sa zameriame na stručný popis vývoja miestnych daní a poplatkov, ako aj na zmeny súvisiace s podielom miestnych samospráv na dani z príjmov fyzických osôb.

Miestne dane – stručná genéza

Miestne dane sú upravené zákonom č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku za komunálne odpady a drobné stavebné odpady. Tento zákon vznikol „zlúčením“ zákona č. 317/1992 Zb. o dani z nehnuteľností, zákona č. 544/1990 Zb. o miestnych poplatkoch a zákona č. 87/1994 Z. z. o cestnej dani. V začiatkoch fiškálnej decentralizácie tak odrážal (ako jeden z najvýznamnejších zákonov) snahu o zmenu rozpočtového určenia daní slovenskej daňovej sústavy. Zahŕňal zvýšenie právomocí miestnej samosprávy pri zvyšovaní a znižovaní základných daňových sadzieb, úpravu nových miestnych daní, ktoré vznikli transformáciou miestnych poplatkov na miestne dane a tiež zmenu rozpočtového určenia dane z motorových vozidiel (vznikla transformáciou z cestnej dane) v prospech vyšších územných celkov. V dôsledku rôznych praktických potrieb samospráv bol tento zákon (582/2004 Z. z.) viackrát novelizovaný. Z hľadiska fiškálnej decentralizácie sa však považuje za jeden z kľúčových zákonov upravujúcich ich finančný systém. Skutočnosť, že sa samosprávam umožnilo samostatne rozhodovať o výške jednotlivých daňových sadzieb, sa odstránil predchádzajúci „daňový mantinelizmus“, ktorý do značnej miery ovplyvňoval daňový výnos a tým aj výšku príjmov rozpočtov miest a obcí.

Najvýznamnejšou miestnou daňou, ktorú predmetný zákon upravuje, je daň z nehnuteľností, ktorá zahŕňa daň z pozemkov, daň zo stavieb a daň z bytov.

Spôsob zdaňovania nehnuteľností nezaznamenal v priebehu procesu fiškálnej decentralizácie výrazné zmeny, aj keď registrujeme v tejto súvislosti viac ako 40 novelizácií zákona o miestnych daniach. Uskutočnili sa viac-menej „kozmetické úpravy“ zákona súvisiace so znížením alebo zvýšením počtu skupín nehnuteľností či s redukovaním výšky maximálnej daňovej sadzby, ktorú môže samospráva určiť vo všeobecne záväznom nariadení. Napríklad, v rámci dane z pozemkov sa pri rozdelení pozemkov do skupín znížil počet z 8 skupín v roku 2005 na 5 skupín v roku 2025; pri dani zo stavieb sa naopak predmet dane postupne rozšíril. Kým v roku 2005 boli stavby rozdelené do 7 skupín, v roku 2025 ich máme 9. Pribudli stavby hromadných garáží a stavby hromadných garáží umiestnených pod zemou. Na druhej strane, možnosť samospráv určiť najvyššiu ročnú sadzbu dane z pozemkov do výšky 20-

⁶ NEUBAUEROVÁ, Erika: Fiškálne aspekty decentralizácie verejnej správy. Bratislava : Ekonóm, 2003. s. 72. - ISBN 80-225-1711-9

násobku a pri dani zo stavieb až do výšky 40-násobku najnižšej ročnej sadzby určenej správcom dane vo všeobecne záväznom nariadení (v zmysle novely zákona č. 517/2005 Z. z.), bola postupne zredukovaná na aktuálne platný 10-násobok . V prípade pozemkov, ktoré sú funkčne spojené so stavbou jadrového zariadenia, nesmie ročná sadzba dane presiahnuť 100-násobok ročnej sadzby dane z pozemkov (0,25 %).

Daň z pozemkov sa určuje ako súčin základu dane (výmera pozemku x všeobecná hodnota pozemku) a stanovenej daňovej sadzby, pričom sa výpočet základu dane líši v závislosti od druhu pozemku, ktorý je predmetom zdanenia (rôzne sa stanovuje všeobecná hodnota majetku). Pri väčšine druhov je všeobecná hodnota pozemku stanovená v rámci predmetného zákona, nemá však nič spoločné s „trhovou“ cenou. Výnimkou sú lesné pozemky, rybníky a hospodársky využívané plochy, kde sa všeobecná hodnota určuje na základe vyhlášky Ministerstva spravodlivosti Slovenskej republiky č. 492/2004 o stanovení všeobecnej hodnoty majetku.

Pri určení výšky dane zo stavieb sa vychádza najmä zo zastavanej plochy a z počtu nadzemných aj podzemných podlaží stavby. Výmera podlahovej plochy je kľúčová aj pri zdaňovaní bytov. V ostatnom období sa čoraz viac diskutuje o možnostiach zvýšiť rozpočtové príjmy práve z týchto daní, zavedením napr. cenových máp, ktoré by odrážali potenciál nehnuteľností priniesť do rozpočtov samospráv viac zdrojov v nadväznosti na ich polohu v rámci danej samosprávy či vyšším zdanením druhej, tretej a ďalších nehnuteľností. V tejto súvislosti sa žiada poznamenať, že už v minulosti (do roku 2004) existoval v rámci zákona o dani z nehnuteľností tzv. koeficient polohovej renty, ktorý zvyšoval výšku daňových povinností obyvateľov samospráv podľa toho, či vlastnili nehnuteľnosť v Bratislave, v krajskom meste, v okresnom meste alebo v obci s nižším počtom obyvateľov. V neposlednom rade, aj súčasný zákon o miestnych daniach ponúka možnosť správcom dane z nehnuteľností podľa miestnych podmienok v obci alebo v jej jednotlivých časti alebo v jednotlivom katastrálnom území znížiť alebo zvýšiť ročnú sadzbu dane – tak pri pozemkoch, ako aj pri stavbách a bytoch. (§8 ods. 2, §12 ods. 2, § 16 ods. 2).

Možné zmeny systému zdaňovania nehnuteľností je však potrebné poňať systémovo a koncepčne. Podľa analytikov UMB⁷, v európskom kontexte patríme ku krajinám s najnižším zdanením nehnuteľností. V porovnaní k veľkosti ekonomiky sú len tri krajiny, ktoré majú nižšie výnosy z dane z nehnuteľností – Litva, Česká republika a Estónsko. Aby sme dosiahli priemer Európskej únie, museli by sme mať výnos z týchto daní takmer päťnásobne vyšší. K reforme dane z nehnuteľností však treba

⁷ Bližšie pozri: Analytici NBS: Od podlahy k hodnote – zdaňovanie nehnuteľností na Slovensku. Analytický komentár č. 138. NBS: 30.7.2024. Dostupné na: <https://nbs.sk/dokument/5ff9ca50-6015-455a-abf1-135442ae29ed/stiahnut?force=false>

prístupovať s ohľadom na špecifiká a historické zvyklosti Slovenska, čo si bude vyžadovať starostlivé nastavenie systému, predovšetkým v jeho začiatkoch.

Okrem dane z nehnuteľností upravuje zákon o miestnych daniach aj ostatné miestne dane, ktoré sa pretransformovali na miestne dane z miestnych poplatkov.

Transformácia miestnych poplatkov na miestne dane súvisela najmä s celkovou snahou vtedajšej vlády zjednodušiť daňovo-odvodový systém v rámci reformných procesov, ktorých súčasťou bola aj fiškálna decentralizácia. Udiali sa tieto zmeny:

- na miestne dane sa pretransformovali tieto miestne poplatky: miestny poplatok za psa, miestny poplatok za užívanie verejného priestranstva, miestny poplatok za predajné automaty, miestny poplatok za nevýherné hracie prístroje, miestny poplatok za vjazd a zotrvanie motorového vozidla v historickej časti mesta, miestny poplatok za jadrové zariadenie;
- miestny poplatok za ubytovaciu kapacitu a miestny poplatok za kúpeľný a rekreačný pobyt boli zlúčené do dane za ubytovanie;
- zrušené boli tieto poplatky: miestny poplatok z reklamy, miestny poplatok zo vstupného, miestny poplatok z predaja tabakových výrobkov a alkoholických nápojov a miestny poplatok za užívanie bytu alebo časti bytu na iné účely ako na bývanie.

V rámci legislatívnej úpravy zostal v zákone o miestnych daniach zachovaný len miestny poplatok za komunálne odpady a drobné stavebné odpady, nakoľko ako jediný má charakter tzv. užívateľského poplatku, teda poplatku, ktorého platením sa užívatelia verejného statku – v tomto prípade služby odvozu a likvidácie odpadu – podieľajú na úhrade nákladov, ktoré sú s touto službou spojené. Podľa ekonomickej klasifikácie rozpočtovej klasifikácie je tento poplatok zaradený do skupiny daní za špecifické služby.

Sústavu miestnych daní teda v súčasnosti (2025) tvoria: daň z nehnuteľností (daň z pozemkov, daň zo stavieb, daň z bytov), daň za psa, daň za užívanie verejného priestranstva, daň za ubytovanie, daň za predajné automaty, daň za nevýherné hracie prístroje, daň za vjazd a zotrvanie motorového vozidla v historickej časti mesta, daň za jadrové zariadenie a miestny poplatok za komunálne odpady a drobné stavebné odpady.

Zákonom o miestnych daniach bola upravená aj daň z motorových vozidiel, ktorú mohli ukladať vyššie územné celky. Vplyvom viacerých faktorov, ktoré ovplyvnili proces fiškálnej decentralizácie, sa výnos dane z motorových vozidiel stal od roku 2016 v plnej výške príjmom štátneho rozpočtu (bližšie v ďalšom texte).

Miestne poplatky

Ako už bolo vyššie spomenuté, miestne poplatky v podobe, v akej sme ich poznali do roku 2004, boli zrušené alebo boli pretransformované na miestne dane. Neznamená

to však, že samospráva už nemôže mať príjmy z iných druhov poplatkov. Tieto sú však zaradené do kategórie nedaňových príjmov, v prevažnej miere majú charakter administratívnych a iných poplatkov a platieb. Ide napr. o správne poplatky, poplatky a platby z nepriemyselného a náhodného predaja a služieb (za predaj výrobkov, tovarov a služieb – reklama v obecných novinách, odvysielané relácie v miestnom rozhlase, služby v domovoch smútku atď.), poplatky za jasle, materské školy, školské kluby detí a mnohé ďalšie.

V tejto súvislosti si dovoľíme ešte jednu poznámku. V teoretickej rovine považujeme daň za zákonom stanovenú, spravidla pravidelne sa opakujúcu peňažnú platbu, ktorá plynie do rozpočtu niektorého zo subjektov verejnej správy, a to bez priameho protiplnenia. Na druhej strane, oproti poplatku, ktorý je spravidla jednorazový a poplatník ho platí za nejakú konkrétnu službu, sa očakáva určité protiplnenie. Ak však vychádzame z ekonomickej klasifikácie rozpočtovej klasifikácie, niektoré poplatky sú zaradené do kategórie 100 Daňové príjmy (133 Dane za špecifické služby), čo môže spôsobiť určitú nepresnosť pri používaní správneho terminologického aparátu. Ide napríklad o miestny poplatok za komunálne odpady a drobné stavebné odpady (upravený zákonom č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku za komunálne odpady a drobné stavebné odpady) a o poplatok za rozvoj, upravený samostatným zákonom č. 447/2015 Z. z. o miestnom poplatku za rozvoj a o zmene a doplnení niektorých zákonov.

	mesto	2017	2018	2019	2020	2021	2022	2023	2024
1	Bánovce nad Bebravou								x
2	Banská Bystrica							x	x
3	Banská Štiavnica								x
4	Bardejov							x	x
5	Bratislava	x	x	x	x	x	x	x	x
6	Dunajská Streda				x	x	x	x	x
7	Galanta				x		x	x	x
8	Hlohovec		x	x	x	x	x	x	x
9	Košice				x	x	x	x	x
10	Krupina								x
11	Malacky	x	x	x	x	x	x	x	x
12	Martin								x
13	Nitra				x	x	x	x	x
14	Nové Mesto nad Váhom				x	x	x	x	x
15	Pezinok	x	x	x	x	x	x	x	x
16	Piešťany				x	x	x	x	x
17	Poprad				x	x	x	x	x
18	Prešov								x
19	Ružomberok								x
20	Sabinov								x
21	Senec	x	x	x	x	x	x	x	x
22	Senica				x	x	x	x	x
23	Skalica	x	x	x	x	x	x	x	x
24	Šaľa				x	x	x	x	x

25	Trenčín							x
26	Trnava	x	x	x	x	x	x	x
27	Tvrdošín							x
28	Zlaté Moravce						x	x
29	Žilina						x	x

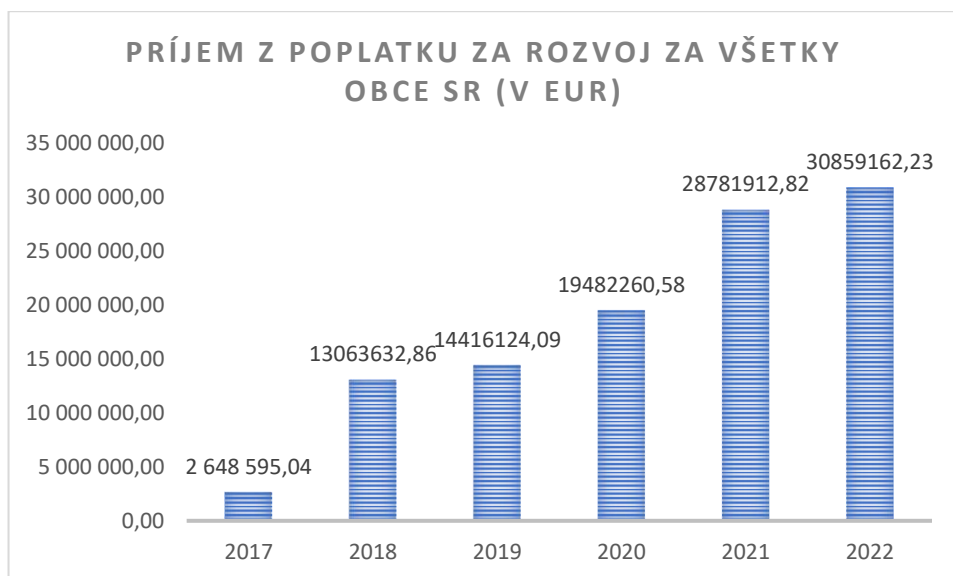
Tabuľka č. 1
Zavádzanie poplatku za rozvoj v okresných a krajských mestách

Za významnú zmenu v oblasti poplatkov môžeme považovať zavedenie poplatku za rozvoj (november 2016)⁸. Pohľad na postupné zavádzanie poplatku za rozvoj vo vybraných mestách ponúka tabuľka č. 1.

Prvotným zámerom jeho zavedenia bolo, aby sa na miestach, kde na základe stavebného rozvoja územia vznikne potreba vybudovania sociálnej a technickej infraštruktúry, dala využiť jeho príjmová, rozvojová, ale aj protikorupčná funkcia. Legislatíva tak umožnila samosprávam získavať ďalšie rozpočtové zdroje využiteľné na rozvoj spravovaného územia. Výnosy z tohto poplatku však môžu byť použité iba na pokrytie kapitálových výdavkov súvisiacich so stavebnými nákladmi na stavbu vrátane nákladov na vysporiadanie pozemku, resp. súvisiacich s kúpou nehnuteľnosti slúžiacej na zákonom vymedzené účely (napr. zariadenia starostlivosti o deti, zariadenia slúžiace na poskytovanie sociálnych, športových a kultúrnych služieb, zariadenia sociálneho bývania, školy, školské zariadenia, zdravotnícke zariadenia atď.). Jedným z opatrení na zmiernenie dôsledkov pandémie Covid-19 bola možnosť obcí do konca roka 2020 využívať príjmy z miestneho poplatku za rozvoj na pokrytie bežných výdavkov miestnej samosprávy.⁹ Tento poplatok je schválený všeobecne záväzným nariadením, výlučne miestnymi samosprávnymi orgánmi a platí len na území obce. Trend vývoja výnosu tohto poplatku zachytáva Obrázok č. 1.

⁸ Zákon NR SR č. 447/2015 Z. z. o miestnom poplatku za rozvoj a o zmene a doplnení niektorých zákonov.

⁹ ČERNĚNKO, Tomáš – NEUBAUEROVÁ, Erika – ZUBALOVÁ, Alena: Impact of the COVID-19 Pandemic on the Budget of Slovak Local Governments: Much Cry and Little Wool? In: Scientific papers of the University of Pardubice [elektronický zdroj]. Series D. - Pardubice : Fakulta ekonomicko-správní Univerzity of Pardubice, 2021. - ISSN 1804-8048. - Vol. 29, no. 1 (Special Issue) (2021), pp. [1-14.] online.



Obrázok č. 1

Príjem poplatku za rozvoj za všetky obce SR

Zdroj: NKÚ SR¹⁰. Vlastné spracovanie.

Je však nutné poznamenať, že aj v tejto oblasti ešte stále existujú významné rezervy. Zo 64 okresných miest tento poplatok v roku 2024 nevyberalo 49 z nich a 7 okresných miest ho prvý krát vybralo až v roku 2024. V prípade krajských miest je situácia podobná. Z ôsmich krajských miest v roku 2022 poplatok za rozvoj vyberali len štyri mestá, v roku 2023 to bolo šesť miest a posledné dve krajské mestá sa pridali až v roku 2024.¹¹

Dňa 1.11.2025 nadobúda účinnosť zákon č. 144/2025 Z. z., ktorým sa mení a dopĺňa zákon č. 447/2015 Z. z. o miestnom poplatku za rozvoj a zároveň sa dopĺňa nový Stavebný zákon č. 25/2025 Z. z. v znení zákona č. 77/2025. Táto novela prináša viacero zmien, ktoré by mohli byť v súvislosti s predmetným poplatkom významné. Zvyšuje sa sadzba poplatku z 3 eur – 35 eur na 5 eur – 50 eur a zároveň je umožnené samosprávam znížiť sadzbu tohto poplatku až o 75 % pre stavby umiestnené v priemyselných parkoch, čo vytvára priestor pre ciele investičné stimuly. Zavádza sa tiež tzv. inflačný koeficient, na základe ktorého sa sadzba miestneho poplatku

¹⁰ NKÚ SR: Aktuality. Poplatok za rozvoj obciam pomáha, nevyužívajú ho ale ani všetky krajské mestá. Bratislava: 4. augusta 2023. Dostupné na: https://www.nku.gov.sk/aktuality/-/asset_publisher/OkVQsC5cs53F/content/poplatok-za-rozvoj-obciam-pomaha-nevyuzivaju-ho-ale-ani-vsetky-krajske-mesta

¹¹ Slovensko sa člení na 79 okresov, pričom Bratislava má 5 okresov a Košice 4. To predstavuje 72 „okresných“ miest. Z nich je 8 sídlom samosprávneho kraja, čiže v konečnom dôsledku máme 8 krajských a 64 okresných miest.

bude každoročne automaticky upravovať podľa vývoja inflácie. Novela rozširuje aj možnosti samospráv využiť výnosy tohto poplatku, a to nie len na tradičnú technickú infraštruktúru, ale aj na environmentálne opatrenia, podporu zelenej infraštruktúry či vypracovanie územnoplánovacích dokumentácií. V neposlednom rade sa posilňuje aj transparentnosť hospodárenia s výnosmi z poplatku.

Podiely na centrálne vyberaných daniach

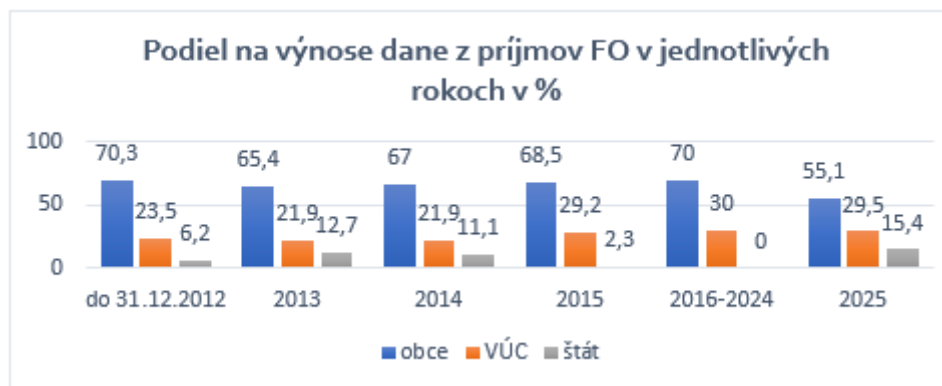
Podiely na centrálne vyberaných daniach, hovorovo tiež podielové dane, sa z hľadiska finančného hospodárenia samospráv chápu ako ich vlastné daňové príjmy. Do roku 2004 existovali na Slovensku tri podielové dane: daň z príjmov fyzických osôb zo závislej činnosti a funkčných požitkov, daň z príjmov právnických osôb a cestná daň. Po zohľadnení princípov fiškálnej decentralizácie sa jedinou podielovou daňou stala daň z príjmov fyzických osôb ako celok (okrem dane vyberanej zrážkou). Rozhodlo sa, že na jej výnose budú participovať samosprávy na obidvoch stupňoch, teda obce aj vyššie územné celky. Pomerne malá časť výnosu sa plánovala ponechať v štátnom rozpočte ako rezerva vlády.

Výhodami systému podieľania sa nižších vládnych úrovní na výnose jednej dane sú transparentnosť, ľahšia dlhodobá prognóza výberu dane a možnosť dlhodobého finančného plánovania. Na druhej strane, existuje aj niekoľko nevýhod: príjmy samospráv sú závislé od výnosu jedinej dane – riziko vyššej volatility príjmov, nemožnosť samospráv stanoviť základ a sadzbu dane, daň z príjmov môže podliehať politicky motivovaným zmenám, nestabilita zákona o dani z príjmov – napr. od prijatia zákona č. 595/2003 o dani z príjmov zo 4. decembra 2003 bolo **do roku 2025 cca 135 novelizácií** tohto zákona.

Okrem zákona č. 564/2004 Z. z. o rozpočtovom určení výnosu dane z príjmov územnej samosprávy a o zmene a doplnení niektorých zákonov, zohráva významnú úlohu v procese fiškálnej decentralizácie aj nariadenie vlády č. 668/2004 Z. z. o rozdeľovaní výnosu dane z príjmov územnej samosprávy v znení neskorších predpisov. Toto nariadenie rozpracováva rozpočtové určenie, kritériá, spôsob rozdeľovania a poukazovania výnosu dane z príjmov FO s výnimkou dane z príjmov, ktorá sa vyberá zrážkou. Určuje kritériá rozdelenia výnosu dane medzi jednotlivé subjekty verejnej správy. Nariadenie vychádza zo samosprávnych kompetencií a ich objemu, nadväzuje na objem transformovaných zdrojov určuje váhy rozdelenia výnosu medzi jednotlivé kritériá.

Obrázok č. 2 prezentuje vývoj percentuálnych podielov jednotlivých subjektov verejnej správy na výnose dane z príjmov FO. Prakticky až do roku 2012 bol tento podiel stabilizovaný vo výške 70,3 % podielu na DPFO pre obce, 23,5 % pre VÚC a 6,2 % si ponechával ako rezervu štát. Krízové vplyvy rokov 2008-2010, najmä zvýšenie nezamestnanosti, mali za následok zníženie objemu výnosu DPFO, čo determinovalo

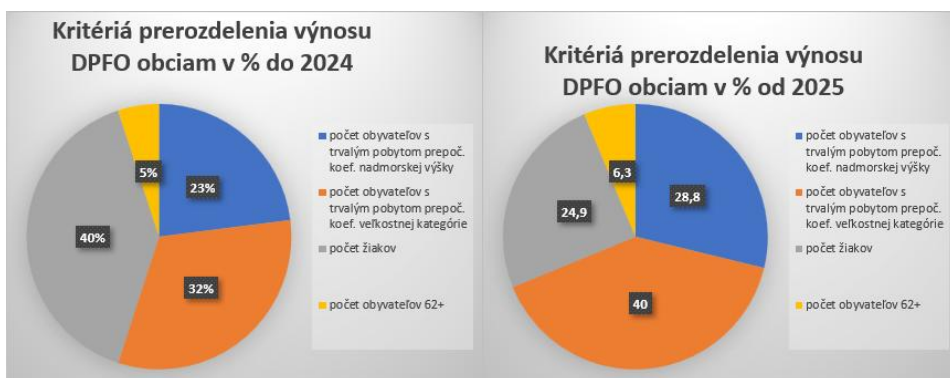
prehodnotenie nastaveného systému a viedlo k postupným zmenám percentuálnych podielov samosprávy na výnose dane. V konečnom dôsledku sa podiel na dani ustálil vo výške 70 % pre obce a 30 % pre vyššie územné celky. Takto stanovený podiel platil od roku 2016 až do roku 2024, aj keď bol sprevádzaný zmenou rozpočtového určenia dane z motorových vozidiel v neprospech VÚC. Spomínaná daň sa stala od roku 2016 príjmom štátneho rozpočtu.



Obrázok č. 2

Vývoj percentuálnych podielov na výnose dane z príjmov FO

Ostatná zmena rozpočtového určenia DPFO sa udiala v roku 2025. V súvislosti so zmenou financovania regionálneho školstva a aj konsolidáciou verejných financií bol percentuálny podiel na dani z príjmov FO znížený obciam na 55,1 %, vyšším územným celkom na 29,5 %, čo vytvorilo priestor na participáciu štátu na výnose tejto dane, konkrétne vo výške 15,4 %. Je však potrebné poznamenať, že sa popri tom zmenil aj systém financovania regionálneho školstva, čo túto zmenu vysvetľuje. Zámerom nie je znížiť samospráve objem prostriedkov na financovanie školstva, ktoré je v jej kompetencii, ale v zásade dohliadnuť a zabezpečiť, aby sa prostriedky určené na financovanie vzdelávania reálne do školstva aj dostali. Rozpočtový systém totiž funguje o. i. na princípe jednotnosti rozpočtu, čo znamená, že neexistuje priama účelová väzba medzi konkrétnym druhom príjmu a konkrétnym druhom výdavku. Znamená to, že všetky príjmy, ktoré samospráva má (vrátane výnosu DPFO), môže použiť na zabezpečenie svojich výdavkov podľa „vlastného uváženia“.



Obrázok č. 3

Zmena percentuálneho podielu prerozdeľovacích kritérií – obce

Táto zmena mala zásadný vplyv aj na zmenu prerozdeľovacích kritérií medzi jednotlivé samosprávy na miestnej úrovni. Percentuálnu zmenu jednotlivých prerozdeľovacích kritérií pre obce, platnú do roku 2024 a od roku 2025, zachytáva obrázok č. 3. Percentuálna váha kritérií prerozdelenia výnosu DPFO pre VÚC sa nemenila.

Záver

V dvadsať rokov trvajúcom procese fiškálnej decentralizácie zohralo svoju úlohu viacero vplyvov. Vstup Slovenskej republiky do Európskej únie znamenal nevyhnutnosť prehodnotenia existujúcej slovenskej daňovej sústavy, ktorá by sa približovala európskym štandardom – miestne dane nevynímajúc. Dopady finančnej krízy rokov 2008 – 2010 rozprúdili diskusie najmä v súvislosti so systémom existencie jedinej podielovej dane – dane z príjmov fyzických osôb, intenzívne sa hovorilo o prípadných možnostiach vytvorenia efektívnejšieho daňového mixu. Zmeny makroekonomického prostredia, ale aj mnohé ďalšie vplyvy viedli k viacerým úpravám a novelizáciám legislatívy súvisiacej s finančným systémom samospráv. V súčasnosti sa azda viac, ako kedykoľvek predtým, dostávajú samosprávy do pozície, kedy by mali využiť svoj potenciál v oblasti finančného manažmentu. Aj napriek tomu, že sa čoraz intenzívnejšie diskutuje o efektívnejšom finančnom systéme samospráv (napr. zmeny v zdaňovaní nehnuteľností so zohľadnením hodnoty nehnuteľnosti), už dnes existujú viaceré legislatívne možnosti, ktoré môže samospráva využiť a podporiť tým zvýšenie svojej príjmovej základne (napr. prostredníctvom daňovej právomoci v rámci miestnych daní). Na druhej strane, osobitnú analýzu by si zaslúžili aj zmeny finančných tokov smerujúcich od štátu k územnej samospráve, a to najmä prostredníctvom podielových daní. Ukazuje sa, že súčasný systém prerozdelenia má za úlohu hlavne korigovať regionálne a miestne disparity. V kontexte meniaceho sa makroekonomického prostredia a nových

európskych trendov smerovania miestnych samospráv k zvýšenej efektívnosti hospodárenia, by mal byť tento systém transparentnejší a postupne smerovať k podpore konkurencieschopnosti samospráv pri poskytovaní miestnych verejných služieb, s čím súvisí optimálne nastavenie finančných tokov založené o. i. aj na princípe zásluhovosti samospráv na tvorbe objemu finančných prostriedkov určených na prerozdeľovanie.

Zoznam použitej literatúry

1. BARTOLINI David, STOSSBERG Sibylle, BLÖCHLIGER Hansjörg: Fiscal Decentralisation and Regional Disparities. OECD Economics Department Working Papers No. 1330, 2016. <https://dx.doi.org/10.1787/5jlpq7v3j237-en>
2. ČERNĚNKO, Tomáš – NEUBAUEROVÁ, Erika – ZUBALOVÁ, Alena: Impact of the COVID-19 Pandemic on the Budget of Slovak Local Governments: Much Cry and Little Wool? In: Scientific papers of the University of Pardubice [elektronický zdroj]. Series D. - Pardubice : Fakulta ekonomicko-správní Univerzity of Pardubice, 2021. - ISSN 1804-8048. - Vol. 29, no. 1 (Special Issue) (2021), pp. [1-14] online.
3. KLIMOVSÝ, Daniel: Základy verejnej správy. Košice: UPJŠ v Košiciach, 2008. 269 strán. ISBN 978-80-7097-713-2.
4. NEUBAUEROVÁ, Erika: Fiškálne aspekty decentralizácie verejnej správy. Bratislava : Ekonóm, 2003. - 168 s. - ISBN 80-225-1711-9
5. Nariadenie vlády č. 668/2004 Z. z. o rozdeľovaní výnosu dane z príjmov územnej samosprávy v znení neskorších predpisov
6. Vyhláška Ministerstva spravodlivosti Slovenskej republiky č. [492/2004 Z. z.](#) o stanovení všeobecnej hodnoty majetku.
7. Zákon NR SR č. 447/2015 Z. z. o miestnom poplatku za rozvoj a o zmene a doplnení niektorých zákonov.
8. Zákon NR SR č. 564/2004 Z. z. o rozpočtovom určení výnosu dane z príjmov územnej samosprávy v znení neskorších predpisov
9. Zákon NR SR č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku za komunálne odpady a drobné stavebné odpady v znení neskorších predpisov.
10. NKÚ SR: Aktuality. Poplatok za rozvoj obciam pomáha, nevyužívajú ho ale ani všetky krajské mestá. Bratislava: 4. augusta 2023. Dostupné na: https://www.nku.gov.sk/aktuality/-/asset_publisher/OkVQsC5cs53F/content/poplatok-za-rozvoj-obciam-pomaha-nevyuzivaju-ho-ale-ani-vsetky-krajske-mesta
11. Analytici NBS: Od podlahy k hodnote – zdaňovanie nehnuteľností na Slovensku. Analytický komentár č. 138. NBS: 30.7.2024. Dostupné na:

<https://nbs.sk/dokument/5ff9ca50-6015-455a-abf1-135442ae2ged/stiahnut?force=false>

Kontaktné údaje

doc. Ing. Erika Neubauerová, PhD.

erika.neubauerova@flaw.uniba.sk

Právnická fakulta, Univerzita Komenského v Bratislave

doc. Mgr. Ing. Tomáš Černěňko, PhD.

tomas.cernenko@euba.sk

Národohospodárska fakulta, Ekonomická univerzita v Bratislave

FIŠKÁLNA DECENTRALIZÁCIA NA SLOVENSKU – DOPADY ZMENY FINANCOVANIA MATERSKÝCH ŠKÔL NA ROZPOČTY MIESTNYCH SAMOSPRÁV¹

FISCAL DECENTRALISATION IN SLOVAKIA - IMPACTS OF CHANGES IN KINDERGARTEN FINANCING ON LOCAL GOVERNMENT BUDGETS

Tomáš Černěňko², Erika Neubauerová³

Abstrakt: Fiškálna decentralizácia mala priniesť samospráve možnosti zvýšenia kontroly nad vlastnými príjmami. Napriek tomu sa od jej zavedenia samospráve hneď niekoľkokrát zmenili pravidlá hry – najčastejšie spôsob prerozdelenia dane z príjmu fyzických osôb, ktorá predstavuje najvýznamnejší časť príjmov mnohých samospráv. Rovnakým smerom sa vybrala aj ostatná zmena, ktorá bola vyvolaná zmenou financovania materských škôl – presunom „neadresných“ finančných prostriedkov poukazovaných obciam na adresný normatívny príspevok, ktorý podobne ako v prípade financovania základných škôl nasleduje konkrétneho žiaka. Cieľom príspevku je analyzovať vplyv tejto zmeny vo financovaní miestnej samosprávy – financovaním materských škôl prostredníctvom normatívneho príspevku – na rozpočty miestnych samospráv. Analýza vplyvu vychádza z porovnania medzироčnej zmeny príjmu všetkých obcí, ktorú následne skúma ako všeobecne tak aj z pohľadu obcí, ktoré materské školy prevádzkujú a tých, ktoré tak nerobia. Zmeny príjmov obcí sú skúmané na úrovni veľkostných kategórií obcí a ich zastúpenia v jednotlivých krajocho Slovenska. Výsledkom je zistenie, že zmena spôsobu financovania materských škôl nespôsobila výrazné zmeny v celkových príjmoch miestnej samosprávy.

Kľúčové slová: fiškálna decentralizácia, miestna samospráva, materské školy, normatívny príspevok

¹ Príspevok je spracovaný v rámci projektu APVV – 22 – 0482 „Financovanie územnej samosprávy – potenciál funkčných mikroregiónov“

² Katedra verejnej správy a regionálneho rozvoja, Národohospodárska fakulta, Ekonomická univerzita v Bratislave

³ Ústav ekonomických vied, Právnická fakulta, Univerzita Komenského v Bratislave

Abstract: Fiscal decentralisation was supposed to give local governments the opportunity to increase control over their own revenues. Nevertheless, since its introduction, the rules of the game have changed several times for local governments – most often the way of redistributing personal income tax, which represents the most significant part of the revenues of many local governments. The other change that was triggered by the change in the financing of kindergartens – the transfer of “non-targeted” funds transferred to municipalities to a targeted normative contribution, which, like the case of primary school financing, follows a specific pupil. The aim of the paper is to analyse the impact of this change in the financing of local governments – by financing kindergartens through a normative contribution – on the budgets of local governments. The impact analysis is based on a comparison of the year-on-year change in the income of all municipalities, which is subsequently examined both in general and from the perspective of municipalities that operate kindergartens and those that do not. Changes in municipal revenues are examined at the level of size categories of municipalities and their representation in individual regions of Slovakia. The result is that the change in the method of financing kindergartens did not cause significant changes in the total revenues of local governments.

Key words: fiscal decentralization, local government, kindergartens, normative contribution

Úvod

Pred 20 rokmi boli v rámci fiškálnej decentralizácie znovunastavené základné princípy financovania miestnej samosprávy. Cieľom bolo posilniť jej nezávislosť a zbaviť ju v oblasti financií závislosti na politickom rozhodovaní. Základným princípom bolo určenie daní, ktorých výnos bude prináležať miestnej samospráve a daní a poplatku(ov), ktoré budú plne v gescii územnej samosprávy. Napriek tomu došlo od roku 2005 k viacerým zásahom, ktoré vtedy nastavený systém financovania upravili.

Jednou z posledných výrazných zmien bolo vyňatie financovania materských škôl z príspevku, ktorý bol obciam poskytovaný z výnosu dane z príjmov fyzických osôb (ďalej DPFO) a jeho transformácia na normatívny príspevok. Toto rozhodnutie je výsledkom implementácie reforiem v rámci Plánu obnovy a odolnosti SR (komponent 6, Reforma 1).

Kedže podiel na DPFO predstavuje pre mnohé obce najvýznamnejšiu časť príjmov⁴ sú ich obavy ohľadom dopadov takejto výraznej zmeny na príjmy miest a obcí pochopiteľné. Cieľom nášho príspevku je preto analyzovať vplyv tejto zmeny vo financovaní miestnej samosprávy na rozpočty miestnych samospráv.

V čom spočíva zmena a prečo je dôležitá

Ako sme uviedli vyššie, základnou zmenou je zníženie podielu DPFO, ktorý bude prerozdelený medzi samosprávy zo 70% (do 31.12.2024) na 55,1% (od 1.1.2025)⁵. Vo finančnom vyjadrení to predstavuje pri výnose DPFO z roku 2024 2,647 mld. € pri 70% a 2,084 mld. € pri 55,1% (platné od 1.1.2025). Rozdiel medzi jednotlivými podielmi DPFO je 563 mil. €, čo môžeme pokladať za výšku, ktorú mali miestne samosprávy vynaložiť na poskytovanie služieb predprimárneho vzdelávania.

Ak spravíme rovnaký prepočet s predpokladaným podielom DPFO určeným miestnej samosprávou v roku 2025, dostaneme pri podiele 70% 2,848 mld. € a pri 55,1% podiele 2,242 mld. €, čo predstavuje rozdiel vo výške 606 mil. €.

Vo výsledku však obce dostali v rámci normatívnych príspevkov od Ministerstva školstva, výskumu, vývoja a mládeže SR poukázaných 654 mil. €, čo predstavuje o 7,9% viac, ako by tomu bolo bez zmeny legislatívy. To však neznamená, že sa tieto prostriedky v rovnakom pomere dostanú aj k jednotlivým samosprávam a naša výskumná otázka (cieľ príspevku) preto ostáva aj naďalej platná.

Černěňko a Neubauerová⁶ ukazujú, že v prípade materských škôl v Bratislave veľmi často dochádza k „nesúladu“ medzi spádovou materskou školou a miestom kde dieťa v skutočnosti materskú školu navštevuje často naprieč jednotlivými mestskými časťami, ktoré sú zriaďovateľmi prevažnej väčšiny materských škôl. K tomu je potrebné pripočítať, že v mnohých prípadoch (mestských časti) sa ako kritérium pre prijatie dieťaťa do materskej školy posudzuje aj trvalý pobyt dieťaťa a rodičov. V prípade mestskej časti Ružinov bolo (v roku 2023) na trvalý pobyt naviazaných 10 z 22 bodov, ktoré mohlo dieťa počas rozhodovania o zaradení do materskej školy získať. Vzhľadom na pôvodný spôsob financovania materských škôl (súčasť podielu

⁴ ČERNĚŇKO, Tomáš – NEUBAUEROVÁ, Erika – ZUBALOVÁ Alena: Impact of the COVID-19 Pandemic on the Budget of Slovak Local Governments: Much Cry and Little Wool? In: Scientific papers of the University of Pardubice. Series D. - Vol. 29, no. 1 (Special Issue) 2021

⁵ Dôvodová správa k zákonu č. 290/2024 Z.z. predpokladala zníženie podielu DPFO poukázaného obciam na 56,1%. V článku uvedených 55,1% je dôsledkom novelizácie zákonom č. 278/2024 Z.z. (Zákon, ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s ďalším zlepšovaním stavu verejných financií).

⁶ ČERNĚŇKO, Tomáš – NEUBAUEROVÁ, Erika: Kindergartens in Bratislava - Is There Room for More Value? In: Public Economics and Administration 2023 : Proceedings of the 15th International Scientific Conference : 5th September 2023, Ostrava, Czech Republic. - Ostrava : VSB -Technical University of Ostrava, 2023.

obce na DPFO, ktorý vo veľkej miere staval (a stavia) na počte osôb s trvalým pobytom v obci) je možné toto správanie mestských častí vnímať ako racionálne. Po novom však peniaze idú priamo za dieťaťom (poskytovateľom služby) bez ohľadu na jeho trvalé bydlisko – dopyt a ponuka prestávajú byť závislé na mieste trvalého pobytu dieťaťa alebo rodičov.

Zmena financovania na adresný normatívny príspevok však okrem toho umožňuje aj paradigmatickú zmenu vnímania tejto verejnej služby. Pre samosprávu sa otvára priestor uspokojiť potreby nielen svojich obyvateľov ale aj ľudí, ktorí v ich jurisdikciách pracujú a pomôcť tak k tvorbe lepšieho podnikateľského prostredia a silnejšej miestnej ekonomiky. To si však vyžaduje zmenu doterajšieho spôsobu vnímania poskytovania verejných služieb od zákonnej povinnosti k plneniu cieľa a tvorbe hodnoty pre užívateľov verejných služieb. Tejto paradigmatickej zmene v produkcii verejných služieb sa bližšie venovali napr. Osborne, Radnor a Nasi⁷, Osborne a Strokosch⁸ alebo Osborne⁹.

Poskytovanie tejto verejnej služby tak má možnosť prestať byť politicky motivované a zameriavať sa na zlepšovanie kvality služby a plnenie skutočného (zamýšľaného) cieľa predprimárneho vzdelávania – vzdelávania nie stráženia detí. Ak sa samosprávam podarí túto príležitosť správne uchopiť výsledkom by mala byť lepšia verejná služba (väčšie prekrytie ponuky a dopytu) a teda vyššia spokojnosť obyvateľov.

Dáta a metódy

Údaje

Údaje o príjmoch miestnej samosprávy pochádzajú z Ministerstva financií SR. Jedná sa o Východiskové štatistické údaje a podiel obcí na výnose DPFO pre rok 2025 a Východiskové štatistické údaje a podiel obcí na výnose DPFO pre rok 2024 (prognóza september).

Údaje o pridelených normatívnych prostriedkoch materským školám pochádzajú z Ministerstva školstva, výskumu, vývoja a mládeže SR. Jedná sa o Normatívne určené objemy finančných prostriedkov pre materské školy na rok 2025 (vrátane doplatku garantovaného minima).

⁷ OSBORNE, Stephen – RADNOR, Zoe – NASI, Greta: A new theory for public service management? Toward a (Public) service dominant approach? *The American Review of Public Administration*, 2013

⁸ OSBORNE, Stephen – STROKOSCH, Kirsty: It takes Two to Tango?. *British Journal of Management*, 24: S31-S47. 2013

⁹ OSBORNE, Stephen P. (2018) From public service-dominant logic to public service logic: are public service organizations capable of co-production and value co-creation?, *Public Management Review*, 20:2, 225-231, 2018

Metódy

Údaje o príjmoch miestnej samosprávy za rok 2024 boli použité bez úpravy.

Príjmy miestnej samosprávy za rok 2025 na úrovni jednotlivých obcí boli vypočítané ako súčet agregovaných normatívnych príspevkov pre poskytovateľov predprimárneho vzdelávania na úrovni obcí a podielu príslušnej obce na DPFO.

Následne bola vypočítaná medziročná zmena vo výške príjmu každej jednej obce (v absolútnom a relatívnom vyjadrení).

Vlastná analýza údajov prebiehala podľa kritérií: veľkostná kategória obce, „krajská“ príslušnosť, poskytovateľ služby (áno/nie).

Výsledky

Nasledujúca tabuľka (Tabuľka č. 1) predstavuje podiel obcí v jednotlivých krajoch SR a veľkostných kategóriách, ktoré sú zriaďovateľom materskej školy. Ako je možné vidieť, škôlky zriaďujú vo väčšej miere až obce vo veľkostnej kategórii 501 – 1000 obyvateľov a (takmer) plne prítomné sú vo všetkých obciach väčších ako 1001 obyvateľ. Z pohľadu krajov je najviac obcí, ktoré majú zriadenú materskú školu v Bratislavskom kraji (97%) a najmenej (54%) v Banskobystrickom kraji. Podpriemerné hodnoty (61% a 69%) sú aj v Prešovskom resp. Košickom kraji, ktoré patria spolu s už spomínaným Banskobystrickým krajom k najviac fragmentovaným krajom na Slovensku a zároveň krajom s najvyšším podielom najmenej rozvinutých okresov.

	Banskobystrický kraj	Bratislavský kraj	Košický kraj	Nitriansky kraj	Prešovský kraj	Trenčiansky kraj	Trnavský kraj	Žilinský kraj	spolu
do 250	4%		3%	8%	6%	3%		2%	4%
251 – 500	41%	100%	50%	48%	63%	46%	61%	41%	51%
501 – 1000	89%	90%	87%	96%	93%	88%	93%	90%	91%
1001 – 2000	100%	100%	100%	100%	100%	100%	100%	100%	100%
2001 – 3000	100%	100%	100%	100%	100%	100%	100%	100%	100%
3001 – 4000	100%	100%	100%	100%	94%	100%	100%	100%	99%
4001 – 5000	100%	100%	100%	100%	100%	100%	100%	100%	100%
5001 – 10 000	100%	100%	100%	100%	100%	100%	100%	100%	100%
10 001 – 20 000	100%	100%	100%	100%	100%	100%	100%	100%	100%
20 001 – 50 000	100%	100%	100%	100%	100%	100%	100%	100%	100%
50 001 – 100 000	100%			100%	100%	100%	100%	100%	100%
100 001+		100%	100%						100%
spolu	54%	97%	69%	82%	61%	76%	91%	77%	70%

Tabuľka č. 1

Podiel obcí so škôlkami (podľa krajov a veľkostných kategórií)

V tabuľke 2 (nižšie) uvádzame zmeny príjmov všetkých obcí. Ako môžeme vidieť, k poklesu došlo iba v jednom prípade – Prešovský kraj a obce vo veľkostnej kategórii 4001 – 5000 obyvateľov. Inak vo všetkých sledovaných skupinách obcí, či už podľa krajov alebo veľkostných kategórií došlo k zvýšeniu príjmov obcí. Celoslovensky sa táto hodnota zvýšila o 9,42%, najväčší nárast príjmov¹⁰ (o 15,82%) zaznamenali obce vo veľkostnej kategórii 50 001 – 100 000 obyvateľov. Z pohľadu krajov bol najväčší prírastok v Trnavskom kraji (10,69%). Najväčší nárast príjmov (25,98%) zaznamenali obce v Bratislavskom kraji vo veľkostnej kategórii 251 - 500 obyvateľov.

Podobnú situáciu môžeme vidieť v obciach, ktoré škôlku majú (tabuľka 3, nižšie). Celkový príjem týchto obcí sa medziročne zvýšil o 9,57%, rovnako tak najväčšími beneficiarntami ostávajú obce v Trnavskom kraji a z pohľadu veľkostných kategórií obce vo veľkosti 50 001 – 100 000 obyvateľov.

	Banskobystrický kraj	Bratislavský kraj	Košický kraj	Nitriansky kraj	Prešovský kraj	Trenčiansky kraj	Trnavský kraj	Žilinský kraj	spolu
do 250	5,38%	13,23%	5,47%	13,64%	5,56%	6,52%	5,14%	5,89%	6,04%
251 – 500	6,76%	25,98%	7,97%	6,70%	8,59%	6,97%	12,06%	15,91%	8,61%
501 – 1000	7,95%	12,37%	10,31%	10,40%	9,70%	10,17%	11,94%	13,33%	10,24%
1001 – 2000	8,11%	12,29%	9,68%	9,24%	8,82%	10,97%	10,90%	9,36%	9,66%
2001 – 3000	6,54%	9,68%	7,68%	9,85%	8,13%	9,55%	9,30%	10,32%	8,90%
3001 – 4000	6,19%	16,61%	5,55%	8,44%	15,96%	7,51%	9,49%	11,51%	10,85%
4001 – 5000	7,42%	16,78%	2,92%	6,83%	-0,65%	6,89%	7,68%	10,09%	7,03%
5001 – 10 000	7,52%	10,69%	2,96%	7,38%	8,49%	6,65%	9,20%	6,33%	7,30%
10 001 – 20 000	7,76%	11,24%	8,79%	6,83%	4,56%	7,34%	8,90%	7,90%	7,66%
20 001 – 50 000	6,94%	6,14%	5,46%	7,08%	6,43%	5,72%	6,55%	6,94%	6,42%
50 001 – 100 000	15,54%			15,38%	19,88%	12,55%	19,84%	13,10%	15,82%
100 001+		9,30%	12,64%						10,24%
spolu	8,50%	9,69%	8,95%	9,30%	9,66%	8,47%	10,69%	9,92%	9,42%

Tabuľka č. 2

*Medziročná (2024/2025) zmena príjmu všetkých obcí
(podľa krajov a veľkostných kategórií)*

	Banskobystrický kraj	Bratislavský kraj	Košický kraj	Nitriansky kraj	Prešovský kraj	Trenčiansky kraj	Trnavský kraj	Žilinský kraj	spolu
do 250	9,77%		10,15%	8,16%	6,63%	5,44%		8,64%	10,50%

¹⁰ Príjmami a celkovými príjmami myslíme príjmy z podielu DPFO a normatívneho príspevku

251 – 500	9,85%	25,98%	11,79%	8,52%	10,45%	9,04%	13,84%	23,45%	11,44%
501 – 1000	8,18%	12,39%	10,90%	10,53%	10,45%	10,96%	13,33%	14,19%	10,86%
1001 – 2000	8,11%	12,29%	9,68%	9,24%	8,82%	10,97%	10,90%	9,36%	9,66%
2001 – 3000	6,54%	9,68%	7,68%	9,85%	8,13%	9,55%	9,30%	10,32%	8,90%
3001 – 4000	6,19%	16,61%	5,55%	8,44%	17,34%	7,51%	9,49%	11,51%	11,08%
4001 – 5000	7,42%	16,78%	2,92%	6,83%	-0,65%	6,89%	7,68%	10,09%	7,03%
5001 – 10 000	7,52%	10,69%	2,96%	7,38%	8,49%	6,65%	9,20%	6,33%	7,30%
10 001 – 20 000	7,76%	11,24%	8,79%	6,83%	4,56%	7,34%	8,90%	7,90%	7,66%
20 001 – 50 000	6,94%	6,14%	5,46%	7,08%	6,43%	5,72%	6,55%	6,94%	6,42%
50 001 – 100 000	15,54%			15,38%	19,88%	12,55%	19,84%	13,10%	15,82%
100 001+		9,30%	12,64%						10,24%
spolu	8,77%	9,69%	9,14%	9,40%	10,00%	8,58%	10,81%	10,01%	9,57%

Tabuľka č. 3
Medziročná (2024/2025) zmena príjmu obcí so škôlkami
(podľa krajov a veľkostných kategórií)

	Banskobystrický kraj	Bratislavský kraj	Košický kraj	Nitriansky kraj	Prešovský kraj	Trenčiansky kraj	Trnavský kraj	Žilinský kraj	spolu
do 250	4,93%	13,23%	5,09%	5,67%	5,19%	6,61%	5,14%	5,71%	5,28%
251 – 500	2,77%		1,51%	3,62%	2,72%	3,76%	7,17%	5,75%	3,20%
501 – 1000	4,44%	11,99%	3,90%	5,91%	-3,36%	-0,04%	-14,51%	1,19%	0,59%
1001 – 2000									
2001 – 3000									
3001 – 4000					-11,58%				-11,58%
4001 – 5000									
5001 – 10 000									
10 001 – 20 000									
20 001 – 50 000									
50 001 – 100 000									
100 001+									
spolu	3,88%	12,15%	3,09%	4,39%	1,53%	3,42%	-1,11%	4,59%	3,03%

Tabuľka č. 4
Medziročná (2024/2025) zmena príjmu obcí bez škôlok
(podľa krajov a veľkostných kategórií)

V Tabuľke č. 4 vidíme, že príjmy obcí bez škôlky narástli v priemere o 3,03%. Rovnako tak je vidieť, že v prípade väčšiny sledovaných skupín obcí došlo rovnako tak k nárastu

príjmov. Ako sme už uviedli vyššie, pre zistenie príčin nižšieho alebo dokonca poklesu príjmov obcí je potrebné ďalšie skúmanie.

Záver

Na základe vyššie uvedeného môžeme konštatovať, že zmena výšky poukázaného podielu výnosu dane z príjmu fyzických osôb zo 70% na 55,1% a vnútorná zmena výpočtu podielu jednotlivých obcí na tomto výnose sa spolu so zavedením normatívneho financovania materských škôl (z makro pohľadu) *negatívne nepremietla* do celkovej výšky príjmov obcí. Analýza nevylučuje, že mohlo dôjsť k individuálnym poklesom príjmov jednotlivých miest a obcí z dôvodu reformy (viď tabuľky 2 až 4 vyššie). Medziročné porovnanie príjmov nedokáže izolovať vplyv reformy, nakoľko sa zmiešava vplyv viacerých premenných – štatistické zmeny vstupujúce prerozdeľovania a taktiež medziročne vyšší výber DPFO plynúci z makroekonomického prostredia.

Celkovo príjmy obcí vsledovanom období (medzi rokmi 2024 a 2025) narástli o 9,42%. Vlastné príjmy obcí sa zmenou financovania síce znížili ale boli kompenzované účelovo viazaným transferom. Obce tak prišli o flexibilitu pri nakladaní s finančnými prostriedkami, na druhú stranu však rodičia získali istou garancie minimálnych výdavkov, ktoré bude musieť obec na poskytovanie tejto služby alokovať. Príjmy obcí, ktoré majú škôlku narástli v priemere o 9,57%. Najväčšie prírastky mali obce vo veľkostnej kategórii 50 001 – 100 000 obyvateľov (15,82%).

Rástli však aj príjmy obcí, ktoré škôlku nemajú. Avšak v tomto prípade môžeme hovoriť o medziročnom raste príjmov iba o 3,03%. Z regionálneho pohľadu však vidíme väčšie rozdiely. Obciam bez škôlok v Bratislavskom kraji narástli príjmy o 12,15% kým v Trnavskom kraji došlo k ich poklesu o 1,11%.

Ktorý faktor alebo množina ktorých faktorov sa v akej miere na raste príjmov podieľala nie je na základe našej analýzy možné povedať a preto by bolo vhodné ďalší výskum, ktorý by pracoval s komplexnejšími metódami (napr. difference in differences), smerovať k ich identifikácii. Predpokladáme však, že jedným z faktorov ktorý mal na príjmy obcí vplyv bolo rozhodnutie samospráv či a v akom rozsahu bude služby predprimárneho vzdelávania zabezpečovať. K ďalším faktorom, ktoré neboli predmetom našej analýzy patrí zmena počtu a štruktúry obyvateľov v jednotlivých obciach, ktoré sa na celkových výsledkoch (príjmoch) vzhľadom na samotný mechanizmus prerozdeľovania prirodzene podieľajú.

Najvýraznejšou zmenou v príjmoch miestnej samosprávy sa tak stala ich štruktúra. Z časti vlastných daňových príjmov sa touto zmenou stali transfery. Aj keď je táto zmena pre skutočné poskytovanie služby a jej koncového spotrebiteľa nepodstatná,

zmení postavenie Slovenska v medzinárodných rebríčkoch (porovnovaniach), ktoré sa venujú „finančnej sile“ samospráv.

Aj keď sa tento krok môže na prvý pohľad javiť ako oslabenie finančnej stability samosprávy, nie je to tak. Zmena financovania postavená na normatívnom príspevku umožňuje obciam uchádzať sa o tieto finančné prostriedky na trhu predprimárneho vzdelávania v rámci podnikateľskej činnosti. V prípade, že dokáže poskytovať lepšie služby ako okolité obce alebo obce relevantné pre konečného spotrebiteľa (napr. v mieste bydliska alebo zamestnania) môžu jednoduchším spôsobom získať viac finančných prostriedkov ako tomu bolo predtým. Ak by sa takýto „biznisový“ prístup (produkcie verejných služieb so známou jednotkovou cenou na základe priestorového dopytu) podarilo aplikovať na širšiu skupinu verejných služieb, viedlo by to k úprave počtu ich producentov. To by sa v konečnom dôsledku premietlo do vyššej špecializácie samospráv na produkciu istého typu verejnej služby a optimalizácii využívania dostupných zdrojov v území.

V prípade, že samosprávy takýto krok vyhodnotia ako rizikový alebo z dlhodobého hľadiska nevýhodný, napr. kvôli výkyve v demografickom vývoji¹¹ (ako dôsledok suburbanizácie) ponúka jasne definovaný spôsob financovania služby priestor pre zapojenie partnerov zo súkromného sektora. Obce by tak vedeli na potrebný čas (prechodné obdobie) chýbajúce kapacity (služby) „nakúpiť“ od súkromného poskytovateľa bez rizika umrtnenia kapitálu napr. v budovách pre ktoré následne (vzhľadom na špecifickú architektúru¹²) nebudú schopné nájsť využitie, prípadne bude ich adaptácia na nový účel využitia nákladnejšia.

Normatívne financovanie materských škôl so sebou prinieslo ešte jednu zmenu – okrem naviazania (ďalšej) časti, dovtedy „neutrálnych“ príjmov na konkrétnu skupinu obyvateľov, znížilo trvalo podiel celkovej asignácie výnosu dane z príjmu fyzických osôb bez ohľadu na prípadnú (a v kontexte demografického vývoja očakávanú) zmenu počtu predškôľakov. Obce tak v sumári, vzhľadom na (očakávaný) pokles počtu predškôľakov, dostanú postupne čoraz menší podiel na dani z príjmov fyzických osôb ako tomu bolo pred reformou, pričom zo stávajúceho podielu budú musieť súčasne financovať väčší podiel (objem) služieb pre starnúce obyvateľstvo.

¹¹ V tomto prípade máme na mysli neprirodzenú zmenu štruktúry obyvateľstva najmä zvýšeným prisťahovaním istej skupiny ľudí (napr. mladých, zatiaľ bezdetných) párov či párov s deťmi, ktoré ešte nezačali plniť povinnú predškolskú alebo školskú dochádzku) čo obciam neposkytuje dostatočný priestor reagovať na z toho plynúci zvýšený dopyt po konkrétnej verejnej službe (v našom prípade (a príklade) predprimárneho alebo primárneho vzdelávania). Takéto výkyvy sú lokálneho charakteru a môžeme ich interpretovať ako priestorové odchýlky od všeobecných (celkových) trendov.

¹² Predpokladáme, že obce budú pri výstavbe budov viazaných na produkciu/zabezpečovanie verejných služieb vychádzať z aktuálnych poznatkov a trendov, čo povedie k výstavbe špecifických účelových stavieb, ktoré bude náročnejšie adaptovať na zmenu účelu využitia

Vzhľadom na očakávaný pokles podielu obcí na výnose dane z príjmov fyzických osôb v roku 2026 na 53%¹³ je možné vnímať vyňatie a transformáciu finančných zdrojov na predprimárne vzdelávanie ako (nezamýšľané) pozitívum.

Tento fakt tak pridáva ďalšiu otázku k diskusii o predvídateľnosti a udržateľnosti súčasného modelu financovania miestnej samosprávy. Aj keď zodpovedanie tejto otázky nie je predmetom nášho príspevku, považujeme za dôležité na tento fakt upozorniť.

Zoznam použitej literatúry

1. ČERNĚNKO, Tomáš – NEUBAUEROVÁ, Erika – ZUBALOVÁ, Alena: Impact of the COVID-19 Pandemic on the Budget of Slovak Local Governments: Much Cry and Little Wool? In: Scientific papers of the University of Pardubice. Series D. - Pardubice : Fakulta ekonomicko-správní Univerzity of Pardubice, 2021. - ISSN 1804-8048. - Vol. 29, no. 1 (Special Issue) (2021), pp. [1-14] online.
2. ČERNĚNKO, Tomáš – NEUBAUEROVÁ, Erika: Kindergartens in Bratislava - Is There Room for More Value? In: Public Economics and Administration 2023 : Proceedings of the 15th International Scientific Conference : 5th September 2023, Ostrava, Czech Republic. - Ostrava : VSB -Technical University of Ostrava, 2023. - ISBN 978-80-248-4698-9. - pp. 67-76.
3. OSBORNE, Stephen: From public service-dominant logic to public service logic: are public service organizations capable of co-production and value co-creation?, Public Management Review, 20:2, 225-231, DOI: 10.1080/14719037.2017.1350461
4. OSBORNE, Stephen – RADNOR, Zoe – NASI, Greta: A new theory for public service management? Toward a (Public) service dominant approach? The American Review of Public Administration, 2013 43: 135 DOI: 10.1177/0275074012466935 2012
5. OSBORNE, Stephen – STROKOSCH, Kirsty :It takes Two to Tango?. British Journal of Management, 24: S31-S47. 2013 <https://doi.org/10.1111/1467-8551.12010>
6. Prehľad o výnose dane z príjmov fyzických osôb 2024. Ministerstvo financií SR. Dostupné na <https://www.mfsr.sk/files/archiv/85/Prehľad-o-vynose-dane-z-prijmov-fyzickych-osob-januar-2024.pdf>
7. Prehľad o výnose dane z príjmov fyzických osôb 2025. Ministerstvo financií SR. Dostupné na <https://www.mfsr.sk/files/archiv/4/Prehľad-o-vynose-dane-z-prijmov-FO-januar-2025.pdf>
8. Východiskové štatistické údaje a podiel obcí na výnose DPFO pre rok 2024 (prognóza september). Ministerstvo financií SR. Dostupné na

¹³ Novelizácia Zákona č. 564/2004 Z.z. zákonom 261/2025 Z.z. (Zákon, ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s konsolidáciou verejných financií)

https://www.mfsr.sk/files/archiv/51/Vychodiskove_statisticke_udaje_podiel_obce_proгноza_jun_2024_sept.pdf

9. Východiskové štatistické údaje a podiel obcí na výnose DPFO pre rok 2025. Ministerstvo financií SR. Dostupné na https://www.mfsr.sk/files/archiv/34/Vychodiskove_statisticke_udaje_a_podiel_obci_na_vynose_DPFO_pre_rok_2025.pdf
10. Zákon č. 564/2004 Z.z. o rozpočtovom určení výnosu dane z príjmov územnej samospráve a o doplnení niektorých zákonov

Kontaktné údaje

doc. Mgr. Ing. Tomáš Černěňko, PhD.

tomas.cernenko@euba.sk

Národohospodárska fakulta, Ekonomická univerzita v Bratislave

doc. Ing. Erika Neubauerová, PhD.

erika.neubauerova@flaw.uniba.sk

Právnická fakulta, Univerzita Komenského v Bratislave

DAŇ Z FINANČNÝCH TRANSAKCIÍ – DANOVÝ NEXUS

FINANCIAL TRANSACTION TAX – TAX NEXUS

Toško Beran¹

Abstrakt: Daň z finančných transakcií je v Slovenskej republike upravená zákonom č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ktorý nadobudol účinnosť od 1. januára 2025. Týmto zákonom bolo primárne zavedené zdanenie debetných finančných transakcií vykonaných zo slovenských bankových účtov fyzických osôb podnikateľov, právnických osôb, či organizačných zložiek zahraničných právnických osôb. Jedným z kľúčových inštitútov pre riadnu aplikáciu tejto dane je zadefinovanie daňového nexusu, t. j. vymedzenie vzťahu medzi daňovým subjektom a príslušnou daňovou jurisdikciou, v našom prípade Slovenskou republikou, ktorej územie definuje zákon ako tuzemsko. V zmysle súčasne platnej a účinnej legislatívy sa za daňovníka považuje subjekt, ak spĺňa aspoň jednu z troch ustanovených podmienok: (i) má sídlo alebo miesto podnikania v tuzemsku, (ii) má platobný účet u poskytovateľa platobných služieb so sídlom v tuzemsku, alebo (iii) vykonáva činnosť na území Slovenska. Cieľom príspevku je navrhnúť úpravy de lege ferenda, ktoré presnejšie zadefinujú daňový nexus pri dani z finančných transakcií, inšpirujúc sa pravidlami dane z príjmov pre určenie daňovníka s neobmedzenou a obmedzenou daňovou povinnosťou a určenie zdroja príjmov v Slovenskej republike. Pri spracovaní problematiky daňového nexusu v kontexte dane z finančných transakcií boli využité vedecké metódy právnej analýzy, právnej komparatistiky a metóda výkladu.

Kľúčové slová: daň z finančných transakcií; daňový nexus; daňovník z neobmedzenou daňovou povinnosťou; daňovník z obmedzenou daňovou povinnosťou; stála prevádzkareň; predmet dane.

Abstract: The financial transaction tax in the Slovak Republic is regulated by Act No. 279/2024 Coll. on the Financial Transaction Tax and on Amendments to Certain Acts, as amended, which entered into force on 1 January 2025. This Act primarily introduced the taxation of debit financial transactions executed from Slovak bank accounts held by self-employed individuals, legal entities, or

¹ Univerzita Komenského v Bratislave, Právnická fakulta

organizational units of foreign legal entities. One of the key instruments for the proper application of this tax is the definition of the tax nexus, i.e., the delineation of the relationship between the taxpayer and the relevant tax jurisdiction, in our case the Slovak Republic, whose territory is defined by the Act as the domestic jurisdiction. According to the currently valid and effective legislation, an entity is considered a taxpayer if it meets at least one of the three established conditions: (i) it has its registered seat or place of business in the domestic jurisdiction, (ii) it holds a payment account with a payment service provider established in the domestic jurisdiction, or (iii) it carries out activities in the territory of the Slovak Republic. The aim of this paper is to propose *de lege ferenda* amendments that would more precisely define the tax nexus for the financial transaction tax, inspired by the income tax rules for determining taxpayers with unlimited and limited tax liability and for determining the source of income in the Slovak Republic. The examination of the tax nexus within the framework of the financial transaction tax was conducted employing scientific methodologies, including legal analysis, comparative legal research, and interpretative techniques.

Key words: financial transaction tax; tax nexus; taxpayer with unlimited tax liability; taxpayer with limited tax liability; permanent establishment; subject of the tax.

Úvod

„Tempora mutantur, et nos mutamur in illis²⁾.“

S účinnosťou od 1. januára 2025 bol daňový systém Slovenskej republiky rozšírený o novú daň – daň z finančných transakcií. Zákon č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov (ďalej len „zákon o dani z finančných transakcií“) bol prijatý ako jedno z kľúčových konsolidačných opatrení vlády Slovenskej republiky v reakcii na nepriaznivý vývoj verejných financií. Touto právnou úpravou poslanci Národnej rady Slovenskej republiky 3. októbra 2024³⁾ primárne zaviedli zdanenie debetných finančných transakcií vykonávaných zo slovenských bankových účtov, pričom právna úprava zákona o dani z finančných transakcií sa vzťahuje na fyzické osoby – podnikateľov, právnické osoby a organizačné zložky zahraničných právnických osôb. Cieľom predmetného konsolidačného opatrenia bolo do štátneho rozpočtu zabezpečiť dodatočné príjmy približne 517 miliónov eur v roku zavedenia a viac ako 700 miliónov eur v nasledujúcich rokoch.

²⁾ „Časy sa menia a my sa meníme s nimi.“

³⁾ <https://www.nrsr.sk/web/Default.aspx?sid=udalosti/udalost&MasterID=56966>

Legislatívny proces bol výrazne ovplyvnený potrebou rýchlej reakcie na rastúce makroekonomické riziká. Hrubý dlh verejnej správy sa v tom istom období vyšplhal na hranicu 59,7 % HDP, teda bezprostredne pod 60 % hranicou sankčného pásma podľa ústavného zákona č. 493/2011 Z. z. o rozpočtovej zodpovednosti. Schodok hospodárenia sa očakával blízko úrovne 6 % hrubého domáceho produktu.

Na tieto skutočnosti reagovala vláda Slovenskej republiky predložením návrhu zákona o dani z finančných transakcií v skrátrenom legislatívnom konaní⁴⁾. V odôvodnení skráteneho legislatívneho konania sa uvádza, že bez prijatia dodatočných príjmových opatrení by Slovenskej republike hrozila strata dôvery finančných trhov a rast rizikových prirážok na štátne dlhopisy. Už v roku 2024 Európska komisia aktivovala voči Slovensku procedúru nadmerného deficitu, v rámci ktorej bola krajina povinná predložiť konsolidačný plán⁵⁾. V prípade jeho nesplnenia by Slovensku ako členovi eurozóny mohla každých šesť mesiacov hroziť pokuta až do výšky 0,05 % HDP, čo pri objeme ekonomiky na úrovni približne 120 miliárd eur predstavuje okolo 60 miliónov eur. Cieľom aj tejto dane, ako súčasti konsolidačných opatrení, bola stabilizácia verejných financií tak, aby sa deficit dostal pod 3% v roku 2027, aby verejný dlh mohol začať opäť klesať.

Nová daň bola nastavená tak, aby nezaťažovala fyzické osoby, ktoré nevykonávajú podnikateľskú činnosť a zároveň, aby jej administratíva bola pre podnikateľské subjekty čo najjednoduchšia a to tak, že prevažnú časť povinností súvisiacich s platením tejto dane preniesla na finančné inštitúcie poskytujúce platobné služby (ďalej len „poskytovatelia platobných služieb“ prípadne „finančné inštitúcie“). Predmetom dane sú najmä prevody, pri ktorých dochádza k odpísaniu finančných prostriedkov z účtu daňovníka, výbery hotovosti a používanie platobných kariet. Naopak, zákon ustanovuje viaceré výnimky – medzi ne patria napríklad platby daní, odvodov a poplatkov do štátneho rozpočtu, ale aj prevody medzi účtami toho istého daňovníka vedenými u jedného poskytovateľa platobných služieb. Zároveň sa však zákonom o dani z finančných transakcií zaviedli aj tzv. protiúnikové opatrenia, ako je napríklad inštitút preúčtovaných nákladov alebo definovanie daňovníka prostredníctvom činnosti, ktorú vykonáva v Slovenskej republike, ktoré mali demotivovať daňovníkov od nežiaduceho daňového správania.

Pôvodný zákon o dani z finančných transakcií bol však už tri krát novelizovaný⁶⁾, pričom predmetom novelizácií bolo predovšetkým rozšírenie výnimiek z osobného

⁴⁾ Návrh vlády na skrátene legislatívne konanie o vládnom návrhu zákona o dani z finančných transakcií a o zmene a doplnení niektorých zákonov.

⁵⁾ <https://www.mfsr.sk/sk/media/tlacove-spravy/slovensko-procedure-nadmerneho-deficitu.html>

⁶⁾ Zákon č. 354/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

rozsahu daňovníkov dane z finančných transakcií a zúženie predmetu dane z finančných transakcií doplnením ďalších platobných operácií, ktoré sú z predmetu dane vylúčené. Okrem týchto úprav však novelizácie obsahovali aj spresnenia k vybraným ustanoveniam zákona o dani z finančných transakcií, ako napríklad doplnenie oznamovania výnimiek platiteľovi dane s cieľom zabezpečiť jeho právnu istotu pri správe tejto dane, alebo úprava mechanizmu výpočtu dane tak, aby sa zjednotili pravidlá pre výpočet dane z domácich a zahraničných platieb⁷⁾.

Cieľom príspevku je identifikovať východiská pre legislatívnu úpravu zákona o dani z finančných transakcií a predložiť možné návrhy úprav „de lege ferenda“ s cieľom jednoznačne definovať daňový nexus tejto dane. Zároveň bude v príspevku obsiahnutá aj reflexia, akým spôsobom boli tieto návrhy následne zapracované do novely zákona o dani z finančných transakcií, ktorá nadobúda účinnosť od 1. januára 2026⁸⁾.

Pri spracovaní problematiky daňového nexusu v kontexte dane z finančných transakcií boli využité vedecké metódy právnej analýzy existujúcej právnej úpravy obsiahnutej v zákone o dani z finančných transakcií a metóda výkladu, ktorá slúži na objasnenie významu právnej normy. Využitá bola aj metóda právnej komparatistiky, najmä porovnanie s úpravou obsiahnutou v zákone o dani z príjmov a medzinárodnými zmluvami o zamedzení dvojitého zdanenia.

S ohľadom na unikátnosť slovenského riešenia dane z finančných transakcií nebolo možné použiť metódu právnej komparatistiky vo vzťahu k úprave dane z finančných transakcií v zahraničí. Napriek skutočnosti, že aj maďarská daň z finančných transakcií sa vyberá z platobných operácií na účtoch, zásadným rozdielom je osobný rozsah dane z finančných transakcií, kde daňovníkmi tejto dane sú práve finančné inštitúcie a ich pobočky v Maďarsku⁹⁾ a nie používatelia platobných účtov. Belgická¹⁰⁾

Zákon č. 26/2025 Z. z. o zmene a doplnení niektorých zákonov v súvislosti so zmenami vyvolanými Stavebným zákonom.

Zákon č. 176/2025 Z. z., ktorým sa mení a dopĺňa zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

⁷⁾ S p o l o č n á s p r á v a výborov Národnej rady Slovenskej republiky o výsledku prerokovania vládneho návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa mení zákon č. 331/2011 Z. z., ktorým sa mení a dopĺňa zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov a ktorým sa menia a dopĺňajú niektoré zákony v znení neskorších predpisov (tlač 501) v druhom čítaní (bod 26)

⁸⁾ Zákon č. 272/2025 Z. z., ktorým sa mení a dopĺňa zákon č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

⁹⁾ CMS Law-Now, Hungary: new tax on financial transactions (12.11.2025), Dostupné na: <https://cms-lawnow.com/en/ealerts/2012/07/hungary-new-tax-on-financial-transactions>

¹⁰⁾ Service Public Fédéral Finances, Taxe sur les opérations de bourse (TOB) (12.11.2025), Dostupné na: <https://finances.belgium.be/fr/entreprises/autres-taxes/taxes-diverses/taxe-operations-bourse#q1> (použitý anglický preklad stránky prostredníctvom Google translate).

a francúzska¹¹⁾) daň z finančných transakcií sú zásadne rozdielného charakteru. Ide predovšetkým o dane zaťažujúce operácie na kapitálových trhoch, ako obchodovanie s finančnými nástrojmi, nie na bežné platobné operácie na platobných účtoch. Preto aj pri definovaní daňového nexusu slovenskej dane z finančných transakcií bolo potrebné jej osobitosť brať do úvahy a nebolo možné použiť inšpiráciu zo zahraničia.

Daňový nexus – de lege lata

§ 3 zákona o dani z finančných transakcií ustanovuje osobný rozsah zákona o dani z finančných transakcií. Upravuje osoby, na ktoré sa tento zákon vzťahuje, t. j. ktorým osobám ukladá povinnosti, alebo priznáva práva. Medzi tieto osoby sa zaradujú daňovníci a platitelia dane. Daňovníkmi sú subjekty, ktoré priamo nesú originálnu daňovú povinnosť, to znamená, že sú to práve tieto subjekty, ktorých finančné transakcie sú zaťažené daňou z finančných transakcií, a to napriek skutočnosti, že v zmysle zákona o dani z finančných transakcií priamo nezodpovedajú za plnenie daňových povinností voči správcovi dane. Zákon o dani z finančných transakcií ukladá povinnosti spojené s platením dane z finančných transakcií platiteľom dane a ustanovuje ich aj zodpovednými za ich riadne a včasné plnenie. Platiteľom dane sú subjekty, ktoré na jednej strane vyberajú daň od daňovníkov a na druhej strane vybratú daň odvádzajú do štátneho rozpočtu a sú za ňu zodpovední¹²⁾.

Medzi daňovníkov dane z finančných transakcií sa zahŕňajú fyzické osoby – podnikatelia. Ide predovšetkým o živnostníkov, ale aj o osoby vykonávajúce slobodné povolania, ako sú advokáti, daňoví poradcovia, alebo súkromní lekári, ďalej o samostatne hospodáriacich roľníkov, ako aj o iné osoby, ktoré vykonávajú podnikateľskú alebo inú samostatne zárobkovú činnosť na základe osobitného oprávnenia či licencie. Za daňovníka sa považuje aj fyzická osoba-podnikateľ, ktorej bolo povolenie na podnikanie vydané v inom štáte, ak má určitú formu prítomnosti na Slovensku. Naopak, fyzické osoby, ktoré prenajímajú nehnuteľnosť bez poskytovania doplnkových služieb alebo vykonávajú činnosť len podľa autorského zákona, sa za daňovníkov nepovažujú, keďže tieto činnosti nenapĺňajú znaky podnikania. Pre účely určenia statusu fyzickej osoby ako podnikateľa, nie je rozhodujúce, ako sú zatriedené príjmy dosahované z tejto činnosti na účely zákona o dani z príjmov, ale či sa táto činnosť v zmysle jednotlivých osobitných predpisov,

¹¹⁾ Bulletin Officiel des Finances Publiques – Impôts, TCA - Taxes sur les transactions financières - Taxe sur les acquisitions de titres de capital ou assimilés - Modalités de taxation (12.11.2025), Dostupné na: <https://bofip.impots.gouv.fr/bofip/7575-PGP.html/identifiant=BOI-TCA-FIN-10-30-20250528> (použitý anglický preklad stránky prostredníctvom Google translate).

¹²⁾ Toško Beran: Zákon o dani z finančných transakcií – komentár, Wolters Kluwer, 6/2025, 88 strán, strana 14, ISBN 978-80-571-0768-2

ktoré definujú jej základné parametre, považuje za podnikanie resp. za výkon inej samostatne zárobkovej činnosti¹³⁾).

Daňovníkom môže byť aj právnická osoba. Ide o subjekty práva so samostatnou právnou subjektivitou, ktorým právny poriadok priznáva spôsobilosť mať práva a povinnosti. Typickými príkladmi sú obchodné spoločnosti, štátne podniky, družstvá, ale aj politické strany či niektoré subjekty neziskového sektora. Na účely dane z finančných transakcií sa za daňovníka považuje aj organizačná zložka zahraničnej osoby, predovšetkým pobočka alebo iná forma zastúpenia zahraničného subjektu, ktorá vykonáva svoju činnosť na území Slovenska. Organizačné zložky tuzemských subjektov sa za samostatných daňovníkov nepovažujú, keďže sú súčasťou zriaďovateľa.

Okrem uvedených právnych foriem ustanovuje zákon o dani z finančných transakcií ako podmienku na to, aby bol subjekt považovaný za daňovníka, aj skutočnosť, že takýto subjekt musí mať určitú formu prítomnosti v Slovenskej republike, takzvaný daňový nexus. Túto prítomnosť definuje zákon splnením aspoň jednej z nasledujúcich podmienok, a to sídlo alebo miesto podnikania je v Slovenskej republike, platobný účet vedený poskytovateľom platobných služieb, ktorý má sídlo v Slovenskej republike alebo vykonávaním samotnej činnosti daňovníka v Slovenskej republike. Tieto podmienky nemusia byť splnené súčasne a na to, aby fyzickej osobe podnikateľovi, právnickej osobe alebo organizačnej zložke zahraničnej osoby vzniklo postavenie daňovníka dane z finančných transakcií postačí, ak naplní aspoň jednu z uvedených troch podmienok¹⁴⁾.

Z pohľadu definície daňovníka sa takéto určenie daňového nexusu javí ako dostatočné, avšak pri určovaní predmetu došlo medzi zástupcami odbornej verejnosti k diskusii o možnom rozpore zákona o dani z finančných transakcií s právom Európskej únie. Časť spektra konštatuje rozpor s ohľadom na možné diskriminačné účinky tejto dane¹⁵⁾, avšak naopak niektorí experti tento rozpor neidentifikujú¹⁶⁾.

Rovnako zástupcovia odbornej verejnosti poukázali aj na možné riziko exterritoriality¹⁷⁾. Riziko exterritoriality je spojené najmä s nadmerne širokou

¹³⁾ Toško Beran: Zákon o dani z finančných transakcií – komentár, Wolters Kluwer, 6/2025, 88 strán, strana 15, ISBN 978-80-571-0768-2

¹⁴⁾ Toško Beran: Zákon o dani z finančných transakcií – komentár, Wolters Kluwer, 6/2025, 88 strán, strana 16, ISBN 978-80-571-0768-2

¹⁵⁾ Renáta Bláhová: Nový Zákon o dani z finančných transakcií z pohľadu práva EÚ, Bulletin Slovenskej komory daňových poradcov 1/2025, Slovenská komora daňových poradcov, 2025

¹⁶⁾ Aneta Kollman Steinhübllová: DAŇ Z FINANČNÝCH TRANSAKCIÍ V KONTEXTE PRÁVA EURÓPSKEJ ÚNIE, Míľniky práva v stredoeurópskom priestore 2025 (zväzok II), Právnická fakulta Univerzity Komenského, 2025, strana 1027

¹⁷⁾ Transakčná daň má stále vážne nedostatky – tlačová správa Slovenskej komory daňových poradcov z 19. 02. 2025 <https://new.skdp.sk/clanky/transakcna-dan-ma-stale-vazne-nedostatky>

definíciou predmetu dane, pri ktorej ustanovenie jednoznačného daňového nexusu absentuje. S ohľadom na prísne gramatický výklad je možné dovodiť, že ak subjekt naplní znaky daňovníka dane z finančných transakcií budúc, v zmysle zákona o dani z finančných transakcií, predmetom dane všetky jeho finančné transakcie vykonávané na celom svete, bez ohľadom na existenciu prepojenia so Slovenskou republikou. S cieľom zabrániť takémuto extenzívnemu výkladu vydalo Ministerstvo financií Slovenskej republiky v zmysle splnomocňovacieho ustanovenia obsiahnutého v Daňovom poriadku¹⁸⁾ metodické usmernenie, ktorým zužujúcim spôsobom usmernilo aplikáciu pravidiel zahrňovania finančných transakcií do predmetu dane z finančných transakcií, aby sa potenciálnej exteritorialite zabránilo¹⁹⁾.

Daňový nexus – de lege ferenda

Pri novom nastavení daňového nexusu dane z finančných transakcií je potrebné posilniť jednoznačnosť a právnu istotu určenia postavenia daňovníkov, ako aj definovania predmetu dane, pričom je možné čerpať inšpiráciu z existujúcich pravidiel a inštitútov vlastných pre daň z príjmov. Ako je uvedené v predchádzajúcej časti v zmysle platného a účinného zákona sa v súčasnosti medzi daňovníkov zaraďujú aj organizačné zložky zahraničných osôb. Tento prístup sa javí ako problematický, keďže organizačná zložka sama osebe nemá právnu subjektivitu a nositeľom práv a povinností je vždy materská zahraničná právnická osoba. Napriek tomu, že organizačná zložka môže byť zapísaná v obchodnom registri, jej existencia by mala byť z daňového hľadiska posudzovaná ako forma výkonu činnosti prostredníctvom stálej prevádzkarne. Navrhovaná úprava preto smeruje k vypusteniu organizačnej zložky ako samostatného daňovníka a k jej subsumovaniu pod pojem stálej prevádzkarne, čím by malo dôjsť k zosúladeniu s ustáleným chápaním výkonu činnosti a konceptu stálej prevádzkarne obdobne, ako je tomu v oblasti dane z príjmov²⁰⁾ a v medzinárodných daňových zmluvách²¹⁾.

Kľúčovým prvkom pripravovanej úpravy je rozdelenie daňovníkov na tých, ktorí majú neobmedzenú daňovú povinnosť, a tých, ktorí majú daňovú povinnosť obmedzenú.

¹⁸⁾ § 160 ods. 2 Daňového poriadku.

¹⁹⁾ Usmernenie Ministerstva financií Slovenskej republiky č. MF/008722/2025-77 k postupu pri posudzovaní vykonávania činnosti daňovníka v tuzemsku, spôsobu zdanenia preúčtovaných nákladov a automatizovanej kompenzácií zostatkov podľa zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

²⁰⁾ § 16 zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.

²¹⁾ Čl. 5 modelovej zmluvy o zamedzení dvojitého zdanenia v oblasti daní z príjmov a zabránení daňovému úniku a vyhýbaniu sa daňovým povinnostiam. OECD (2019), Model Tax Convention on Income and on Capital 2017 (Full Version), OECD Publishing, Paris, <https://doi.org/10.1787/g2g972ee-en>.

Tento princíp je zaužívaný v slovenskej daňovej legislatíve a analogicky funguje v zákone o dani z príjmov²²⁾). Daňovníci s neobmedzenou daňovou povinnosťou sú fyzické osoby a právnické osoby so sídlom alebo miestom podnikania v Slovenskej republike. V prípade právnických osôb ide o subjekty, ktoré majú svoje sídlo zapísané v obchodnom registri alebo inom príslušnom registri (napríklad obchodné spoločnosti, družstvá alebo politické strany či cirkvi). Pri fyzických osobách-podnikateľoch sa za miesto podnikania považuje adresa formálne zapísaná v živnostenskom registri alebo inom príslušnom registri, nie adresa trvalého pobytu. Pri daňovníkoch s neobmedzenou daňovou povinnosťou by podliehali zdaneniu všetky finančné transakcie, ktoré uskutočnia, bez ohľadu na to, či sú realizované prostredníctvom poskytovateľov platobných služieb so sídlom v Slovenskej republike alebo v zahraničí.

Naopak, daňovníci s obmedzenou daňovou povinnosťou sú zahraničné subjekty bez sídla alebo miesta podnikania v Slovenskej republike, ktorých finančné transakcie by však mali mať väzbu s územím Slovenskej republiky. Pre vznik daňovej povinnosti by bolo rozhodujúce, či im na Slovensku vznikne stála prevádzkareň. Tento pojem sa navrhuje spresniť tak, aby odstránil existujúce výkladové nejasnosti súvisiace so súčasnou úpravou výkonu činnosti na Slovensku. Stálou prevádzkarňou by malo byť trvalé miesto, prostredníctvom ktorého zahraničný subjekt vykonáva svoju činnosť na Slovensku. Za trvalosť sa považuje vykonávanie činnosti aspoň počas prevažnej časti zdaňovacieho obdobia, teda minimálne 16 dní v kalendárnom mesiaci.

Stála prevádzkareň môže vzniknúť rôznymi formami. Ide napríklad o prípady tzv. agentskej stálej prevádzkarne, keď zahraničný subjekt pôsobí prostredníctvom osoby, ktorá v jeho mene pravidelne uzatvára alebo prerokúva zmluvy, pričom nie je rozhodujúce, či ide o zamestnanca v pracovnoprávnom vzťahu alebo o inú osobu viazanú občianskoprávnou či obchodnoprávnou zmluvou. Rovnako môže ísť aj o tzv. službovú stálu prevádzkareň, kedy daňovník alebo osoby pre neho pracujúce poskytujú na území Slovenska služby alebo o tzv. stavebnú stálu prevádzkareň, kedy sa na území Slovenska nachádza stavenisko, miesto vykonávania stavebných projektov a montážnych projektov.

Za výkon činnosti prostredníctvom stálej prevádzkarne v Slovenskej republike, by sa nad rámec zaužívaný pre oblasť dane z príjmov, považovalo aj využívanie nehnuteľností alebo dopravných prostriedkov, ktoré predstavujú poistné riziko umiestnené v tuzemsku, napríklad pri poistených nehnuteľnostiach na Slovensku alebo pri dopravných prostriedkoch evidovaných v slovenských registroch. Ak výkon činnosti presiahne polovicu kalendárneho mesiaca, vzniká daňová povinnosť na celé zdaňovacie obdobie a všetky finančné transakcie subjektu v tomto období podliehajú

²²⁾ § 2 písm.d) a e) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.

dani, ak nie sú zo zákona oslobodené. Obdobný daňový nexus vychádzajúci z umiestnenia poistného rizika na Slovensku sa uplatňuje aj pre daň z poistenia²³⁾.

Osobitnú kategóriu tvoria elektronické rozhrania umiestnené v tuzemsku. Navrhovaná úprava zohľadňuje špecifický charakter služieb informačnej spoločnosti²⁴⁾ a zahrňuje do definície stálej prevádzkarne subjekty, ktoré prostredníctvom elektronického rozhrania predávajú tovar alebo služby, prípadne sprostredkujú predaj medzi predávajúcimi a kupujúcimi. Ide o e-shopy predávajúce tovar alebo poskytujúce služby priamo zákazníkovi alebo o tzv. marketplace platformy, prostredníctvom ktorých je sprostredkovaný predaj tovaru alebo poskytnutie služby medzi nezávislými stranami. Pod elektronickým rozhraním umiestneným v tuzemsku by sa malo rozumieť najmä webová stránka alebo aplikácia prevádzkovaná pod doménou „.sk“, prípadne ak je táto webová stránka hostovaná na serveri umiestnenom na Slovensku alebo ak je inak technicky či prevádzkovo spätá s územím Slovenskej republiky. Podobné zadefinovania výkonu činnosti v oblasti digitálnej ekonomiky prostredníctvom online trhu²⁵⁾ alebo digitálnej platformy, ktoré sú umiestnené v Slovenskej republike, je obsiahnuté aj v metodickom usmernení Ministerstva financií Slovenskej republiky²⁶⁾.

Samostatným kritériom daňového nexusu a teda prepojenia finančných transakcií subjektov, ktoré nemajú na Slovensku sídlo ani miesto podnikania, s územím Slovenskej republiky by bolo vedenie platobného účtu u poskytovateľa platobných služieb so sídlom v Slovenskej republike. Ak by fyzická osoba-podnikateľ alebo právnická osoba mala účet vedený u slovenského poskytovateľa platobných služieb, stala by sa daňovníkom s obmedzenou daňovou povinnosťou a to aj v prípade, ak by jej na Slovensku nevznikla stála prevádzkareň na účely dane z finančných transakcií. V takomto prípade by však predmetom dane boli len finančné transakcie realizované prostredníctvom tohto účtu, pričom by však nebolo relevantné za akým účelom by tieto finančné transakcie boli vykonávané, a teda by nebola relevantná ani skutočnosť či sú vykonávané v súvislosti s výkonom činnosti daňovníka na území Slovenskej republiky.

²³⁾ zákon č. 213/2018 Z. z. o dani z poistenia a o zmene a doplnení niektorých zákonov v znení zákona č. 408/2021 Z. z.

²⁴⁾ § 2 písm. a) a b) zákona č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.

²⁵⁾ Zákon č. 108/2024 Z. z. o ochrane spotrebiteľa a o zmene a doplnení niektorých zákonov.

²⁶⁾ čl. III ods. 1 písm. b) a c) Usmernenie Ministerstva financií Slovenskej republiky č. MF/008722/2025-77 k postupu pri posudzovaní vykonávania činnosti daňovníka v tuzemsku, spôsobu zdanenia preúčtovaných nákladov a automatizovanej kompenzácie zostatkov podľa zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Novela zákona o dani z finančných transakcií s účinnosťou od 1. januára 2026

Dňa 15. apríla 2025 bol na rokovanie Národnej rady Slovenskej republiky skupinou poslancov predložený návrh zákona, ktorým sa mení a dopĺňa zákon o dani z finančných transakcií (ďalej len „novela zákona o dani z finančných transakcií“). Samotný návrh bol však počas druhého čítania v pléne Národnej rady Slovenskej republiky podstatným spôsobom upravený pozmeňujúcim a doplňujúcim návrhom poslanca Adama Lučanského²⁷⁾. V rámci spolupráce s poslancami Národnej rady Slovenskej republiky sme pri práci na koncepte predmetného pozmeňujúceho a doplňujúceho návrhu vychádzali práve z východísk „de lege ferenda“ zadefinovaných v predchádzajúcej časti príspevku. Druhou determinujúcou líniou, ktorá ovplyvňovala prácu na znení pozmeňujúceho a doplňujúceho návrhu bola politická rovina deklarovaná aj v dôvodovej správe priloženej k pôvodnému poslaneckému návrhu novely zákona o dani z finančných transakcií. Jej cieľom bolo podľa predkladateľov upraviť rozsah subjektov, ktoré sú daňovníkmi podľa zákona o dani z finančných transakcií, a to z dôvodu potreby zabezpečiť spravodlivejšie, hospodárnejšie a administratívne únosnejšie uplatňovanie tejto dane²⁸⁾. Z tohto dôvodu sa z osobného rozsahu zákona o dani z finančných transakcií vypustili všetky fyzické osoby podnikatelia.

Vo vzťahu k definovaniu daňového nexusu dane z finančných transakcií sme v plnej miere implementovali všetky navrhované úpravy „de lege ferenda“ a to predovšetkým došlo k vypusteniu organizačnej jednotky ako samostatného daňovníka dane z finančných transakcií a zavedeniu daňovníka s neobmedzenou a obmedzenou daňovou povinnosťou. Za daňovníka z neobmedzenou daňovou povinnosťou sa od 1. januára 2026 bude považovať tá právnická osoba, ktorá má sídlo na území Slovenska²⁹⁾. Naopak za daňovníka s obmedzenou daňovou povinnosťou sa definovala právnická osoba, ktorá nemá sídlo na území Slovenska, ale na Slovensku má platobný účet, alebo tu vykonáva činnosť prostredníctvom stálej prevádzkarne³⁰⁾. Za týmto účelom sa aj základné definície zákona o dani z finančných transakcií rozšírili v rozsahu navrhovanom v predchádzajúcej časti príspevku o definíciu stálej prevádzkarne na účely dane z finančných transakcií³¹⁾.

²⁷⁾ <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=573902>

²⁸⁾ Dôvodová správa – všeobecná časť,

<https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=564740>

²⁹⁾ § 3 ods. 1 písm. a) zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení účinnom od 1. januára 2026.

³⁰⁾ § 3 ods. 1 písm. b) zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení účinnom od 1. januára 2026.

³¹⁾ § 2 ods. 2 zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení účinnom od 1. januára 2026.

Za prijatie tejto novely zákona o dani z finančných transakcií, ktorej súčasťou boli aj zmeny obsiahnuté v pozmeňujúcom a doplňujúcom návrhu hlasovalo spoločne všetkých 128 prítomných poslancov³²⁾).

Záver

Základnou podmienkou efektívneho fungovania každej dane je jasne vymedzený daňový nexus, ktorý určuje, kedy subjekt vstupuje do postavenia daňovníka a čo je predmetom dane. Vyššie navrhovaná úprava by podľa môjho názoru priniesla do systému dane z finančných transakcií systematiku zaužívanú v iných daňových zákonoch, a preto by bolo možné sa oprieť vo väčšej miere aj o ustálené metodické usmernenia, odbornú literatúru a medzinárodne uznávané koncepty. Zavedením rozlíšenia medzi daňovníkmi s neobmedzenou daňovou povinnosťou a daňovníkmi s obmedzenou daňovou povinnosťou by sa posilnila predvídateľnosť a jednoznačnosť posúdenia daňového postavenia subjektov a rozsah v akom budú ich finančné transakcie podliehať dani. Spresnením definície stálej prevádzkarne a vypustením organizačnej zložky ako samostatného daňovníka sa odstránia výkladové problémy, ktoré sa v praxi opakovane objavujú. Zároveň sa tým zabezpečí, že daňová povinnosť bude viazaná na tie finančné transakcie, ktoré majú určitú väzbu so Slovenskou republikou. Celkovým cieľom je preto dosiahnuť vyváženú právnu úpravu, ktorá nebude pôsobiť extenzívne ani reštriktívne, ale zabezpečí spravodlivé a udržateľné zdaňovanie finančných transakcií. Ak takáto úprava bola príliš široká, mohlo by vzniknúť riziko exteritoriality a nežiadúceho zdanenia transakcií bez skutočnej väzby na Slovenskú republiku. Naopak, ak by bola nová úprava navrhnutá príliš úzko, mohla by vytvárať priestor pre špekulatívne konanie daňovníkov, ktorí by sa mohli snažiť nežiaducim spôsobom optimalizovať svoje daňové povinnosti súvisiace s daňou z finančných transakcií, resp. sa snažiť riadnemu plneniu týchto daňových povinností vyhnúť úplne. Uvedené návrhy precizovania daňového nexusu dane z finančných transakcií boli zapracované do novely zákona o dani z finančných transakcií, prostredníctvom poslaneckého návrhu, čím sa mitigovali doterajšie interpretačné nejasnosti a zvýšila sa právna istota adresátov zákona o dani z finančných transakcií.

Zoznam použitej literatúry

1. Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.
3. Zákon č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

³²⁾ <https://www.nrsr.sk/web/Default.aspx?sid=schodze/hlasovanie/hlasklub&ID=56989>

4. Návrh vlády na skrátené legislatívne konanie o vládnom návrhu zákona o dani z finančných transakcií a o zmene a doplnení niektorých zákonov.
5. Spoločná správa výborov Národnej rady Slovenskej republiky o výsledku prerokovania vládneho návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa mení zákon č. 331/2011 Z. z., ktorým sa mení a dopĺňa zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov a ktorým sa menia a dopĺňajú niektoré zákony v znení neskorších predpisov (tlač 501) v druhom čítaní.
6. Usmernenie Ministerstva financií Slovenskej republiky č. MF/008722/2025-77 k postupu pri posudzovaní vykonávania činnosti daňovníka v tuzemsku, spôsobu zdanenia preúčtovaných nákladov a automatizovanej kompenzácii zostatkov podľa zákona č. 279/2024 Z. z. o dani z finančných transakcií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
7. Modelová zmluva o zamedzení dvojitého zdanenia v oblasti daní z príjmov a zabránení daňovému úniku a vyhýbaniu sa daňovým povinnostiam. OECD (2019), Model Tax Convention on Income and on Capital 2017 (Full Version), OECD Publishing, Paris, Dostupné na: <https://doi.org/10.1787/g2g972ee-en>
8. Toško Beran: Zákon o dani z finančných transakcií – komentár, Wolters Kluwer, 6/2025, 88 strán, ISBN 978-80-571-0768-2.
9. Renáta Bláhová: Nový Zákon o dani z finančných transakcií z pohľadu práva EÚ, Bulletin Slovenskej komory daňových poradcov 1/2025, Slovenská komora daňových poradcov, 2025, str. 20 až 23.
10. Aneta Kollman Steinhübllová: DAŇ Z FINANČNÝCH TRANSAKCIÍ V KONTEXTE PRÁVA EURÓPSKEJ ÚNIE, Mílniky práva v stredoeurópskom priestore 2025 (zväzok II), Právnická fakulta Univerzity Komenského, 2025, str. 1027 až 1033.
11. Transakčná daň má stále vážne nedostatky – tlačová správa Slovenskej komory daňových poradcov z 19. 02. 2025, Dostupné na: <https://new.skdp.sk/clanky/transakcna-dan-ma-stale-vazne-nedostatky>
12. CMS Law-Now, Hungary: new tax on financial transactions (12.11.2025), Dostupné na: <https://cms-lawnow.com/en/ealerts/2012/07/hungary-new-tax-on-financial-transactions>
13. Service Public Fédéral Finances, Taxe sur les opérations de bourse (TOB) (12.11.2025), Dostupné na: <https://finances.belgium.be/fr/entreprises/autres-taxes/taxes-diverses/taxe-operations-bourse#q1> (použitý anglický preklad stránky prostredníctvom Google translate)
14. Bulletin Officiel des Finances Publiques – Impôts, TCA - Taxes sur les transactions financières - Taxe sur les acquisitions de titres de capital ou assimilés - Modalités de taxation (12.11.2025), Dostupné na: <https://bofip.impots.gouv.fr/bofip/7575->

[PGP.html/identifiant=BOI-TCA-FIN-10-30-20250528](https://pgp.html/identifiant=BOI-TCA-FIN-10-30-20250528) (použitý anglický preklad stránky prostredníctvom Google translate)

15. The Center for Economic and Policy Research, Financial Transactions Taxes Around the World (12. 11. 2025), Dostupné na: <https://cepr.net/publications/financial-transactions-taxes-around-the-world/>

Kontaktné údaje

JUDr. Toško Beran

beran3@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

VIDA – DPH V DIGITÁLNOH VEKU

VIDA – VAT IN THE DIGITAL AGE

Aneta Kollman Steinhüblová¹

Abstrakt: Autorka sa vo svojom príspevku zameriava na balík opatrení v oblasti dane z pridanej hodnoty v digitálnom veku, tzv. balík ViDA (DPH v digitálnom veku). Cieľom príspevku je objasnenie niektorých ustanovení legislatívnych aktov balíka ViDA so zameraním na digitálne platformy poskytujúce služby krátkodobého prenájmu ubytovania a služby cestnej prepravy cestujúcich. Hlavným zámerom bolo poukázať na možné výkladové odchýlky vznikajúce v chápaní niektorých členských štátov, ktoré môžu priniesť riziká rozdielného uplatňovania jednotlivými členskými štátmi. Autorka poukazuje na otvorené otázky, ktoré vystali z potenciálnych modelových situácií pravdepodobne sa vyskytujúcich v budúcnosti v praxi a ktorých interpretáciu Európska komisia plánuje objasniť prostredníctvom vysvetľujúcich poznámok. Záverom je možné konštatovať, že riadna implementácia opatrení z balíka ViDA by mala prispieť k vyššiemu a efektívnejšiemu výberu DPH. Na jednej strane dôjde k zníženiu administratívnej záťaže zavedením jednotnej registrácie pre DPH, avšak na strane druhej dôjde k jej zvýšeniu zavedením záznamovej povinnosti pre digitálne platformy. V príspevku boli pri výklade legislatívnych aktov v rámci balíka ViDA použité metódy dedukcie a komparácie. Zo súboru opatrení balíka ViDA ktorý tvorí komplexný celok, boli analýze podrobené len selektívne časti s cieľom lepšie pochopiť jeho podstatu a funkciu, pričom metódou syntézy sa následne poukázalo na súvislosti medzi zložkami jednotlivých opatrení balíka ViDA.

Kľúčové slová: balík ViDA, DPH, platformová ekonomika, služby krátkodobého prenájmu ubytovania, služby cestnej prepravy cestujúcich

Abstract: The author focuses in her contribution on the package of measures concerning value added tax in the digital age, the so – called ViDA package (VAT in the Digital Age). The aim of the contribution is to clarify certain provisions of the legislative acts of the ViDA package, with a focus on digital platforms providing short – term accommodation rental services and passenger transport services by road. The main objective was to point out the

¹ Univerzita Komenského v Bratislave, Právnická fakulta

possible interpretative discrepancies arising from the understanding of some Member States, which may lead to risks of differing application by individual Member States. The author highlights open questions arising from potential model situations likely to occur in practice in the future, whose interpretation the European Commission plans to clarify through explanatory notes. In conclusion, it can be stated that proper implementation of the measures from the ViDA package should contribute to a higher and more efficient collection of VAT. On the one hand, the administrative burden will be reduced through the introduction of a single VAT registration, but on the other hand, it will be increased by the introduction of record – keeping obligations for digital platforms. In interpreting the legislative acts within the ViDA package, the methods of deduction and comparison were used. From the set of ViDA package measures, which forms a comprehensive whole, only selective parts were analyzed to better understand its nature and function. Subsequently, the synthesis method was used to demonstrate the interconnections between the components of the individual ViDA measures.

Key words: ViDA package, VAT, platform economy, short – term accommodation rental services, passenger transport services by road

Úvod

Dňa 11. marca 2025 Rada Európskej únie (ďalej len „Rada EÚ“) prijala súbor opatrení v oblasti dane z pridanej hodnoty (ďalej len „DPH“) v digitálnom veku tzv. legislatívny balík ViDA (v preklade „DPH v digitálnom veku“)². Balík ViDA bol zverejnený v Úradnom vestníku Európskej Únie dňa 25. marca 2025. Predmetný balík ViDA tvoria tri legislatívne akty, a to smernica Rady (EÚ) 2025/516, ktorou sa mení smernica 2006/112/ES, pokiaľ ide o pravidlá DPH pre digitálny vek (ďalej len „smernica ViDA“), nariadenie Rady (EÚ) 2025/517, ktorým sa mení nariadenie (EÚ) č. 904/2010, pokiaľ ide o opatrenia administratívnej spolupráce v oblasti DPH potrebné pre digitálny vek (ďalej len „nariadenie ViDA“) a vykonávacie nariadenie Rady (EÚ) 2025/518, ktorým sa mení vykonávacie nariadenie (EÚ) č. 282/2011, pokiaľ ide o požiadavky na informácie pri určitých úpravách DPH (ďalej len „vykonávacie nariadenie ViDA“). Opatrenia v oblasti DPH v digitálnom veku vyplývajúce z legislatívneho balíka ViDA sú členské štáty Európskej únie (ďalej len „EÚ“) povinné postupne zavádzať do svojich vnútroštátnych právnych poriadkov s finálnym termínom zavedenia zmien do januára roku 2035. Legislatívne začiatky tohto balíka však siahajú až do roku 2022, kedy bol predstavený Európskou komisiou.

² ViDA – v anglickom jazyku znamená „VAT in the digital age“, v preklade do slovenského jazyka znamená „DPH v digitálnom veku“.

Balík ViDA predstavuje súbor opatrení navrhovaných Európskou úniou, ktorý má reagovať na aktuálne výzvy digitálnej ekonomiky. Cieľom balíka ViDA je modernizácia a zefektívnenie systému DPH, ktorá má priniesť zníženie daňových podvodov a administratívnej záťaže prostredníctvom zavedenia povinnej elektronickej fakturácie v reálnom čase. Ďalším účelom je zabezpečenie rozšírenia využitia digitálnych platforiem na uľahčenie dodania a zavedenie jednotnej registrácie pre DPH v rámci schém tzv. One Stop Shop (ďalej len „OSS“) a tzv. Import One – Stop Shop (ďalej len „iOSS“). V rámci zmien, ktoré prinesie balík ViDA budú musieť členské štáty zaviesť v národných legislatívach povinnú elektronickú fakturáciu za ustanovených podmienok a taktiež sa zavedú vylepšenia systému iOSS na posilnenie kontroly členských štátov.

Príspevok má za cieľ identifikovať otvorené otázky v aplikačnej praxi na modelových situáciách, ktorých interpretáciu v budúcnosti objasní Európska komisia prostredníctvom svojich vysvetľujúcich poznámok. Aplikovaný metodický prístup zahŕňa metódy komparácie, dedukcie, analýzy a čiastočne syntézy. Na predmetnú tému doposiaľ neboli publikované odborné a vedecké články v rozsahu poskytujúcom v značnej miere nové poznatky z oblasti aplikačných problémov fungovania digitálnych platforiem pri sprostredkovaní určitých služieb krátkodobého prenájmu ubytovania do 30 nocí a služieb cestnej prepravy cestujúcich.

Tri piliere balíka ViDA

Balík opatrení ViDA pozostáva z troch hlavných pilierov.

Pilier I zavádza povinnosť digitálneho vykazovania transakcií v reálnom čase (v preklade Digital Reporting Requirements³) na základe elektronickej fakturácie. Primárne sa jedná o požiadavku na digitálne oznamovanie údajov o intrakomunitárnych zdaniteľných obchodoch a požiadavku na zabezpečenie interoperability.

Pilier II zavádza koncept domnelého dodávateľa (v preklade Deemed Supplier Regime⁴) v platformovej ekonomike. Jedná sa o požiadavku na digitálne platformy v sektore dopravy pri poskytovaní služieb cestnej prepravy cestujúcich a v sektore ubytovacích služieb pri poskytovaní služieb krátkodobého prenájmu ubytovania⁵, aby účtovali DPH namiesto základného dodávateľa.

³ Zaužívaná skratka „DRR“.

⁴ Zaužívaná skratka „DSR“.

⁵ Podľa čl. 28a ods. 1 smernice Rady o spoločnom systéme dane z pridanej hodnoty 2006/112/ES s účinnosťou od 1. júla 2028 sa za služby krátkodobého prenájmu ubytovania považuje neprerušený prenájom ubytovania tej istej osobe na maximálne 30 nocí. Toho času sa jedná o čl. 3 ods. 1 smernice ViDA.

Pilier III zavádza jednotnú registráciu pre DPH (v preklade Single VAT Registration⁶) v celej EÚ. Toto opatrenie má za cieľ zníženie potreby povinnej registrácie pre DPH v inom členskom štáte.

„To, či členské štáty EÚ zavedú povinnosti týkajúce sa tuzemskej elektronickej fakturácie a digitálneho vykazovania transakcií v reálnom čase od 1. januára 2028 alebo neskôr, závisí od pravidiel, ktoré prijímú samotné členské štáty, a stále to môže viesť k rozdielnemu systému digitálneho vykazovania transakcií o DPH v celej EÚ, hoci rozdiely budú menšie kvôli štandardu EÚ, ktorý je potrebné uplatniť.“⁷

Fázovanie legislatívnych zmien

Ihneď po nadobudnutí platnosti balíka ViDA mohli členské štáty za určitých stanovených podmienok zaviesť povinnú elektronickú fakturáciu a taktiež sa zaviedli vylepšenia systému iOSS na posilnenie kontroly členských štátov.

Od 1. januára 2027 budú uplatňované menšie relevantné legislatívne zmeny, ktoré prinesú také objasnenia, ktoré budú mať pozitívny dopad na používateľov schém OSS a iOSS.

Od 1. júla 2028 budú môcť členské štáty uplatňovať opatrenia týkajúce sa domnelého dodávateľa pre platformovú ekonomiku pri poskytovaní služieb cestnej prepravy cestujúcich a pri poskytovaní služieb krátkodobého prenájmu ubytovania. Avšak platí tu výnimka, že členské štáty môžu implementáciu odložiť do 1. januára 2030. Súčasne v tomto momente nadobudne účinnosť aj reforma jednotnej registrácie pre DPH. Tiež dôjde k rozšíreniu schémy OSS. Prelomovým opatrením bude povinné uplatňovanie systému prenosu daňovej povinnosti⁸ pre neidentifikovaných dodávateľov.

Od 1. júla 2030 vstúpia do účinnosti opatrenia týkajúce sa povinnosti digitálneho vykazovania transakcií v reálnom čase na základe elektronickej fakturácie. Tieto opatrenia budú mať hlavne vplyv na podniky uskutočňujúce cezhraničné dodanie typu business-to-business (ďalej len ako „B2B“).

Do 1. januára 2035 je stanovený termín pre členské štáty na zosúladenie povinnosti digitálneho vykazovania tuzemských transakcií v reálnom čase zavedenej v ich národných legislatívach pred 1. januárom 2024 so systémom EÚ vyplývajúcim z právnych noriem EÚ, čím sa uskutoční záverečná fáza tohto komplexného balíka ViDA.

⁶ Zaužívaná skratka „SVR“.

⁷ HEINEMANN, M. - STILLER, W.: Digitalization and cross-border tax fraud: evidence from e-invoicing in Italy. *International Tax and Public Finance* (2025). eISSN 1573-6970. s. 8 [online]. [cit. 19-09-2025] Dostupné na internete: <https://www.1webofscience-1com-1g8dbuk310oe4.han5.savba.sk/wos/woscc/full-record/WOS:001171150300001>.

⁸ Prenos daňovej povinnosti je tiež známy ako „mechanizmus Reverse Charge“.

Schémy OSS a iOSS

Schéma OSS predstavuje osobitnú úpravu dane, ktorá je v platnosti od 1. júla 2021. Jedná sa o koncept jednotného kontaktného miesta. Táto schéma je určená pre podnikateľov, ktorí predávajú tovar alebo služby konečným zákazníkom, resp. osobám bez identifikačného čísla pre DPH (ďalej len „IČ DPH“) v iných členských štátoch EÚ. Typicky sa predovšetkým jedná o napr. e – shopy.

Schéma iOSS predstavuje osobitnú úpravu dane, ktorá je v platnosti od 1. júla 2021. Jedná sa o koncept jednotného kontaktného miesta pre dovoz. Táto schéma umožňuje podať jediné daňové priznanie k DPH za transakcie podliehajúce DPH vo viacerých členských štátoch EÚ. Pri uplatňovaní tejto osobitnej úpravy odpadá povinnosť podať samostatné daňové priznanie k DPH v jednotlivých členských štátoch EÚ. Je to systém EÚ, ktorý má za cieľ zjednodušiť výber a platbu DPH pri predaji tovaru na diaľku (v preklade Distance Sales of Imported Goods⁹) z krajín mimo EÚ zákazníkom v EÚ. Umožňuje predajcom vybrať DPH pri predaji od zákazníka, zaplatiť ju raz prostredníctvom jediného portálu a zabrániť tak, aby zákazníci platili DPH a poplatky pri dovoze.

Aj tu však platia obmedzenia, nakoľko takúto osobitnú úpravu môžu využívať iba dodávatelia tovaru na diaľku s hodnotou tovaru nepresahujúcou prah 150 eur, ktorý je zasielaný alebo dovážaný do EÚ z územia tretích štátov pre zákazníkov, resp. osoby neidentifikované pre DPH. Taktiež sa týka len tovaru, ktorý nie je predmetom spotrebnej dane. Ďalej môžu túto osobitnú úpravu využívať iba prevádzkovatelia elektronického rozhrania, ktorí síce nie sú priamymi dodávateľmi tovaru, ale vo svojej podstate uľahčujú dodávanie tovaru na diaľku dovážaného z tretích štátov pôvodným vyššie uvedeným dodávateľom, a z tohto dôvodu sa považujú za dodávateľov tovaru na diaľku. Vzťahuje sa na sprostredkovateľov, ktorí sú poverenými osobami len na podávanie daňových priznaní k iOSS a na úhrady platieb DPH z predaja tovaru s hodnotou nepresahujúcou 150 eur, ktorý je dovážaný z tretích krajín zákazníkom z EÚ vyššie uvedenými dodávateľmi tovaru na diaľku alebo prevádzkovateľmi elektronického rozhrania, a to v ich mene a na ich účet.

Digitálne platformy

„Platformy sú prostredia, ktoré uľahčujú výmeny medzi inak oddelenými entitami.¹⁰ Napríklad softvérové platformy uľahčujú výmenu údajov medzi počítačmi; platformy sociálnych médií uľahčujú výmenu obsahu medzi ľuďmi, a (online) obchodné

⁹ Zaužívaná skratka „DSIG“.

¹⁰ Lamensch, M., et al. (2021). New EU VAT-related obligations for e-commerce platforms worldwide: A qualitative impact assessment. World Tax Journal, 13(3), 441-479. <https://doi.org/10.59403/15yff24>. In: ISMER, R.: And They Lived Happily Ever After? Future Challenges for E-invoicing and Digital Reporting After the Adoption of the ViDA Package. Ec Tax Revue, 2025-2. eISSN 1875-8363 s. 2.

platformy alebo trhoviská uľahčujú výmenu tovarov a služieb. Obchodný model platformy tak vytvára hodnotu prepojením kupujúcich a predávajúcich. Sieťový efekt zohráva kľúčovú úlohu. V skutočnosti, čím viac kupujúcich a predávajúcich je na platforme, tým väčšiu hodnotu vytvára pre obe strany.¹¹¹²

Model domnelého dodávateľa

Model domnelého dodávateľa sa pre oblasti poskytovania služieb cestnej prepravy cestujúcich a poskytovania služieb krátkodobého prenájmu ubytovania definuje ako digitálna platforma, ktorá sa podieľa na spojení zákazníka s poskytovateľom služieb cestnej prepravy cestujúcich a služieb krátkodobého prenájmu ubytovania pri uskutočnení transakcií týkajúcich sa takýchto služieb. Domnelý dodávateľ sa v takomto prípade stáva osobou povinnou platiť daň.

Nejedná sa však o nový typ právnej fikcie v rámci systému DPH. Táto právna fikcia už bola zavedená aj v prípade pravidiel DPH v oblasti elektronického obchodu (v preklade e – commerce), a to v zmysle čl. 14a smernice Rady o spoločnom systéme dane z pridanej hodnoty 2006/112/ES (ďalej len „smernica o DPH“), kedy sa z digitálnej platformy v niektorých situáciách vytvoril domnelý dodávateľ.

Podľa čl. 14a ods. 1 smernice o DPH s účinnosťou od 1. januára 2027 ak zdaniteľná osoba uľahčuje predaj tovaru na diaľku dovážaného z tretích území alebo tretích krajín v zásielkach so skutočnou hodnotou nepresahujúcou 150 eur prostredníctvom použitia elektronických rozhraní, ako sú trhoviská, platformy, portály alebo podobné prostriedky, táto zdaniteľná osoba sa považuje za osobu, ktorá tento tovar sama prijala a dodala.¹³ Podľa čl. 14a ods. 2 smernice o DPH ak zdaniteľná osoba v rámci EÚ prostredníctvom elektronických rozhraní uľahčuje dodanie tovaru zdaniteľnou osobou neusadenou v EÚ pre nezdaniteľnú osobu, táto zdaniteľná osoba sa považuje na osobu, ktorá tento tovar sama prijala a dodala.¹⁴ S účinnosťou od 1. januára 2027 sa pôsobnosť tohto čl. 14a ods. 2 smernice o DPH rozširuje o dodanie tovaru aj pre

¹¹ OECD, (2019). An introduction to online platforms and their role in the digital transformation (p. 23). OECD Publishing. <https://doi.org/10.1787/53e5f593-en>; Filistrucchi, L., Geradin, D., & Van Damme, E. (2012). Identifying two-sided markets (TILEC Discussion Paper No. DP 2012-008, p. 2); Katz, M., & Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives*, 8(2), 93-115. In ISMER, R.: And They Lived Happily Ever After? Future Challenges for E-invoicing and Digital Reporting After the Adoption of the ViDA Package. *Ec Tax Revue*, 2025-2. eISSN 1875-8363 s. 2.

¹² ISMER, R.: And They Lived Happily Ever After? Future Challenges for E-invoicing and Digital Reporting After the Adoption of the ViDA Package. *Ec Tax Revue*, 2025-2. eISSN 1875-8363 s. 2 [online]. [cit. 19-09-2025 Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001489270400001>.

¹³ Toho času sa jedná o čl. 2 ods. 1 smernice ViDA.

¹⁴ V slovenskom právnom poriadku transponované do ust. § 8 ods. 7 zákona č. 222/2004 Z. z. zákon o dani z pridanej hodnoty.

zdaniteľnú osobu a nezdaniteľnú právnickú osobu, ktorej nadobudnutia tovaru nepodliehajú DPH podľa čl. 3 ods. 1 smernice o DPH.

Cieľom ustanovenia o domnelom dodávateľovi je zabezpečiť výber dane v situácii, kedy je zložité vybrať daň od základného dodávateľa z dôvodu jeho usadenia v treťom štáte alebo s cieľom bojovať proti daňovým podvodom, v prípade ak sa tovar neusadeného dodávateľa nachádza v rôznych skladoch v EÚ a premiestňuje sa do iných členských štátov.

Funkcia platformovej ekonomiky v oblasti poskytovania služieb cestnej prepravy cestujúcich a poskytovania služieb krátkodobého prenájmu ubytovania sa posilňuje, najmä čo sa týka zabezpečenia výberu DPH zjednodušeným spôsobom, nakoľko je jednoduchšie vybrať DPH od sprostredkovateľa a nezaťažiť základných poskytovateľov, a tým pádom dochádza aj k odstráneniu narúšania hospodárskej súťaže.

Domnelý dodávateľ podľa čl. 28a smernice o DPH

V čl. 28a smernice o DPH s účinnosťou od 1. júla 2028 sa definuje základný model výberu DPH od digitálnych platforiem. V tomto článku sa ustanovuje, že zdaniteľná osoba, ktorá prostredníctvom použitia elektronických rozhraní, ako sú trhoviská, platformy, portály alebo podobné prostriedky, v rámci EÚ uľahčuje poskytovanie, služieb krátkodobého prenájmu ubytovania, konkrétne neprerušený prenájom ubytovania tej istej osobe na maximálne 30 nocí, alebo poskytovanie služieb cestnej prepravy cestujúcich, sa považuje za osobu, ktorá tieto služby sama prijala a poskytla. S výnimkou prípadov, keď osoba poskytujúca tieto služby poskytla zdaniteľnej osobe, ktorá uľahčuje poskytovanie služby, svoje identifikačné číslo na účely DPH pridelené v členských štátoch, v ktorých sa poskytnutie uskutočňuje, alebo identifikačné číslo, ktoré jej bolo pridelené v súlade s čl. 362 alebo s čl. 369d smernice o DPH a zároveň táto osoba oznámila zdaniteľnej osobe, ktorá uľahčuje poskytovanie služby, že uplatní akúkoľvek DPH splatnú za dané poskytnutie služby. Článkom 28a smernice o DPH s účinnosťou od 1. júla 2028 dochádza k zavedeniu modelu tzv. domnelého dodávateľa, ktorý bude fungovať na dichotómii a to tak, že z jednej transakcie, ktorou je poskytovanie služieb cestnej prepravy cestujúcich a poskytovanie služieb krátkodobého prenájmu ubytovania prostredníctvom digitálnej platformy pre zákazníka, sa právnou fikciou vytvoria dve samostatné transakcie. Prvá transakcia sa uskutoční medzi základným poskytovateľom služieb cestnej prepravy cestujúcich a služieb krátkodobého prenájmu ubytovania a digitálnou platformou. V tomto prípade sa jedná o transakciu, ktorá je na strane poskytovateľa služieb cestnej prepravy cestujúcich a služieb krátkodobého prenájmu ubytovania oslobodená od dane podľa čl. 136b smernice o DPH¹⁵ s účinnosťou od 1. júla 2028.

¹⁵ Toho času sa jedná o čl. 3 ods. 4 smernice ViDA.

Druhá transakcia sa uskutoční medzi digitálnou platformou a konečným zákazníkom. V tomto prípade sa jedná o transakciu, ktorá bude podliehať DPH.

Predmetným rozdelením pôvodnej transakcie sa z digitálnej platformy defacto vytvoril domnelý dodávateľ so všetkými právami a povinnosťami platiteľa dane. Dôsledkom toho, že platforma bude poskytovať služby cestnej prepravy cestujúcich a poskytovať služby krátkodobého prenájmu ubytovania zdaňovať, sa zabezpečí rovnaký režim DPH, ako v súčasnosti uplatňujú hotely a taxislužby, čím už nebude dochádzať k narúšaniu hospodárskej súťaže.

Model domnelého dodávateľa neuplatní platforma len v prípade, ak je základným poskytovateľom služieb cestnej prepravy cestujúcich a služieb krátkodobého prenájmu ubytovania jedna z osôb, uvedených v čl. 28a v písmene a) smernice o DPH. V prípade, ak by mal základný poskytovateľ služieb cestnej prepravy cestujúcich a služieb krátkodobého prenájmu ubytovania pridelené IČ DPH, sa ekonomická platforma nestane domnelým dodávateľom a uplatní DPH len zo služby uľahčenia, resp. sprostredkovania.

Smernica ViDA v časti platformového hospodárstva explicitne nevyklučuje uplatňovanie osobitnej úpravy pre malé a stredné podniky. Uvedené znamená, že v prípade ak sa členský štát domnieva, že na jeho území nedochádza k narušeniu hospodárskej súťaže, môže vylúčiť z tohto pravidla zdaniteľné osoby, ktoré na jeho území využívajú osobitnú úpravu pre malé podniky.

„Podľa článku 5c vykonávacieho nariadenia o DPH platforma nebude zodpovedná za nedoplatok na DPH, ak dostala nesprávne informácie od pôvodného dodávateľa (alebo od akejkoľvek tretej strany) a je „závislá“ od týchto informácií a „môže preukázať, že nevedela a nemohla rozumne vedieť, že tieto informácie boli nesprávne“. Dôkazné bremeno teda nesie platforma.“¹⁶

Implementácia platformovej ekonomiky

Pre správnu implementáciu platformovej ekonomiky je potrebné zabezpečiť spoločné a rovnaké chápanie pojmov vyplývajúcich z balíka ViDA všetkými členskými štátmi EÚ. Takýto výklad je zväčša poskytovaný prostredníctvom tzv. vysvetľujúcich poznámok (v preklade Explanatory notes), ktoré sú vypracované Európskou komisiou spoločne s expertami z členských štátov a so zástupcami z expertnej skupiny

¹⁶ MERKX, M. et al.: Qualitative Assessment of Two Recent EU Commission Proposals to Impose (More) VAT Obligations on Platforms. World Tax Journal, 2024 -16. -53. eISSN 2352-9237.s. 15 [online]. [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001513981800001>.

pre DPH (v preklade VAT Expert Group)¹⁷ (ďalej len „VEG“) a zo skupiny pre budúcnosť DPH (v preklade Group on the future of VAT)¹⁸ (ďalej len „GFV“).

V septembri 2025 sa v Madride uskutočnil workshop v rámci programu Fiscalis k téme implementácie platformovej ekonomiky v kontexte balíka ViDA, kde boli v rámci modelových situácií expertami z národných administratív, z Európskej komisie a zástupcami súkromného sektora analyzované potencionálne situácie, ktoré môžu v budúcnosti v praxi vzniknúť. V priebehu roka 2026 sú naplánované práce na vysvetľujúcich poznámkach prostredníctvom konzultácií v skupinách VEG a GFV. Na prvý štvrtrok roku 2027 je naplánovaná finalizácia a následné zverejnenie vyššie uvedených vysvetľujúcich poznámok. Do 30. júna 2028 majú členské štáty povinnosť prijať a zverejniť potrebné právne predpisy vo svojich vnútroštátnych právnych poriadkoch, ktoré zabezpečia riadnu a správnu implementáciu opatrení vyplývajúcich z balíka ViDA. Od 1. júla 2028 tieto opatrenia nadobudnú účinnosť.

Teoretické problémy vyplývajúce z balíka ViDA – čl. 28 smernice o DPH verzus čl. 28a smernice o DPH

Z opatrení vyplývajúcich z balíka ViDA, ktoré budú postupne zavedené členskými štátmi, vystavajú už pred vydaním vysvetľujúcich poznámok rôzne teoretické problémy, ktoré môžu byť v praxi neraz rôzne riešené. Autorka v nasledujúcej časti príspevku nastoľuje otázky k teoretickým problémom a prezentuje vlastné názory na ich riešenia, ktoré nemusia byť zhodné s konečnými riešeniami prijatými v budúcnosti.

Ako spolu súvisia čl. 28 smernice o DPH a čl. 28a smernice o DPH ? Je možné stanoviť hranicu medzi čl. 28 smernice o DPH a čl. 28a smernice o DPH ?

Čl. 28 smernice o DPH definuje klasickú situáciu sprostredkovania, ak zdaniteľná osoba koná vo vlastnom mene, ale na účet inej osoby, považuje sa, že sama dostala a dodala tovar alebo službu. Čl. 28a smernice o DPH (čl. 3 ods. 1 smernice ViDA) je špeciálne ustanovenie pre digitálne platformy pri sprostredkovaní určitých služieb krátkodobého prenájmu ubytovania do 30 nocí a služieb cestnej prepravy cestujúcich. Čl. 28 smernice o DPH ustanovuje všeobecné pravidlo (to platí pre všetky prípady sprostredkovania). Čl. 28a smernice o DPH je právna úprava *lex specialis* pre digitálne platformy. Tento článok zakladá automaticky postavenie domnelého

¹⁷ Zaužívaná skratka „VEG“. Je expertná skupina pre DPH je poradným orgánom Európskej komisii a poskytuje jej poznatky o príprave nových legislatívnych aktov a iných politických iniciatív a o praktickom vykonávaní právnych predpisov v oblasti DPH.

¹⁸ Zaužívaná skratka „GFV“. Je súbor neformálnych expertných skupín Európskej komisie zložených zo zástupcov národných daňových správ. Poskytuje Európskej komisii fórum pre konzultácie s expertmi na DPH z členských štátov o predlegislatívnych iniciatívach.

dodávateľa bez ohľadu na právnu kvalifikáciu sprostredkovateľskej zmluvy. Ak ide o digitálnu platformu, použije sa čl. 28a smernice o DPH. Ak ide o klasické sprostredkovanie, napr. cestovná agentúra predáva lístky iného dopravcu na základe mandátnej zmluvy, použije sa čl. 28 smernice o DPH.

Je možné stanoviť hranicu medzi čl. 28a smernice o DPH a osobitnou úpravou pre cestovné kancelárie (TOMS¹⁹) podľa čl. 306 a nasl. smernice o DPH ?

Osobitná úprava pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH sa uplatňuje, ak zdaniteľná osoba koná vo vlastnom mene a využíva služby tretích strán (napr. hotel alebo doprava) na poskytovanie komplexného balíka. Čl. 28a smernice o DPH sa vzťahuje iba na digitálne platformy sprostredkujúce samostatné služby krátkodobého prenájmu ubytovania do 30 nocí a služieb cestnej prepravy cestujúcich. V prípade ak digitálna platforma predáva balíčky (napr. dovolenky alebo zájazdy) uplatní sa osobitná úprava pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH. Ak digitálna platforma sprostredkuje len jednu službu krátkodobého prenájmu ubytovania do 30 nocí alebo službu cestnej prepravy cestujúcich uplatní sa čl. 28a smernice o DPH. Je vhodné objasniť, že osobitná úprava pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH sa neuplatní na čistý marketplace typu Booking alebo Airbnb, ale uplatní sa na cestovnú kanceláriu organizujúcu dovolenkový zájazd. Osobitná úprava pre cestovné kancelárie a cestovné agentúry je upravená v ust. § 65 zákona č. 222/2004 Z. z. zákon o dani z pridanej hodnoty (ďalej len „zákon o DPH“).

Môže sa uplatniť režim domnelého dodávateľa, ak sú splnené podmienky na uplatnenie osobitnej úpravy pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH ?

Režim domnelého dodávateľa a režim osobitnej úpravy pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH sa navzájom vylučujú. Ak zdaniteľná osoba spĺňa podmienky pre osobitnú úpravu pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH, to znamená, že poskytuje balíček služieb, tak čl. 28a smernice o DPH sa neuplatní. Čl. 28a smernice o DPH je určený na digitálne sprostredkovanie samostatných služieb, nie na komplexné cestovné balíky.

Existuje spôsob, ako môže digitálna platforma zistiť, či by mal základný dodávateľ používať osobitnú úpravu pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH ?

¹⁹ TOMS je zjednodušujúce opatrenie, ktoré umožňuje poskytnutie balíka služieb ako jedného plnenia.

Digitálna platforma si musí vyžiadať od dodávateľa (napr. hotela alebo cestovnej kancelárie) informáciu o tom, či predáva balík služieb podľa osobitnej úpravy pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH alebo len samostatnú službu krátkodobého prenájmu ubytovania do 30 nocí alebo službu cestnej prepravy cestujúcich. Právnu zodpovednosť za správne uplatnenie osobitnej úpravy pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH nesie základný dodávateľ, nie digitálna platforma. Digitálna platforma má povinnosť viesť presné záznamy v zmysle vykonávacieho nariadenia ViDA (napr. údaje o identite dodávateľa alebo povahe služby). Nie je možné, aby si digitálna platforma sama určila, či bude uplatňovať aplikáciu osobitnej úpravy pre cestovné kancelárie (TOMS) podľa čl. 306 a nasl. smernice o DPH. Rozhodnutie o výbere režimu je výlučne na základnom dodávateľovi.

Záver

V rámci procesu implementácie opatrení vyplývajúcich z balíka ViDA týkajúcich sa digitálnych platforiem poskytujúcich služby krátkodobého prenájmu ubytovania a služby cestnej prepravy cestujúcich je potrebné objasnenie niektorých ustanovení legislatívnych aktov tohto balíka. Závažným problémom sa javia možné výkladové odchýlky vznikajúce v chápaní niektorých členských štátov, ktoré môžu priniesť riziká rozdielného uplatňovania jednotlivými členskými štátmi. V súčasnej dobe vystali otvorené otázky, ktoré vychádzajú z potenciálnych modelových situácií pravdepodobne sa vyskytujúcich v budúcnosti v praxi a ktorých interpretáciu Európska komisia plánuje objasniť prostredníctvom vysvetľujúcich poznámok.

Záverom je možné konštatovať, že riadna implementácia opatrení z balíka ViDA by mala prispieť k vyššiemu a efektívnejšiemu výberu DPH. Na jednej strane dôjde k zníženiu administratívnej záťaže zavedením jednotnej registrácie pre DPH, avšak na strane druhej dôjde k jej zvýšeniu zavedením záznamovej povinnosti pre digitálne platformy. Možno sa tak domnievať, že balík ViDA sa bude javiť pre súkromný sektor ako výhoda, no zároveň aj ako nevýhoda. Rovnováhu medzi novými povinnosťami a oprávneniami prinesie len prax.

Aktuálne ustanovenia o domnelých dodávateľoch už majú značný prevádzkový vplyv na digitálne platformy pôsobiace v sektore business-to-customer (ďalej len ako „B2C“) vrátane nových fakturačných povinností. Potreba digitálnych platforiem zaviesť nové interné procesy na určenie základných transakcií, resp. či zdaniteľné osoby konajú alebo nekonajú ako domnelí dodávatelia, a pokiaľ možno zrážať DPH z transakcií a organizovať vrátenie dane sa javí ako administratívna záťaž. Toto všetko spôsobuje nové náklady a riziká a pravdepodobne to bude mať vplyv na fungovanie obchodného modelu digitálnych platforiem. Prínosom je posilnenie

nástrojov v boji proti daňovým podvodom a daňovým únikom a odstránenie deformácie hospodárskej súťaže.

Zoznam použitej literatúry

1. ISMER, R.: And They Lived Happily Ever After? Future Challenges for E-invoicing and Digital Reporting After the Adoption of the ViDA Package. *Ec Tax Revue*, 2025-2. eISSN 1875-8363. [online]. [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001489270400001>.
2. MERKX, M. et al.: Qualitative Assessment of Two Recent EU Commission Proposals to Impose (More) VAT Obligations on Platforms. *World Tax Journal*, 2024 -16. -53. eISSN 2352-9237. [online]. [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001513981800001>.
3. HEINEMANN, M. - STILLER, W.: Digitalization and cross-border tax fraud: evidence from e-invoicing in Italy. *International Tax and Public Finance* (2025). eISSN 1573-6970. s. 8 [online]. [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001171150300001>.
4. MERKX, M. et al.: VAT in the Digital Age Package: Viva la ViDA or Livin' la ViDA Loca? *EC Tax Review*, 2023, s. 127-141. [online] [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e4.han5.savba.sk/wos/woscc/full-record/WOS:001009540000005>.
5. PANTAZATOU, K.: Why EU revenue matters: A case for an EU digital levy. *European Law Open*. 2024-3. [online] [cit. 19-09-2025] Dostupné na internete: <https://www.cambridge.org/core/journals/european-law-open/article/why-eu-revenue-matters-a-case-for-an-eu-digital-levy/C654A73689FoECEDB4032DBD6542BA76>.
6. MERKX, M. et al.: VAT in the Digital Age Package: Singling Out the Single VAT Registration. *EC Tax Review*. 2023-32. eISSN1875-8363. [online] [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e7.han5.savba.sk/wos/woscc/full-record/WOS:001050611300004>.
7. YORDANOVA, Z.: Role of Artificial Intelligence in Facilitating Open Innovation in VAT Management. In *Supply Chains Olympus International Conference*. 2024. ISSN1865-0929. [online] [cit. 19-09-2025] Dostupné na internete: <https://link-1springer-1com-1g8dbukh71b45.han5.savba.sk/book/10.1007/978-3-031-69344-1>.
8. ISMER, R.: Tax Technology for the European Union. *Ec Tax Revue*, 2023-6. eISSN 1875-8363. [online]. [cit. 19-09-2025] Dostupné na internete:

<https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\ECTA\ECTA2023029.pdf>.

9. ZIELINSKI, R. et al.: Growing impact of third-parties in VAT taxation - insights from digital platforms. JOHN PAUL II CATHOLIC UNIV LUBLINAL RACLAWICKIE 14, LUBLIN 2024. eISSN 2719-4264. [online] [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e7.han5.savba.sk/wos/woscc/full-record/WOS:001382908600010>.
10. ALLUNHAYDAN, AS.: Electronic invoicing and it's impact on tax compliance. AL-BAYADER-AL-RAWNAQ NEIGHBORHOOD ABDULLAH AL SHAHWAN ST. JORDAN. 2025. eISSN 2518-5551. [online] [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e7.han5.savba.sk/wos/woscc/full-record/WOS:001545150400003>.
11. MERKX, M.: Rendering Platforms Liable for VAT and Import Duties: Desperate Times Call for Desperate Measures, but What about Proper Checks and Balances? EC Tax Review, 2024-33. eISSN 1875-8363. s. 185-196 [online] [cit. 19-09-2025] Dostupné na internete: <https://www-1webofscience-1com-1g8dbuk3100e7.han5.savba.sk/wos/woscc/full-record/WOS:001366254300002>.
12. DANCÁK, J.: Elektronická fakturácia a digitálne oznamovanie v kontexte smernice ViDA. Bulletin SKDP, 2025-3. s. 10-18. ISSN 2644-688X. [online] [cit. 19-09-2025] Dostupné na internete: https://new.skdp.sk/sites/default/files/2025-09/SKDP_3_2025_web.pdf.

Kontaktné údaje

JUDr. Aneta Kollman Steinhüblová

steinhublov1@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

FINANČNÉ PRÁVO V DIGITÁLNOH VEKU: AKO REGULÁTORI ČELIA NÁRASTU ONLINE PODVODOV¹

FINANCIAL LAW IN THE DIGITAL AGE: HOW REGULATORS CONFRONT THE RISE OF ONLINE FRAUD

Peter Beňo²

Abstrakt: Príspevok skúma, ako súčasný a navrhovaný európsky rámec platobných služieb reaguje na online platobné podvody a kde pretrvávajú regulačné nedostatky. Cieľom je presne vymedziť pojem online platobného podvodu vo väzbe na súhlas platiteľa a na rozdiel medzi neautorizovanými a autorizovanými platobnými operáciami. Metodologicky text kombinuje doktrínálnu analýzu právnych predpisov a regulačných dokumentov s komparáciou pripravovaného balíka a poukázaním na aplikačnú prax poskytovateľov platobných služieb. Zistenia ukazujú nejednotnosť pri posudzovaní hrubej nedbanlivosti, nerovnováhu v rozdelení dôkazných bremien a nedostatky v úprave transakčného monitoringu. Súčasne sa potvrdzuje dôležitosť inštitútov ako verifikácia príjemcu a tiež výmeny údajov medzi poskytovateľmi platobných služieb pre prevenciu a včasnú detekciu podvodov, pričom pripravované zmeny smerujú k zosilneniu priebežného monitorovania a k štandardizovanejším preventívnym povinnostiam. Vedeckým prínosom je konceptuálne ukotvenie online platobného podvodu prostredníctvom kategórie skutočný verzus vylákaný súhlas a jeho prepojenie na procesné a dôkazné štandardy. Praktickým prínosom je rámec odporúčaní pre poskytovateľov a dohliadacie orgány, zameraný na nastavenie monitoringu, verifikácie príjemcu a zdieľania informácií s cieľom znížiť mieru podvodov a zefektívniť alokáciu zodpovednosti.

Kľúčové slová: online, podvody, scam, fraud, phishing, platby

Abstract: The article examines how the current and proposed European framework for payment services addresses online payment fraud and where regulatory gaps persist. Its aim is to define the concept of online payment fraud with reference to the payer's consent and the distinction between

¹ Článok vznikol v rámci realizácie projektu VEGA 1/0212/23 Finančné inovácie ako determinant súčasnej a anticipovanej regulácie na finančnom trhu (výzvy a riziká)

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

unauthorised and authorised payment transactions. Methodologically, the text combines doctrinal analysis of legislation and regulatory documents with a comparison of the forthcoming package and observations on the application practices of payment service providers. The findings indicate inconsistency in the assessment of gross negligence, an imbalance in the allocation of evidentiary burdens, and shortcomings in the regulation of transaction monitoring. At the same time, the importance of instruments such as payee verification and data sharing among payment service providers is confirmed for prevention and timely detection of fraud, while the proposed changes move toward strengthened ongoing monitoring and more standardised preventive obligations. The scientific contribution lies in the conceptual anchoring of online fraud through the category of genuine versus induced consent and its linkage to procedural and evidentiary standards. The practical contribution is a set of recommendations for providers and supervisory authorities focused on configuring monitoring, payee verification, and information sharing to reduce fraud and streamline the allocation of liability.

Key words: online, fraud, scam, phishing, payments

Úvod

Digitalizácia platieb zásadne zmenila spôsob, akým sa pohybujú peniaze, aj spektrum rizík, ktorým používatelia a poskytovatelia platobných služieb čelia.³ Podvodníci sa dnes čoraz menej spoliehajú na technické obchádzanie systémov a čoraz viac útočia na človeka a na jeho pozornosť, rozhodovanie a dôveru.⁴ Dochádza tak tomu, že transakcie, ktoré technicky vyzerajú bezchybne a prejdú silnou autentifikáciou klienta (ďalej len „SCA“)⁵, môžu byť výsledkom sofistikovanej manipulácie. Nové formy online podvodov teda ukazujú, že riziko tejto formy kriminality sa nedá merať len technickou bezchybnosťou transakcie. Naším cieľom je

³ Napr. HARASIM, Janina – KLIMONTOWICZ, Monika: Digitalisation as a determinant of new payment methods' development: The evidence from eurozone and Poland. In: *Proceedings of the European Conference on Innovation and Entrepreneurship (ECIE)*. 2021. DOI: 10.34190/EIE.21.194. Dostupné online (cit. 26.09.2025): <https://doi.org/10.34190/EIE.21.194>; DE', Rahul – PANDEY, Neena – PAL, Abhipsa: Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. In: *International Journal of Information Management*, 55, (2020), 102171. DOI: 10.1016/j.ijinfomgt.2020.102171.

⁴ Napr. NICHOLLS, Jack – KUPPA, Aditya – LE-KHAC, Nhien-An: Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. In: *IEEE Access*, 9, (2021). DOI: 10.1109/ACCESS.2021.3134076.

⁵ SCA je overenie identity používateľa aspoň dvoma prvkami z kategórií poznatok, vlastníctvo a inherencia, ktoré sú navzájom nezávislé, s dynamickým prepojením na sumu a príjemcu platby

preto sformulovať pracovné vymedzenie online platobného podvodu, identifikovať hlavné slabiny existujúceho legislatívneho rámca a posúdiť, do akej miery pripravovaný balík tieto medzery adresuje.

Ambíciou textu nie je rekapitulovať celé spektrum podvodov, ani všetky aspekty boja proti nim ale ponúknuť rámec základný rámec pre pochopenie aktuálnych legislatívnych nedostatkov a medzier a zhodnotiť navrhované legislatívne zmeny z hľadiska ich potenciáli tieto medzery a nedostatky odstrániť. Pri analýze online platobných podvodov akcentujeme súhlas platiteľa⁶, potrebu precíznejšie vymedzenia pojmov, dôkazné štandardy a výsledkovo orientovaný monitoring, ako nosné piliere modernej obrany proti online platobným podvodom.

Pojem online platobný podvod

Je treba uviesť, že neexistuje všeobecne použiteľná legálna definícia online platobného podvodu. Explicitné vymedzenie je však potrebné už v úvode, lebo priamo rámcuje následnú analýzu jednotlivých inštitútov, ktorým sa budeme venovať ďalej v texte.

Podvod, ako taký, je hlavne trestný čin, ktorého skutková podstata je uvedená v § 221 Trestného zákona⁷. Predmetom článku však nie sú všetky typy podvodov, ale podvodné platby na internete. Zároveň trestný zákon predpokladá spôsobenie malej škody (v súčasnosti 700 EUR). Predmetom článku sú však aj podvodné transakcie, kde spôsobená finančná strata je nižšia ako v Trestnom zákone zakotvená hranica malej škody. Pojem podvodu podľa Trestného zákona je teda pre naše účely na jednej strane príliš široký a na druhej strane príliš úzky.

Určité vymedzenie podvodnej platobnej transakcie môžeme nájsť v usmerneniach Európskeho orgánu pre bankovníctvo (ďalej len „EBA“) o oznamovaní podvodov⁸. Tieto usmernenia uvádzajú v bode 1.1., že ako podvody sa majú vykazovať neautorizované platobné operácie a platobné operácie vykonané na základe

⁶ Ide o chápanie, ktoré stavia do centra pozornosť práve súhlas používateľa. Podvod sa nevníma len ako technické obchádzanie systému alebo neoprávnený prevod peňazí. Hlavným kritériom je, či používateľ skutočne súhlasil s transakciou alebo s využitím svojich prostriedkov. Ak bol súhlas získaný podvodne, napr. klamlivými informáciami, manipuláciou alebo sociálnym inžinierstvom – transakcia sa považuje za podvodnú, aj keď technicky prešla všetkými kontrolami.

⁷ § 221 zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov

⁸ EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Usmernenia EBA o podávaní správ o podvodoch podľa PSD2 (konsolidované znenie, verzia 2). Paríž: EBA, september 2024. 47 s. Dostupné na: https://www.eba.europa.eu/sites/default/files/2024-09/73138852-34d6-452d-ad5c-42de2a2foegd/EBA%202018%20Guidelines%20on%20fraud%20reporting%20-%20Consolidated%20version%20v2_SK.pdf

manipulácie platiteľa.⁹ Samotné usmernenia uvádzajú, že ide o definíciu používanú v súvislosti s reportovaním štatistických dát o podvodoch. Táto definícia bude slúžiť ako základ definície online platobného podvodu pre účely tohto článku.

Pre účely analýzy sa budeme zameriavať výlučne na podvody vykonanými formou platobnej operácie. Platobná operácia je definovaná v § 2 ods. 2 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoPS“). Z definície platobnej operácie vyplýva, že základným predpokladom jej riadneho vykonania je priamo pokyn, resp. súhlas (v jeho mene) používateľa platobných služieb. Súhlas, resp. jeho absenciu, s vykonaním platobnej operácie preto považujeme za nevyhnutnú súčasť našej definície online platobného podvodu.

Keďže špecificky sa zameriavame na online platobné podvody, je potrebné zohľadniť aj spôsob vykonania platobnej operácie. Z tohto dôvodu budeme vychádzať z definície platobnej operácie na diaľku zakotvenou v § 2 ods. 4o ZoPS.

Z definície EBA vyššie vyplýva, že jednou z foriem podvodných platobných operácií môže byť aj tzv. manipulačný podvod. Pri takomto podvode síce súhlas s vykonaním platobnej operácie zdánlivo udelí, nejde však o skutočný súhlas, nakoľko používateľ platobných služieb konal v omyle, do ktorého ho uviedol páchatel'.¹⁰ Tento aspekt nesprávneho súhlasu je preto kľúčovým prvkom našej definície online platobného podvodu a preto túto formu podvodov a problematiku súhlasu rozoberáme v nasledujúcich kapitolách tohto článku. Zároveň je však potrebné rozlišovať situácie, kedy dochádza k vykonaniu platobnej operácie bez súhlasu používateľa platobných služieb a nejde pritom o podvod. Môže ísť napríklad o situácie uvedené v § 3 ods. 2 ZoPS (napr. výkon rozhodnutia). Toto je takisto potrebné zohľadniť, aby naša definícia nebola príliš široká.

V zmysle vyššie uvedeného teda na účely tohto článku definujeme online platobný podvod ako platobnú operáciu na diaľku zrealizovanú bez skutočného súhlasu používateľa platobných služieb, pokiaľ neexistovali zákonné dôvody na jej vykonanie bez súhlasu používateľa platobných služieb.

⁹ Na účely oznamovania štatistických údajov o podvodoch v súlade s týmito usmerneniami by poskytovateľ platobných služieb mal pre každé vykazované obdobie oznámiť:

a. vykonané neautorizované platobné transakcie vrátane straty, odcudzenia alebo zneužitia citlivých platobných údajov alebo platobného nástroja, či už zistiteľné platiteľom alebo nie, pred platbou a či boli alebo neboli spôsobené hrubou nedbanlivosťou platiteľa alebo vykonané bez súhlasu platiteľa („neoprávnené platobné transakcie“); a

b. platobné transakcie uskutočnené v dôsledku manipulácie platiteľa podvodníkom s vydaním platobného príkazu alebo poskytnutie pokynu poskytovateľovi platobných služieb v dobrej viere k platobnému účtu, o ktorom sa domnieva, že patrí k oprávnenému príjemcovi platby („manipulácia platiteľa“).

¹⁰ Napr. BRAITHWAITE, Jo: 'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like? In: *Journal of Financial Regulation*, 10, 2, (2024), 174–193. <https://doi.org/10.1093/jfr/fjae006>

Stručná história legislatívneho vývoja

Na úvod tejto časti uvádzame, že legislatívny vývoj sledujem vo väzbe na vymedzený problém a cieľ článku, t. j. ukázať ako sme sa dostali do súčasného legislatívneho stavu a do akej miery súčasný rámec rieši online platobné podvody.

Spolu s prudkým rozvojom digitálnych technológií a internetu na začiatku 21. storočia sa otvoril priestor nielen pre nové legálne obchodné príležitosti, ale aj pre digitálne formy nelegálnych aktivít. Nárast elektronického obchodu (e-commerce) vytvoril potrebu bezpečných a efektívnych digitálnych platieb. Tento dynamický rast však zároveň sprevádzala aj zvýšená zraniteľnosť voči podvodným praktikám, ktoré sa začali prispôsobovať novým technológiám a platobným mechanizmom.¹¹

Z finančnoprávneho hľadiska bol na začiatku 21. storočia rámec EÚ pre retailové platby a boj proti podvodom roztrieštený. Kľúčovým (nezáväzným) dokumentom bola odporúčanie Komisie z 30. júla 1997 o transakciách uskutočňovaných elektronickými platobnými nástrojmi, a najmä o vzťahu medzi vydavateľom a držiteľom (97/489/ES)¹².

Popri tomto odporúčaní existoval aj trestnoprávny pilier – rámcové rozhodnutie Rady z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov (2001/413/JHA)¹³, ktoré zjednotilo základné skutkové podstaty podvodov a falšovania bezhotovostných platobných prostriedkov.

Prelomovou legislatívou z hľadiska úpravy digitálnych platieb bola prvá smernica o platobných službách (PSD1)¹⁴. Táto po prvýkrát komplexne harmonizovala práva a povinnosti pri poskytovaní platobných služieb. Z pohľadu podvodov stanovila mechaniku vrátenia prostriedkov pri neoprávnených transakciách a obmedzila zodpovednosť platiteľa do 150 EUR (ak nešlo o podvod platiteľa alebo hrubú neobstarávanosť). Zároveň kodifikovala mechanizmus refundácie pri SEPA inkasách, čím posilnila dôveru v bezhotovostné platby.

Na rastúcu online kriminalitu zareagovala Európska centrálna banka (ďalej len „ECB“) a EBA v roku 2011 zriadením Európskeho fóra pre bezpečnosť retailových platieb (European Forum on the Security of Retail Payments), tzv. SecuRe Pay. Jeho Odporúčania pre bezpečnosť internetových platieb (2013) a následné usmernenia

¹¹ Napr. TAWDE, Samiksha Dattaprasad – ARORA, Sandhya – THAKUR, Yashasvee Shitalkumar: Online Payment Fraud Detection for Big Data. In: *Lecture Notes in Computer Science (LNCS)*, (2024). DOI: 10.1007/978-3-031-50583-6_22.

¹² 97/489/EC: Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder

¹³ 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment

¹⁴ Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES

EBA o bezpečnosti internetových platieb (2014) premostili obdobie medzi PSD1 a PSD2. Zaviedli princípy silnej autentifikácie, ochrany citlivých údajov a minimálne bezpečnostné požiadavky.¹⁵

Aktuálne platnú právnu úpravu predstavuje druhá smernica o platobných službách (PSD2).¹⁶ Z hľadiska podvodov je zásadným krokom v posilnení ochrany používateľov a bezpečnosti platobných transakcií. Zaviedla povinnosť uplatňovať silnú autentifikáciu klienta (Strong Customer Authentication – SCA) a zároveň splnomocnila Európsku komisiu prijať záväzné regulačné technické štandardy o SCA a bezpečnej komunikácii, ktoré boli následne kodifikované v sekundárnej legislatíve. Okrem toho znížila maximálnu hranicu zodpovednosti platiteľa pri neoprávnených transakciách na 50 eur a poskytovateľom platobných služieb uložila povinnosť systematicky reportovať štatistiky podvodov. Praktický efekt týchto opatrení sa prejavil najmä po plošnom zavedení SCA, keď došlo k výraznému poklesu podvodov pri diaľkových kartových platbách.¹⁷

S rýchlosťou platieb prichádzali nové typy podvodov. Tzv. nariadenie o okamžitých platbách¹⁸ preto zaviedlo službu overenia príjemcu (IBAN-meno). Cieľom je znížiť množstvo chybných a podvodných platieb ešte pred odoslaním prostriedkov. Zavedenie mechanizmov overenia príjemcu pri okamžitých platbách síce pomáha predchádzať chybným a podvodným transakciám, no z hľadiska komplexnej prevencie podvodov je rovnako nevyhnutné venovať pozornosť širšej oblasti kybernetickej bezpečnosti. V tejto oblasti boli v nedávnej minulosti prijaté viaceré zásadné predpisy. Smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2)¹⁹ zavádza horizontálne požiadavky kybernetickej bezpečnosti a oznamovania incidentov. Nariadenie o digitálnej

¹⁵ EURÓPSKA CENTRÁLNA BANKA: Odporúčania pre bezpečnosť internetových platieb – výsledky verejnej konzultácie. Frankfurt nad Mohanom: ECB, január 2013. 16 s. Dostupné na: <https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf>

¹⁶ Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES

¹⁷ Podľa údajov ECB za rok 2021 klesol objem card-not-present podvodov približne o 12 % oproti roku 2020, pričom aj naďalej tvorili rozhodujúcu časť (okolo 84 %) hodnoty všetkých kartových podvodov. Tento pokles je priamo pripisovaný implementácii SCA

¹⁸ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/886 z 13. marca 2024, ktorým sa menia nariadenia (EÚ) č. 260/2012 a (EÚ) 2021/1230 a smernice 98/26/ES a (EÚ) 2015/2366, pokiaľ ide o okamžité úhrady v eurách

¹⁹ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

prevádzkovej odolnosti finančného sektora (DORA)²⁰ prináša jednotné pravidlá pre informačné a komunikačné technológie (ICT) vo finančných subjektoch, vrátane testovania, správy rizík a reportovania veľkých incidentov. Spoločne tak vytvárajú základnú ochrannú vrstvu, ktorá nepriamo znižuje aj podvodné riziká.

V trestnoprávnej rovine smernica o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu²¹ nahradila rámcové rozhodnutie z roku 2001 a harmonizovala trestnoprávne definície podvodov a falšovania bezhotovostných platobných prostriedkov. Cielmi nielen na zneužitie platobných nástrojov a prostredníkov, ale aj na krádež poverení (napr. phishing), obchodovanie s nástrojmi na páchanie týchto trestných činov a cezhraničnú spoluprácu a podporu obetiam.

Identifikovaný trend vývoja

Legislatívny a regulačný vývoj popísaný v predchádzajúcej kapitole má určitý trend. V EÚ je zreteľný posun od technicky orientovaných podvodov (skimming²², malware²³, „card-not-present“²⁴) k schémam založeným na sociálnom inžinierstve, ktoré cieľia priamo na používateľa a obchádzajú technické bariéry. Zavedenie silnej autentifikácie klienta (SCA) citeľne znížilo priestor pre tradičné technologické útoky.²⁵

²⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011

²¹ Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV

²² Ide o kopírovanie údajov z platobnej karty pri platbe alebo výbere z bankomatu. Podvodníci použijú zariadenie („skimmer“), ktoré sa pripevní na bankomat alebo platobný terminál a skopíruje údaje z magnetického pásika. Následne vyrobí falošnú kartu a pokúsia sa ňou zaplatiť alebo vybrať peniaze.

²³ Škodlivý softvér, ktorý sa dostane do počítača, mobilu alebo priamo do bankomatu/platobného terminálu. Cieľom je získať prihlasovacie údaje, heslá, alebo manipulovať s transakciami.

²⁴ Nastáva vtedy, keď sa platí kartou bez jej fyzickej prítomnosti – typicky online nákup, telefonická objednávka alebo mailová platba. Podvodník získa údaje z karty (číslo karty, dátum expirácie, CVV kód) a použije ich na internetové transakcie.

²⁵ EURÓPSKA CENTRÁLNA BANKA: ECB publikovala štatistiky kartových podvodov. Tlačová správa, 26. máj 2023. Dostupné na: <https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230526~f09bc3c664.en.html>

Podvodníci sa adaptovali presunom k manipulatívnym taktikám (phishing²⁶, vishing/smishing²⁷, spoofing čísla²⁸, „CEO fraud“²⁹, investičné a „romantické“ podvody³⁰), ktoré vedú najmä k tzv. autorizovaným platbám. Podľa European Payment Council ide o rastúci trend, kde „terčom je používateľ, nie technológia“³¹. Rovnaký posun potvrdzuje aj Europol vo svojom hodnotení hrozieb organizovanej kriminality na internete.³²

Bojovať s takouto formou podvodov, založenej na sociálnom inžinierstve a manipulácii, je náročné najmä preto, že útočník neobchádza technológiu, ale presvedčí samotného používateľa, aby urobil požadovaný úkon, napr. potvrdil platbu, zadal kód SCA, či zmenil limity. Transakcia tak z pohľadu poskytovateľa platobných služieb vyzerá technicky bezchybne (správne zariadenie, IP, geolokácia, SCA splnená), takže ju detekčné systémy zväčša vyhodnotia ako legítimnú. Časový tlak a emócie znižujú obozretnosť obete.³³ Páchatelia sa tiež často zameriavajú na zraniteľné skupiny obyvateľov, napr. na starších ľudí, alebo ľudí z nižšou finančnou gramotnosťou.

Hlavné nedostatky aktuálnej právnej úpravy

V tejto časti uvádzame tri systémové slabiny súčasného legislatívneho rámca platobných služieb, ktoré priamo ovplyvňujú ochranu používateľa aj prax

²⁶ Podvodné e-maily alebo webové stránky, ktoré sa tvária ako banka, pošta, štátna inštitúcia či známa firma. Ich cieľom je vylákať prihlasovacie údaje, čísla kariet, heslá alebo presvedčiť obeť, aby stiahla škodlivý súbor.

²⁷ Podvod cez telefón, keď sa útočník vydáva za banku, políciu, IT oddelenie atď. a snaží sa vylákať citlivé údaje alebo prístup.

²⁸ Technika, pri ktorej útočník falšuje telefónne číslo alebo e-mailovú adresu, takže to vyzerá, že volá banka, polícia či dokonca kolega. Používa sa často v kombinácii s vishingom.

²⁹ Forma impersonačného podvodu (Business Email Compromise), pri ktorej sa páchateľ vydáva za vrcholového manažéra alebo vlastníka firmy a naliehavou „internou“ žiadosťou prinúti zamestnanca autorizovať prevod peňazí alebo poskytnúť citlivé údaje

³⁰ Útočník sa zoznami cez sociálne siete alebo zoznamku a buduje dôveru. Po čase začne žiadať peniaze – napr. na „letenku“, „liečbu“, „dlh“ alebo „investíciu“. Emócie a dôvera sú tu kľúčovou zbraňou.

³¹ EUROPEAN PAYMENTS COUNCIL: Payments Threats and Fraud Trends Report 2024. Brusel: EPC, december 2024. 56 s. Dostupné na: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_o.pdf

³² EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2023. Haag: Europol, 2023. 52 s. Dostupné na: <https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf>

³³ LYU, Ce – GAO, Shenghan – ZHANG, Qingqi: The impact of time pressure and type of fraud on susceptibility to online fraud. In: *Frontiers in Psychology*, 16, (2025), 1508363. DOI: 10.3389/fpsyg.2025.1508363.

poskytovateľov. Prvou je rozdelenie zodpovednosti pri neautorizovaných operáciách a nejednoznačný prah hrubej nedbanlivosti, ktorý vnáša výraznú aplikačnú variabilitu. Druhou je neistota pri kvalifikácii „autorizácie“ v situáciách vylákaného súhlasu, čo spôsobuje nerovnomerné rozloženie strát a spory o dôkazné bremená. Treťou je nedostatočná a neharmonizovaná úprava monitorovania transakcií, ktorá neudržateľne spolieha na ex post detekciu. Spoločne tieto tri línie vysvetľujú, prečo je potrebné precizovať pojmy, zjednotiť dôkazné štandardy a posilniť výsledkovo orientované, ideálne priebežné monitorovanie, aby sa znížila regulačná neistota a zvýšila účinnosť prevencie aj kompenzácie podvodov.

a) zodpovednosť za neautorizované platobné operácie v PSD2 a hrubá nedbanlivosť

Ustanovenia § 10 ods. 1 a ods. 2 ZoPS pri neautorizovaných platobných operáciách výslovne kladú dôkazné bremeno na poskytovateľa. Nestačí preukázať, že bol použitý platobný nástroj alebo že prebehla silná autentifikácia, musí byť schopný dokázať riadnu autentifikáciu, zaznamenanie, správne zaúčtovanie a absenciu technickej poruchy. Samotné použitie nástroja neznamená automatický a bezvýhradne súhlas platiteľa.

Otázka výkladu pojmu hrubej nedbanlivosti však zostáva otvoreným a národným právom determinovaným problémom, čo vyvoláva rozdiely v praxi. V niektorých jurisdikciách sa hrubá nedbanlivosť vykladá veľmi reštriktívne, zatiaľ čo v iných právnych poriadkoch je hranica posudzovania správania spotrebiteľa nastavená nižšie, čo poskytovateľom umožňuje častejšie preniesť dôsledky neautorizovaných operácií na klienta. Tento rozdiel v aplikačnej praxi podčiarkuje absenciu harmonizovanej európskej definície a otvára priestor pre asymetrické postavenie účastníkov vnútorného trhu.

b) nejednoznačnosť a nejednotná aplikácia pojmu neautorizovaná transakcia

Legislatíva vychádza z jednoduchej, no dôležitej zásady: platba je autorizovaná len vtedy, ak na ňu platiteľ skutočne udelil súhlas. Samotný fakt, že boli použité jeho prístupové údaje ešte neznamená, že súhlas existoval. V praxi sa preto prípad posudzuje cez otázku: vytvoril a potvrdil platobný príkaz sám platiteľ? Ak nie, ide typicky o neautorizovanú operáciu – napríklad keď páchatel získal prihlasovacie údaje cez phishing, malvér alebo SIM-swap a bez vedomia klienta zadal prevod. Ak však platiteľ príkaz sám zadal a potvrdil, hoci po predchádzajúcej manipulácii (telefonát „z banky“, falošný e-mail či chat, „investičný poradca“ a pod.), z pohľadu ZoPS a PSD2 ide formálne o autorizovanú transakciu, pretože súhlas bol daný. Problém je však to, že tento súhlas bol vylákaný a platiteľ konal v omyle. Práve rozlíšenie medzi „hackom“ (keď príkaz vyvolá útočník bez účasti platiteľa) a „vylákaným súhlasom“ (keď príkaz vyvolá sám platiteľ po manipulácii) spôsobuje v sporoch medzi poskytovateľmi platobných služieb a klientmi najviac nejasností. Pri prvom type

podvodu býva kvalifikácia ako neautorizovaná zrejماً; pri druhom type sa rieši, do akej miery možno na manipuláciu prihladiť pri zodpovednosti a kompenzácií, keďže samotné splnenie technických krokov (napr. zadanie kódu alebo biometrie) ešte nepreukazuje, že platiteľ slobodne a informovane chcel prevod uskutočniť. Tento rámec zároveň kladie vysoké nároky na dokazovanie, t. j. čo presne sa stalo, kto zadal príkaz, aké dôkazy o riadnej autentifikácii existujú a vysvetľuje, prečo sú rozhodnutia v praxi neraz nejednotné. Dokazovanie je komplexné, závislé od kvality interných systémov poskytovateľa a v neposlednom rade aj od národného výkladu pojmu hrubá neobstarlivosť. Výsledkom je stav, v ktorom sa ochrana spotrebiteľa síce deklaratórne posilňuje, avšak aplikačná neistota môže generovať rozdielne závery naprieč jurisdikciami.

Dôsledkom je aj nerovnomerné rozloženie zodpovednosti za straty vzniknuté podvodnými platobnými operáciami medzi používateľmi platobných služieb a poskytovateľmi platobných služieb, ktoré sa v rámci EHP výrazne líši. V značnom počte krajín znášali používatelia platobných služieb viac než polovicu nahlásených strát z podvodov pri kartových platbách, miestami až 80 % alebo viac. Naproti tomu v iných krajinách zostal podiel znášaný používateľmi platobných služieb pod 30 % alebo ešte nižší, pričom väčšinu zvyšku niesli poskytovatelia platobných služieb a/alebo sa kryl inými mechanizmami, napríklad poistnými zmluvami. Podobné, hoci menej výrazné rozdiely sa pozorovali pri úhradách, kde vo veľkej väčšine krajín museli používatelia platobných služieb niesť väčšinu alebo všetky straty, zatiaľ čo v štyroch krajinách niesli poskytovatelia platobných služieb medzi 35 % a 71 % strát.³⁴ Z uvedeného vyplýva, že rozdelenie zodpovednosti za straty z podvodov medzi používateľmi a poskytovateľmi platobných služieb v rámci EHP nie je jednotné a silne závisí od národnej aplikačnej praxe.

c) nedostatočná úprava mechanizmov monitorovania transakcií

Ako jeden z hlavných nástrojov v boji s podvodmi využívajú poskytovatelia platobných služieb rôzne mechanizmy monitorovania transakcií. Mechanizmus monitorovania transakcií by sme mohli definovať ako súbor procesov, pravidiel a technických nástrojov, ktorý priebežne vyhodnocuje transakcie klientov, ideálne v reálnom čase, porovnáva ich s profilom klienta, historickými vzorcami správania a známymi indikátormi podvodov a na základe rizikového skóre rozhoduje o povolení, odmietnutí alebo dodatočnej autentifikácii transakcie.

PSD2 mechanizmy monitorovania transakcií vyslovene neupravuje. Čiastkovú úpravu nájdeme v delegovanom nariadení, ktorým sa dopĺňa smernica Európskeho

³⁴ EURÓPSKY ORGÁN PRE BANKOVNICTVO – EURÓPSKA CENTRÁLNA BANKA: Report on Payment Fraud 2024. Paríž/Frankfurt nad Mohanom: EBA/ECB, august 2024. 44 s. Dostupné na: https://www.eba.europa.eu/sites/default/files/2024-08/465e3044-4773-4e9d-8ca8-b1cd031295fc/EBA_ECB%202024%20Report%20on%20Payment%20Fraud.pdf

parlamentu a Rady (EÚ) 2015/2366, pokiaľ ide o regulačné technické predpisy pre silnú autentifikáciu zákazníka a spoločné a bezpečné otvorené komunikačné normy (ďalej len „RTS SCA“).

RTS SCA v článku 2 ods. 1 a ods. 2 obsahuje základnú úpravu transakčného monitoringu, ktorá platí pre všetkých poskytovateľov platobných služieb, avšak z hľadiska sledovaných faktorov je len čiastková a transakčný monitoring nemusí byť realizovaný v reálnom čase. Uvedené vyplýva z EBA Q&A 2018_4090, podľa ktorej *„všeobecný mechanizmus monitorovania podľa článku 2 týchto RTS nevyžaduje zapnutie „monitorovania rizík v reálnom čase“ a spravidla sa vykonáva „po“ vykonaní platobnej transakcie“*.³⁵ Takýto ex-post monitoring je z hľadiska prevencie podvodov nedostatočný, pretože umožňuje, aby podvodné transakcie prebehli a boli zaznamenané až po ich uskutočnení, čo znižuje možnosť okamžitého zásahu alebo zamedzenia finančnej škody. Tento režim nie je dostačujúci pre aktívnu detekciu a blokovanie podvodov v reálnom čase, čím sa zvyšuje riziko strát pre poskytovateľa aj pre používateľa platobných služieb. RTS SCA obsahuje v článku 18 aj ďalšie požiadavky na mechanizmus monitorovania transakcií, tieto sa však vzťahujú iba na poskytovateľov platobných služieb, ktorí sa rozhodli využívať výnimku zo silnej autentifikácie zákazníka podľa článku 18 RTS SCA (tzv. analýza rizík transakcií).

Aktuálny stav je teda taký, že hoci RTS SCA formálne vyžaduje, aby všetci poskytovatelia mali zavedený mechanizmus monitorovania transakcií, ide len o rámcové minimum, ktoré nereflektuje charakter dnešných podvodov. Právne predpisy neukladajú povinnosť on-line/real-time monitoringu pre všetkých poskytovateľov platobných služieb a EBA výslovne pripúšťa, že všeobecný monitoring môže prebiehať až ex post – čo je pri sociálnom inžinierstve neskoro. Pokročilejšie požiadavky sú podrobnejšie upravené iba pre tých, ktorí využívajú výnimku analýza rizík transakcií, čím vzniká nerovnosť v štandardoch ochrany. Zároveň chýbajú povinné rizikové signály, merateľné ukazovatele (napr. miera zachytenia a false positives) aj pravidlá pre zdieľanie dát medzi poskytovateľmi platobných služieb.

Dôsledkom je nejednotná prax, medzery v prevencii a oslabená pozícia obete pri autorizovaných podvodoch.

Vzhľadom na vyššie uvedené skutočnosti, aktuálnu právnu úpravu mechanizmov monitorovania transakcií považujeme za nedostatočnú a podľa nášho názoru vyžaduje posun k povinnému, priebežnému (real-time) a výsledkovo orientovanému monitoringu pre všetkých poskytovateľov, s harmonizovanými štandardmi, povinnými varovaniami a prepojením na režim kompenzácie.

³⁵ EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Single Rulebook Q&A, otázka č. 2018_4090. Dostupné na: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4090

Hlavné zmeny, ktoré má priniesť pripravovaný právny rámec

Aktuálne prebiehajú na európskej úrovni práce na legislatívnom balíku, ktorý bude modifikovať právnu úpravu platobných služieb, vrátane problematiky platobných podvodov. Súčasťou balíka je tretia smernica o platobných službách (ďalej len „PSD3“)³⁶ a nariadenie o platobných službách (ďalej len „PSR“).³⁷ Aktuálne (september 2025) prebiehajú trialógy. Práva a povinnosti pri poskytovaní platobných služieb, vrátane prevencie podvodov, budú upravené v PSR preto sa v ďalšom výklade budeme venovať výlučne tomuto predpisu.

V rámci problematiky podvodov svoje odporúčania na riešenie svojej situácie publikovala EBA v stanovisku k novým typom platobných podvodov a možným zmierňujúcim opatreniam.³⁸ Analýza týchto odporúčaní umožňuje hodnotiť, do akej miery návrh PSR reflektuje odporúčania EBA a či zavádza efektívne mechanizmy prevencie a zmiernenia rizík.

Pripravovanú legislatívu v kľúčových oblastiach hodnotíme nasledovne:

a) (ne)autorizované platobné operácie a hrubá nedbanlivosť

EBA odporučila, aby sa v PSR spresnili pravidlá zodpovednosti pri podvodoch. Predovšetkým žiada jasnejšie vymedzenie hranice medzi autorizovanými a neautorizovanými transakciami. Samotné použitie silnej autentifikácie podľa nej nemôže postačovať ako dôkaz, že platiteľ transakciu skutočne autorizoval, alebo že konal podvodne. Rovnako nemožno považovať za autorizovanú takú platbu, ktorú síce formálne potvrdil platiteľ, ale v skutočnosti ju zadal podvodník, ani platbu, pri ktorej platiteľ nebol upozornený na nesúlad mena a IBAN.

Návrh PSR obsahuje úpravu uvedeného len čiastočne. Návrh PSR nepreklasifikuje podvody pri platbách iniciovaných platiteľom tak, že by sa transakcia považovala za neautorizovanú vtedy, keď platobný príkaz zadal podvodník a platiteľ ho následne autentifikoval. Namiesto toho návrh PSR zachováva všeobecný rámec autorizácie, ale sprísňuje dôkazné bremeno tým, že uvádza, že samotné použitie platobného nástroja (alebo SCA) nie je dostatočným dôkazom autorizácie a (ii) vytvára

³⁶ EURÓPSKA KOMISIA: Návrh nariadenia Európskeho parlamentu a Rady o platobných službách na vnútornom trhu a o zmene nariadenia (EÚ) č. 1093/2010 a o zrušení smernice (EÚ) 2015/2366 (COM(2023)366 final). Brusel: Európska komisia, 28. jún 2023. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52023PC0366>

³⁷ EURÓPSKA KOMISIA: Návrh nariadenia Európskeho parlamentu a Rady o platobných službách na vnútornom trhu a o zrušení smernice (EÚ) 2015/2366 (COM(2023)367 final). Brusel: Európska komisia, 28. jún 2023. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52023PC0367>

³⁸ EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Stanovisko k novým typom platobných podvodov a možným zmierňujúcim opatreniam. Paríž: EBA, apríl 2024. 41 s. Dostupné na: <https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20of%20fraud%20and%20possible%20mitigations.pdf>

samostatný, podmienený režim náhrady (refundácie) pri impersonačných podvodoch (najmä keď sa podvodník vydáva za poskytovateľa platobných služieb používateľa).

Čo sa týka úpravy dôkazného bremena v súvislosti s neautorizovanými platobnými operáciami, zostáva teda zachovaný režim v PSD2. Článok 55 PSR tento rámec potvrdzuje, avšak sprísňuje dôkazný prah: namiesto formulácie „...použitie platobného nástroja, ktoré zaznamenal poskytovateľ platobných služieb, ..., ako také nie je nevyhnutne dostatočným dôkazom...“, sa výslovne stanovuje, že „nepostačuje“ spoliehať sa len na záznam o použití platobného nástroja. Zároveň sa tento režim unifikuje v celej Európskej únii prostredníctvom priamej aplikovateľnosti nariadenia. Toto by malo v praxi znamenať detailnejšie a presnejšie dôkazné záznamy v reálnom čase, vrátane logov, časových pečiatok a zachytenia jednotlivých procesných krokov a potrebu substantívnych podkladov, ak sa odvolávajú na podvodné konanie alebo hrubú nedbanlivosť zo strany klienta.

EBA ďalej navrhuje bližšie vysvetliť pojem hrubá nedbanlivosť. Pri posudzovaní správania používateľa by sa malo prihliadať na zložitost' podvodu, jeho osobné okolnosti, rozumné dôvody veriť v legitimitu príjemcu a tiež na to, či poskytovateľ mohol podniknúť ďalšie preventívne kroky. Do odôvodnenia PSR by sa mala doplniť otvorená množina kritérií, ako je napríklad vedomé sprístupnenie bezpečnostných prvkov podvodníkom, opakované naletenie rovnakému typu podvodu, ignorovanie varovaní poskytovateľa či oneskorené nahlásenie podvodu.

PSR v rámci recitálov obsahuje výklad a výslovné zakotvenie príkladov hrubej nedbanlivosti. PSD2 ponechávalo pojem v celom rozsahu na vnútroštátny výklad. Návrh PSR (recitál 82) uvádza, že hrubá nedbanlivosť je viac než „bežná“ nedbanlivosť (výrazná ľahostajnosť) a dáva dva konkrétne príklady: (i) uchovávanie prihlasovacích/potvrdzovacích prvkov pri platobnom nástroji v podobe ľahko odhaliteľnej treťou osobou; (ii) opakované padnutie za obeť tomu istému typu „spoofing“ podvodu po predchádzajúcom refundovaní.

PSR, teda vo vzťahu k pojmu hrubá nedbanlivosť poskytuje lepši výklad ako tomu bolo v PSD2R. Stále však platí, že otázka posúdenia hrubej nedbanlivosti ponecháva plne v pôsobnosti členských štátov a uvádza, že dôkazy a stupeň údajnej nedbanlivosti by sa mali posudzovať podľa vnútroštátnej právnej úpravy. Problematické však je, že významná časť vnútroštátnych právnych poriadkov členských štátov, vrátane Slovenskej republiky, neposkytuje bližšie kritériá k posúdeniu, v akých situáciách možno určité konanie považovať za hrubo nedbanlivé a v akých len za nedbanlivé.³⁹ Výsledkom môže byť pretrvávajúca právna neistota a

³⁹ KARPJAKOVÁ, Veronika: Právní rámec boje proti podvodům v bezhotovostních platbách v EU. In: Právník, Roč. 164, č. 3 (2025), s. 227 – 242. Dostupné na: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2025/3/3_Karpjakova_227-242_3_2025.pdf

nerovnaké postavenie spotrebiteľov naprieč EÚ. Do budúcnosti sa preto ako kľúčové javí buď podrobnejšie rozpracovanie tohto pojmu na úrovni sekundárnej legislatívy EÚ, alebo vytvorenie harmonizovaných interpretačných rámcov prostredníctvom soft law nástrojov (napr. usmernení EBA).

b) impersonačný podvod

Ako bolo uvedené v predchádzajúcom texte, PSR by malo zachovať režim autorizovaných a neautorizovaných transakcií (s prísnejším dôkazným bremenom). V záujme ochrany spotrebiteľa sa však v PSR navrhuje osobitný režim pri tzv. impersonačných podvodoch (podvodoch predstieraním identity).⁴⁰ Ide o špecifický prípad, kedy sa presúva zodpovednosť za škodu spôsobenú autorizovanou podvodnou transakciou z používateľa platobných služieb na poskytovateľa platobných služieb.

Takéto ustanovenie je z právneho hľadiska pomerne neštandardné, nakoľko dochádza k presunu zodpovednosti za škodu spôsobenú protiprávnym činom na tretí subjekt (poskytovateľa platobných služieb). Práve z tohto dôvodu sa objavujú argumenty, prečo by takéto ustanovenie nemalo byť prijaté. Ide napríklad o obavy z právnej neistoty. Samotné vymedzenie „zmanipulovania“ a „nezákonného použitia“ mena, e-mailu alebo čísla banky je otvorené výkladu a ťažko sa preukazuje, najmä pri bežnom spoofingu hovorov/SMS.⁴¹ Analýzy upozorňujú, že text nejasne nadväzuje aj na sekundárnu zodpovednosť iných poskytovateľov (napr. online platforiem)⁴² bez jasnej kauzálnej väzby medzi konkrétnym obsahom a vznikom škody, bez procesných lehôt a s veľkou diskrepciou bánk pri požiadavkách na odstránenie obsahu či náhradu, čo je recept na spory a nerovnakú prax.⁴³

Taktiež sa poukazuje na otázne ekonomické dopady, napr. že účinnosť zdieľanej zodpovednosti pri znižovaní podvodov nie je doložená a regulačný zásah môže

⁴⁰ Článok 59 PSR ustanovuje, že „ak používateľ platobných služieb, ktorý je spotrebiteľom, zmanipulovala tretia strana predstierajúca, že je zamestnancom poskytovateľa platobných služieb tohto spotrebiteľa, pričom nezákonne použila meno alebo e-mailovú adresu, alebo telefónne číslo tohto poskytovateľa platobných služieb a toto zmanipulovanie viedlo k následným podvodným autorizovaným platobným transakciám, poskytovateľ platobných služieb vráti spotrebiteľovi celú sumu podvodnej autorizovanej platobnej transakcie pod podmienkou, že spotrebiteľ podvod bezodkladne ohlásil polícii a oznámil ho svojmu poskytovateľovi platobných služieb“

⁴¹ VAN PRAAG, Emanuel: Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation. In: European Banking Institute Working Paper Series, No. 190, (máj 2025), 28 s. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241100

⁴² KELLER, Daphne – LEERSNYDER, Romain: Platform Liability for Platform Manipulation. In: Columbia Law Review, Vol. 124, No. 5 (2024), s. 1359 – 1442. Dostupné na: <https://columbialawreview.org/content/platform-liability-for-platform-manipulation>

⁴³ MARKER, Felix – SEIRA, Enrique – WILSON, Tom: Social Engineering Attacks in Financial Services: Evidence from a Large Field Experiment. In: Proceedings of the 25th ACM Conference on Economics and Computation, (2024), s. 1130 – 1131. DOI: 10.1145/3625546. Dostupné na: <https://dl.acm.org/doi/10.1145/3625546>

vyvolať nežiaduce efekty ako morálny hazard (nižšia opatrnosť časti klientov), zvýšené bariéry vstupu a náklady pre menších hráčov, menej užívateľskej prívetivosti v platbách (spomaľovanie, blokácie), prípadne vylučovanie zraniteľných skupín.⁴⁴

Prikláňame sa k názoru kritikov. Považujeme toto ustanovenie za nesystémové. Narúša doterajšiu architektúru zodpovednosti, ktorú poznáme z PSD2. Kým tam sa pri autorizovaných platbách uvažovalo o náhrade škody najmä vtedy, ak poskytovateľ platobných služieb porušil svoje povinnosti (napr. SCA či transakčný monitoring), navrhovaný režim smeruje k refundácii aj pri autorizovaných prevodoch, ak bol spotrebiteľ zmanipulovaný páchatelom vydávajúcim sa za poskytovateľa platobných služieb. Takto nastavený presun zodpovednosti podľa nášho názoru oslabuje logické prepojenie medzi pochybením jednotlivých aktérov a následkami a vytvára riziko morálneho hazardu. Spotrebiteľ môže mať dojem, že refundácia je „garantovaná“, a môže tak klesať jeho obozretnosť.

Zároveň nepovažujeme za vhodné presúvať zodpovednosť za delikt páchatela na finančnú inštitúciu len preto, že páchatel zneužil jej identitu. Samotné pojmy „zmanipulovanie“ a „nezákonné použitie“ mena, e-mailu alebo telefónneho čísla banky sú otvorené výkladu a v praxi ťažko dokázateľné. Pri typickom spoofingu je mimoriadne náročné preukázať kauzálnu väzbu medzi konkrétnym obsahom alebo technickým úkonom páchatela a následným rozhodnutím spotrebiteľa autorizovať platbu. Neurčitosť definícií povedie k sporom, rozdielnej praxi a nepredvídateľnosti rozhodnutí.

Takisto je podľa nášho názoru na mieste otázka, prečo je v rámci tohto inštitútu vybraný ako zodpovednostný subjekt výlučne poskytovateľ platobných služieb (v prípade, že sa páchatel vydáva za jeho zamestnanca). Ak by sme tento inštitút rozvinuli ad absurdum, bolo by spravodlivé aby v prípade, že sa páchatel bude vydávať za štátneho zamestnanca, bol za spôsobený podvod zodpovedný štát? Zrejme nie.

Z týchto dôvodov sa prikláňame ku kritickému postoju k článku 59 PSR. V aktuálnej podobe považujeme riešenie za nesystémové, právne nejasné a s rizikom zníženia obozretnosti spotrebiteľov. Článok 59 PSR síce reaguje na aktuálny nárast spoofingových útokov, avšak v snahe zvýšiť ochranu spotrebiteľa vytvára významné právne i praktické otázky. Presúvanie zodpovednosti na banky bez jasne vymedzených kritérií nielenže deformuje princíp spravodlivej alokácie rizika, ale zároveň môže oslabiť motiváciu spotrebiteľa postupovať obozretné. Namiesto zavádzania nejasných definícií a problematických mechanizmov by bolo

⁴⁴ COPENHAGEN ECONOMICS: Study on Shared Liability Regime. Kodaň: Copenhagen Economics, december 2024. 72 s. Dostupné na: https://copenhageneconomics.com/wp-content/uploads/2024/12/Copenhagen-Economics_Study-on-shared-liability-regime_20241203_clean-final.pdf

systémovejšie posilniť preventívne opatrenia, harmonizovať kľúčové pojmy a dôkazné bremená a podporiť efektívnu spoluprácu medzi poskytovateľmi, spotrebiteľmi a orgánmi dohľadu.

c) transakčný monitoring

V oblasti monitorovania transakcií má, podľa EBA, monitorovanie prebiehať pred vykonaním platby (pri okamžitých platbách v reálnom čase). Zároveň sa má uplatňovať na všetky kanály, v ktorých sa daný platobný nástroj používa (vrátane bankomatov a platobných terminálov). Monitoring na strane platiteľa má dopĺňať skrining na strane prijímateľa, zameraný na identifikáciu podozrivých vzorcov podľa výšky, pôvodu a frekvencie transakcií vzhľadom na profil účtu, ako aj na odchýlky v mene príjemcu oproti údajom vedeným prijímajúcim PSP. Ak monitorovanie vyhodnotí platbu ako vysoko rizikovú, poskytovateľ platobných služieb ju môže odmietnuť a musí o tom riadne informovať používateľa s uvedením dôvodu a možnosti opätovného zadania. PSP má tiež vykonať šetrenie v spolupráci s protistranou a prípadne transakciu zablokovať, pričom detailné pravidlá by mala upraviť sekundárna legislatíva.

Návrh PSR zavádza ucelený rámec mechanizmov monitorovania transakcií a výmeny údajov o podvodoch. Poskytovatelia platobných služieb musia prevádzkovať monitoring, ktorý podporuje uplatňovanie SCA. Návrh zohľadňuje výnimky z SCA a zároveň umožňuje predchádzať a odhaľovať potenciálne podvodné transakcie vrátane operácií iniciovaných poskytovateľmi platobných iniciačných služieb. Tieto mechanizmy stoja na analýze predchádzajúcich transakcií a online prístupu k účtom, pričom spracúvanie sa obmedzuje na údaje nevyhnutné na uvedené účely: informácie o používateľovi (vrátane prostredia a typického správania pri bežnom používaní bezpečnostných prvkov), údaje o účte a jeho histórii, údaje o samotnej transakcii (vrátane sumy a jedinečného identifikátora príjemcu) a údaje o relácii (napr. rozsah IP adres zariadenia). Uchovávanie týchto údajov je striktne viazané na potrebný čas a nikdy nepokračuje po ukončení vzťahu so zákazníkom. Monitoring musí pritom minimálne zohľadňovať kľúčové rizikové faktory, t. j. zoznamy zneužitých alebo odcudzených autentifikačných prvkov, výšku jednotlivých transakcií, známe podvodné scenáre v platbách, príznaky napadnutia škodlivým softvérom počas krokov autentifikácie a ak PSP poskytuje prístupové zariadenie či softvér, záznamy o ich používaní a odchýlky od obvyklého správania.

Na účely prevencie a detekcie podvodov môžu poskytovatelia v nevyhnutnom rozsahu vymieňať jedinečný identifikátor príjemcu s inými PSP v rámci dohodnutých schém výmeny informácií. Takáto výmena je podložená „dostatočnými dôkazmi“, ktoré sa považujú za splnené napríklad vtedy, ak aspoň dvaja rôzni klienti toho istého poskytovateľa nahlásia, že identifikátor príjemcu bol použitý pri podvodnej úhrade. Podľa nášho názoru ide oproti PSD2 o výrazné zlepšenie. Nový rámec presúva monitoring „dopredu“, k predautorizácii a pri okamžitých platbách do reálneho času

a zavádza obojstranné preverovanie (na strane platiteľa aj príjemcu), čo v praxi vytvára integrovanejší a rýchlejší systém zachytávania anomálií naprieč kanálmi. Za veľmi vhodný možno považovať aj jasný minimálny súbor rizikových faktorov a rozšírenie zdieľania podvodových údajov (vrátane modus operandi) vrátane úpravy vzťahu s ochranou osobných údajov. Schopnosť transakciu odmietnuť alebo pozastaviť s okamžitou informáciou používateľovi, spolu so synergiou s overovaním príjemcu podľa nás výrazne zvyšuje preventívnu účinnosť režimu a smeruje k jednotnejšej praxi v celej EÚ, čo bol slabý bod PSD2.

Za nedostatok v tejto oblasti považujeme opomenutie odporúčania EBA výslovne upraviť možnosť nastavenia „odkladu“ zvýšenia dohodnutých limitov (napr. výdavkových, úverových, maximálnej výšky platieb s daným platobným nástrojom a pod.)⁴⁵, aby toto zvýšenie nadobúdalo účinnosť s primeraným oneskorením. Takáto možnosť bude teoreticky možná na zmluvnom základe, avšak úprava priamo v právnom predpise by bola z nášho pohľadu vhodnejšia.

Zhrnutím možno konštatovať, že návrh PSR v oblasti monitoringu a prevencie podvodov predstavuje kvalitatívny posun oproti PSD2, keďže prináša dynamickejší, prediktívny a v reálnom čase fungujúci rámec s vyššou úrovňou ochrany spotrebiteľa aj poskytovateľov služieb. Vytvára predpoklady na efektívnejšie zdieľanie informácií a koordinovanejšie konanie v rámci EÚ, čo posilňuje odolnosť celého platobného ekosystému. Na druhej strane, určitá nedotiahnutosť v otázke explicitnej regulácie niektorých preventívnych opatrení, ako je absencia úpravy niektorých inštitútov (napr. časovo oneskorené zvyšovanie limitov), naznačuje, že výsledný rámec ešte ponecháva priestor na doplnenie a vylepšenie, aby sa naplno využil jeho potenciál pri znižovaní rizika podvodov.

Záver

V jadre problému stojí človek. Online platobné podvody dnes čoraz častejšie neobchádzajú technológiu, ale vôľu používateľa. Z toho vyplývajú tri kľúčové závery. Po prvé, regulácia aj prax musia pracovať s chápaním online platobného podvodu zohľadňujúcim manipuláciu a vychádzajúcim z rozlišovania skutočného a vylákaného súhlasu používateľa platobných služieb s vykonaním platobnej operácie, ktoré nenecháva podvody založené na autorizovaných platobných operáciách bez účinnej odpovede. Po druhé, prevencia musí byť včasná a obojstranná. Real-time monitoring pred vykonaním platby prepojený na skríning na strane príjemcu, štandardizované zdieľanie dát a jasné pravidlá na rýchle zastavenie či odmietnutie rizikových

⁴⁵ Teda napr. ak si chce klient zvýšiť nejaký limit, napr. úverový rámec, zmena nadobudne účinnosť až s oneskorením, napr. jeden deň. Má sa tým zabrániť tomu, aby tieto limity navýšil podvodník za účelom maximalizácie svojho zisku.

transakcií. Po tretie, zodpovednostný rámec má zostať predvídateľný s väzbou medzi konkrétnym pochybením a následkami, s harmonizovaným výkladom.

PSR v tomto smerovaní predstavuje krok vpred. Posilňuje monitoring, rozširuje spoluprácu a dáta, a tým vytvára predpoklady pre jednotnejšiu prax v celej EÚ. Zároveň však platí, že účinnosť nového režimu bude stáť na detailoch vykonávacej úpravy a dohľadu, na kvalite dát a metrikách (zachytenie rizika, falošné poplachy, časy odozvy), na koherencii s rámcami kyberbezpečnosti a digitálnej odolnosti a napokon aj na edukácii používateľov. Opatrenia zamerané na techniku musia kráčať s opatreniami zameranými na človeka.

Podľa nášho názoru je potrebná pokračovať v posilňovaní včasnej prevencie a spolupráce, spresňovať definície a dôkazné štandardy tam, kde vzniká sporovosť (manipulácia, hrubá nedbanlivosť), a vyhodnocovať dopady politik na základe dôkazov. Takto nastavený rámec najlepšie vyváži tri ciele, ktoré by mali ísť ruka v ruke: ochranu používateľa, právnu istotu a udržateľnú inováciu v platbách.

Zoznam použitej literatúry

1. 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment
2. 97/489/EC: Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder
3. BRAITHWAITE, Jo: 'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like? In: *Journal of Financial Regulation*, 10, 2, (2024), 174–193. <https://doi.org/10.1093/jfr/fjae006>
4. COPENHAGEN ECONOMICS: Study on Shared Liability Regime. Kodaň: Copenhagen Economics, december 2024. 72 s. Dostupné na: <https://copenhageneconomics.com/wp-content/uploads/2024/12/Copenhagen-Economics-Study-on-shared-liability-regime-20241203-clean-final.pdf>
5. EUROPEAN PAYMENTS COUNCIL: Payments Threats and Fraud Trends Report 2024. Brusel: EPC, december 2024. 56 s. Dostupné na: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_o.pdf
6. EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2023. Haag: Europol, 2023. 52 s. Dostupné na:
7. EURÓPSKA CENTRÁLNA BANKA: ECB publikovala štatistiky kartových podvodov. Tlačová správa, 26. máj 2023. Dostupné na:

<https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230526~f09bc3c664.en.html>

8. EURÓPSKA CENTRÁLNA BANKA: Odporúčania pre bezpečnosť internetových platieb – výsledky verejnej konzultácie. Frankfurt nad Mohanom: ECB, január 2013. 16 s. Dostupné na: <https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf>
9. EURÓPSKA KOMISIA: Návrh nariadenia Európskeho parlamentu a Rady o platobných službách na vnútornom trhu a o zmene nariadenia (EÚ) č. 1093/2010 a o zrušení smernice (EÚ) 2015/2366 (COM(2023)366 final). Brusel: Európska komisia, 28. jún 2023. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52023PC0366>
10. EURÓPSKA KOMISIA: Návrh nariadenia Európskeho parlamentu a Rady o platobných službách na vnútornom trhu a o zrušení smernice (EÚ) 2015/2366 (COM(2023)367 final). Brusel: Európska komisia, 28. jún 2023. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52023PC0367>
11. EURÓPSKY ORGÁN PRE BANKOVNÍCTVO – EURÓPSKA CENTRÁLNA BANKA: Report on Payment Fraud 2024. Paríž/Frankfurt nad Mohanom: EBA/ECB, august 2024. 44 s. Dostupné na: https://www.eba.europa.eu/sites/default/files/2024-08/465e3044-4773-4e9d-8ca8-b1cd031295fc/EBA_ECB%202024%20Report%20on%20Payment%20Fraud.pdf
12. EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Single Rulebook Q&A, otázka č. 2018_4090. Dostupné na: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4090
13. EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Stanovisko k novým typom platobných podvodov a možným zmierňujúcim opatreniam. Paríž: EBA, apríl 2024. 41 s. Dostupné na: <https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf>
14. EURÓPSKY ORGÁN PRE BANKOVNÍCTVO: Usmernenia EBA o podávaní správ o podvodoch podľa PSD2 (konsolidované znenie, verzia 2). Paríž: EBA, september 2024. 47 s. Dostupné na: https://www.eba.europa.eu/sites/default/files/2024-09/73138852-34d6-452d-ad5c-42de2a2foegd/EBA%202018%20Guidelines%20on%20fraud%20reporting%20-%20Consolidated%20version%20v2_SK.pdf

15. HARASIM, Janina – KLIMONTOWICZ, Monika: Digitalisation as a determinant of new payment methods' development: The evidence from eurozone and Poland. In: *Proceedings of the European Conference on Innovation and Entrepreneurship (ECIE)*. 2021. DOI: 10.34190/EIE.21.194. Dostupné online (cit. 26.09.2025): <https://doi.org/10.34190/EIE.21.194>; DE', Rahul – PANDEY, Neena – PAL, Abhipsa: Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. In: *International Journal of Information Management*, 55, (2020), 102171. DOI: 10.1016/j.ijinfomgt.2020.102171.
16. KARPJAKOVÁ, Veronika: Právny rámec boje proti podvodom v bezhotovostných platbách v EU. In: *Právnik*, Roč. 164, č. 3 (2025), s. 227 – 242. Dostupné na: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2025/3/3_Karpjakova_227-242_3_2025.pdf
17. KELLER, Daphne – LEERSNYDER, Romain: Platform Liability for Platform Manipulation. In: *Columbia Law Review*, Vol. 124, No. 5 (2024), s. 1359 – 1442. Dostupné na: <https://columbialawreview.org/content/platform-liability-for-platform-manipulation>
18. LYU, Ce – GAO, Shenghan – ZHANG, Qingqi: The impact of time pressure and type of fraud on susceptibility to online fraud. In: *Frontiers in Psychology*, 16, (2025), 1508363. DOI: 10.3389/fpsyg.2025.1508363.
19. MARKER, Felix – SEIRA, Enrique – WILSON, Tom: Social Engineering Attacks in Financial Services: Evidence from a Large Field Experiment. In: *Proceedings of the 25th ACM Conference on Economics and Computation*, (2024), s. 1130 – 1131. DOI: 10.1145/3625546. Dostupné na: <https://dl.acm.org/doi/10.1145/3625546>
20. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/886 z 13. marca 2024, ktorým sa menia nariadenia (EÚ) č. 260/2012 a (EÚ) 2021/1230 a smernice 98/26/ES a (EÚ) 2015/2366, pokiaľ ide o okamžité úhrady v eurách
21. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011
22. NICHOLLS, Jack – KUPPA, Aditya – LE-KHAC, Nhien-An: Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. In: *IEEE Access*, 9, (2021). DOI: 10.1109/ACCESS.2021.3134076.
23. Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES
24. Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich

falšovaníu a pozmeňovaníu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV

25. Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES
26. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)
27. STEENNOT, Reinhard: Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). In: *Computer Law & Security Review*, 34, 4, (2018), 954–964
28. TAWDE, Samiksha Dattaprasad – ARORA, Sandhya – THAKUR, Yashasvee Shitalkumar: Online Payment Fraud Detection for Big Data. In: *Lecture Notes in Computer Science (LNCS)*, (2024). DOI: 10.1007/978-3-031-50583-6_22.
29. VAN PRAAG, Emanuel: Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation. In: *European Banking Institute Working Paper Series*, No. 190, (máj 2025), 28 s. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241100

Kontaktné údaje

Mgr. Peter Beňo

beno34@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

DIGITALIZÁCIA A DATAFIKÁCIA VYKAZOVANIA INFORMÁCIÍ O UDRŽATEĽNOSTI¹

DIGITIZATION AND DATAFICATION OF SUSTAINABILITY REPORTING

Katarína Poliaková²

Abstrakt: Vytváranie, agregovanie, spracovanie, sprístupňovanie a zverejňovanie informácií o udržateľnosti je ústredným prvkom predpisov v oblasti udržateľnosti (CSRD, SFDR, BMR, EUTR, EuGBR). Vykazovanie informácií o udržateľnosti vedie nevyhnutne k digitalizácii dát. Právo EÚ vyžaduje, aby boli od roku 2028 vykazované informácie o udržateľnosti prístupné cez jednotné európske miesto prístupu (ESAP). Doterajšie prístupy prípravy podávania správ o udržateľnosti nie sú efektívne, prirodzene sa vytvára potreba digitalizácie celého procesu podávania správ o udržateľnosti. Moderné digitálne platformy na vykazovanie správ o udržateľnosti predstavujú zlepšenia v dátovom manažmente a zverejňovaní informácií o udržateľnosti, pričom niektoré z nich zahŕňajú funkcie s plne automatizovaným overovaním dát (verifikáciou) alebo s analytickými nástrojmi s podporou umelej inteligencie. Cieľom príspevku je poukázať na to, že prechod na udržateľné podnikanie sa nevyhnutne prelína s digitálnou transformáciou a predstavuje dojitú transformáciu. Rámec udržateľných financií je preto vo svojej podstate dátovou stratégiou a projektom datafikácie, ktorá vykazujúcim podnikom umožňuje využiť komparatívnu výhodu prameniaku z toho, že prešli procesom digitalizácie.

Kľúčové slová: udržateľnosť, vykazovanie, digitalizácia, datafikácia, ESAP

Abstract: Creating, aggregating, processing, making available and publishing sustainability information is central to sustainability regulations (CSRD, SFDR, BMR, EUTR, EuGBR). Reporting sustainability information inevitably leads to digitization of data. EU law requires that, from 2028, the reported sustainability information is accessible via the European Single Access Point (ESAP). The current approaches to the preparation of sustainability reports are not

¹ Príspevok bol spracovaný v rámci projektu VEGA č. 1/0212/23 s názvom „Finančné inovácie ako determinant súčasnej a anticipovanej regulácie na finančnom trhu (výzvy a riziká)“.

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

effective, naturally creating a need for digitization of the entire sustainability reporting process. Modern digital platforms for sustainability reporting represent improvements in data management and disclosure of sustainability information, some of which include features with fully automated data validation (verification) or with AI-enabled analytical tools. The purpose of the paper is to point out that the transition to a sustainable business is inevitably intertwined with the digital transformation and represents a twin transformation. The sustainable finance framework is therefore essentially a data strategy and a datafication project which enables reporting companies to use the comparative advantage stemming from the fact that they have gone through the digitization process.

Key words: sustainability, reporting, digitization, datafication, ESAP

Úvod

V oblasti udržateľných financií dochádza k potrebe digitalizovať existujúce dáta o udržateľnosti alebo získavať nové dáta o udržateľnosti a digitalizovať ich. Kým pred 10 rokmi banky alebo poisťovne nemuseli potrebovať zbierať, uchovávať a spracovávať informácie o tom, či financujú nákup energeticky efektívnej nehnuteľnosti, teraz sú prostredníctvom povinnosti zverejňovať informácie o udržateľnosti ako je napr. GaR (green asset ratio), reguláciou motivované tieto dáta nielen získavať, ale ich aj spracovávať. Je prirodzené, že tieto dáta potrebujú v digitalizovanej podobe, pretože sa s nimi ďalej pracuje. Cieľom príspevku je poukázať na to, že prechod na udržateľné podnikanie sa nevyhnutne prelína s digitálnou transformáciou a predstavuje dojitú transformáciu. Rámec udržateľných financií je preto vo svojej podstate dátovou stratégiou a projektom datafikácie, ktorá vykazujúcim podnikom umožňuje využiť komparatívnu výhodu prameniaku z toho, že prešli procesom digitalizácie.

Digitalizácia, digitálne inovácie a digitálna transformácia

Na potvrdenie stanoveného cieľa je potrebné detailnejšie vysvetliť, čo chápeme pod pojmom digitalizácia, digitálne inovácie, digitálna a dvojité transformácia, keďže rôzni autori vymedzujú predmetné pojmy rozdielne. **Digitalizáciou** rozumieme používanie digitálnych technológií a údajov, ako aj ich vzájomné prepojenie, ktoré vedie k novým činnostiam alebo zmenám existujúcich činností. Základnými prvkami digitalizácie sú (i) dáta a (ii) prepojenie (z anglického interconnection), pričom digitalizácia má tiež transformatívnu povahu, ktorá sa stala stredobodom akademického výskumu s cieľom preskúmať potenciálne a skutočné dopady prijatia

digitálnych technológií na spoločnosť.³ Digitalizácia predstavuje proces konverzie analógových informácií, ako je zvuk, obraz alebo tlačенý text, na digitálne údaje, ktoré môžu byť interpretované digitálnymi zariadeniami bez degradácie a za veľmi nízke náklady. Bez digitalizácie by digitálnym technológiám chýbali dáta, čo by znemožňovalo digitálnu transformáciu.⁴ Predpokladom digitalizácie dát o udržateľnosti je štandardizácia dát, automatizácia procesov a integrácia dátových analytických metód do oblasti finančných služieb a regulačnej a dohľadovej praxe (Reg Tech a SupTech).⁵ Rozvoj digitálnych technológií a ich aplikácia v procesoch dohľadu umožnili efektívnejšie a proaktívnejšie monitorovanie rizík a identifikáciu porušení dodržiavania predpisov a viedli k zníženiu nákladov na dohľad.⁶

Digitalizácia môže prispieť k prechodu na trvalo udržateľné hospodárstvo. Je dôležité uvedomiť si, že digitalizácia môže pozitívne ale aj negatívne vplyvať na udržateľnosť. Neplatí pravidlo, že každá forma digitalizácie pozitívne prispieva k trvalo udržateľnému hospodárstvu. Negatívnym príkladom digitalizácie je potreba veľkých dátových skladov alebo ťažba kryptoaktív, pri ktorých sa zvyšuje spotreba emisií skleníkových plynov. Pozitívnym príkladom digitalizácie však môže byť e-materializácia hudby, kníh, lístkov na verejnú dopravu a pod. bez potreby ich výroby v materializovanej podobe. Ďalším príkladom digitalizácie s pozitívnym dopadom na udržateľnosť môže byť mobilita založená na elektrických vozidlách (električky, EV).⁷

Digitálne inovácie chápeme ako vývoj, nasadenie a používanie elektronických systémov, zariadení, nástrojov a zdrojov, ktoré generujú, ukladajú a spracovávajú dáta.⁸ Digitálne inovácie môžu prispieť k prechodu na trvalo udržateľné hospodárstvo

³ CEZMI OZDEMİR, Alper - PEREZ LUDENA, Miguel: The Impacts of Digitalization: Identifying emerging challenges and opportunities for sustainability reporting. Global Reporting Initiative. 45 s. <https://www.globalreporting.org/media/skogs1e/the-impact-of-digitalization-identifying-emerging-challenges-and-opportunities-for-sustainability-reporting.pdf>

⁴ BRYNJOLFSSON Erik - MCAFEE, Andrew: The Second Machine Age: Work, Progress, and Prosperity In A Time Of Brilliant Technologies. New York, London: Norton & Company, 2014. 336 s. ISBN 978-0-393-35064-7.

⁵ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

⁶ MONKIEWICZ, Jan - MONKIEWICZ, Marek: Financial sector supervision in digital age: transformation in progress. In: Foundations of Management, roč. 14, (2022), s. 25 – 36. eISSN 2300-5661, pISSN 2080-7279, DOI: 10.2478/fman-2022-0002..

⁷ MÄKITIE, Tuukka - HANSON, Jens - DAMMAN, Sigrid - WARDEBERG, Mari: Digital innovation's contribution to sustainability transitions. In: Technology in Society, roč. 73, č. 102255, (2023), s. 1 - 12. ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2023.102255>.

⁸ MÄKITIE, Tuukka - HANSON, Jens - DAMMAN, Sigrid - WARDEBERG, Mari: Digital innovation's contribution to sustainability transitions. In: Technology in Society, roč. 73, č. 102255, (2023), s. 1 - 12. ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2023.102255>.

prostredníctvom prepojenia s udržateľnými inováciami.⁹ Podniky, ktoré rezignujú na digitálne inovácie, môžu dokonca čeliť riziku úpadku, čoho príkladom je spoločnosť Kodak, ktorá neudržala krok s digitálnou revolúciou, v čase svojho vrcholu mala hodnotu 31 miliárd dolárov a zamestnávala 150 tisíc ľudí, avšak pre neschopnosť zachytiť trendy, došlo k jej úpadku¹⁰. Digitalizácia a digitálne inovácie teda môžu predstavovať aj nevyhnutnosť pre podnik na prežitie.

Digitálnou transformáciou rozumieme ekonomické a spoločenské dopady (účinky) digitalizácie a samotnú digitalizáciu.¹¹ Ústredným prvkom digitálnej transformácie je **fyzická infraštruktúra** (dátové centrá, podmorské a podzemné káble z optických vlákien, satelity, mobilné veže a základňové stanice a osobné zariadenia) a **digitálne technológie** (umelá inteligencia (AI), strojové učenie ako súčasť AI, analýza veľkých dát (big data analytics), cloud technológia, internet of things (IoT), rôzne digitálne služby cez online platformy).¹² Niektorými autormi sa označuje digitálna transformácia (z anglického *digital transition*) a prechod na udržateľnosť (z anglického *sustainability transition*) ako dvojité transformácie (z anglického *twin transition*).¹³ **Dvojité transformácie** sa môže deliť na **postupnú** dvojité transformáciu a **radikálnu** dvojité transformáciu. Kým postupná dvojité transformácia predstavuje postupné inovácie prostredníctvom zvyšovania výkonu a hodnoty existujúcej technológie, zmierňuje problémy v prevládajúcich, existujúcich technológiách, radikálna transformácia predstavuje inovácie, ktoré sú zásadnejšie. Radikálne inovácie narúšajú existujúce vzorce výroby a spotreby, vyvoláva potrebu nových vedomostí a kompetencií a môže viesť k vytvoreniu nových odvetví, vedie k

⁹ MÄKITIE, Tuukka - HANSON, Jens - DAMMAN, Sigrid - WARDEBERG, Mari: Digital innovation's contribution to sustainability transitions. In: Technology in Society, roč. 73, č. 102255, (2023), s. 1 - 12. ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2023.102255>.

¹⁰ EDMANS, Alex: The End of ESG. In: Financial Management, roč. 52, č. 1, (2023), s. 3-17. SSRN: <https://ssrn.com/abstract=4221990> or <http://dx.doi.org/10.2139/ssrn.4221990>

¹¹ OECD (2019) Going Digital: Shaping Policies, Improving Lives. Paríž: OECD Publishing. 18 s. <https://doi.org/10.1787/9789264312012-en>

¹² CEZMI OZDEMIR, Alper - PEREZ LUDENA, Miguel: The Impacts of Digitalization: Identifying emerging challenges and opportunities for sustainability reporting. Global Reporting Initiative. 45 s. <https://www.globalreporting.org/media/55kogs1e/the-impact-of-digitalization-identifying-emerging-challenges-and-opportunities-for-sustainability-reporting.pdf>

¹³ HUSAIN, Shaiara, SOHAG, Kazi, WU, Yanrui: The response of green energy and technology investment to climate policy uncertainty: An application of twin transitions strategy. In: Technology in Society, roč. 71, č. 102132, (2022). ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2022.102132>. FERREIRA, Joao J. - FERNANDES, Cristina I., MOTA VEIGA, Pedro, CAPUTO, Andrea: The interactions of entrepreneurial attitudes, abilities and aspirations in the (twin) environmental and digital transitions? A dynamic panel data approach. In: Technology in Society, roč. 71, č. 102121, (2022), ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2022.102121>

rekonfiguráciám sociálno-technických systémov, označované aj ako systémové prechody smerom k zásadne novým vzorcom výroby a spotreby.¹⁴

Vykazovanie informácií o udržateľnosti v digitálnej podobe

Smernica CSRD v recitáli 55 uvádza, že používatelia informácií o udržateľnosti očakávajú, že podniky budú zverejňovať informácie o udržateľnosti elektronicky a tieto informácie o udržateľnosti budú vyhľadateľné, porovnateľné a strojovo čitateľné v digitálnych formátoch¹⁵. Z uvedeného dôvodu smernica CSRD, na rozdiel od smernice NFRD, zavádza v článku 29d povinnosť, aby boli vykazované informácie o udržateľnosti zverejňované **v elektronickom formáte**¹⁶ v súlade s článkom 3 delegovaného nariadenia Komisie (EÚ) 2019/815, pokiaľ ide o regulačné technické predpisy o špecifikácii jednotného elektronického formátu vykazovania (ESEF, z anglického European Single Electronic Format)¹⁷ a zároveň aj **označované** v súlade s delegovaným nariadením Komisie (EÚ) 2019/815. Článok 3 delegovaného nariadenia Komisie (EÚ) 2019/815 uvádza povinný formát zverejňovania - **XHTML**. Článok 4 delegovaného nariadenia Komisie (EÚ) 2019/815 uvádza povinnosť označovania (z anglického *mark up*) konsolidovaných účtovných závierok, ak ročné finančné správy obsahujú konsolidované účtovné závierky podľa IFRS, pričom používajú značkový jazyk XBRL. Článok 5 delegovaného nariadenia Komisie (EÚ) 2019/815 uvádza právo (možnosť) označovania ostatných častí výročných správ. Toto digitálne označovanie znamená, že vyhľadávací software by mal jednoducho identifikovať, ktoré zverejnené dáta poskytujú informácie o konkrétnych rizikách ohrozujúcich udržateľnosti alebo o vplyvoch na udržateľnosť.¹⁸

¹⁴ MÄKITIE, Tuukka - HANSON, Jens - DAMMAN, Sigrid - WARDEBERG, Mari: Digital innovation's contribution to sustainability transitions. In: Technology in Society, roč. 73, č. 102255, (2023), s. 1 - 12. ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2023.102255>.

¹⁵ recitál 55 smernice EP a Rady (EÚ) 2022/2464 pokiaľ ide o vykazovanie informácií o udržateľnosti podnikov (CSRD)

¹⁶ MACCHIAVELLO, Eugenia: Greenwashing in investment intermediation: investor protection and the difficult role of enforcement. In: EUSFiL Research Working Paper Series, č. 28, (2024), 78 s. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4957242

¹⁷ delegované nariadenie Komisie (EÚ) 2019/815 zo 17. decembra 2018, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2004/109/ES, pokiaľ ide o regulačné technické predpisy o špecifikácii jednotného elektronického formátu vykazovania (Ú. v. EÚ L 143, 29.5.2019, s. 1)

¹⁸ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

Jednotné Európske miesto prístupu (ESAP)

V budúcnosti sa plánuje zverejňovať vykazované informácie o udržateľnosti aj v jednotnom európskom mieste prístupu (z anglického *European Single Access Point*, ďalej len „**ESAP**“), ktoré bude poskytovať centralizovaný elektronický prístup k rôznym zverejňovaným informáciám. Jednotné európske miesto prístupu (ESAP) má zriadiť a prevádzkovať od 10. júla 2027 Európsky orgán pre cenné papiere a trhy ESMA (z anglického *European Securities and Markets Authority*).¹⁹ V ESAP budú sprístupnené informácie jednak na **povinnej báze** ako aj na **dobrovoľnej báze**.

Povinne sa v ESAP budú sprístupňovať informácie, ktoré sa povinne zverejňujú podľa 36 osobitných právnych predpisov vymenovaných v prílohe nariadenia (EÚ) 2023/2859²⁰ (ďalej len „**nariadenie ESAP**“). Nariadenie ESAP vymenúva 19 nariadení a 17 smerníc na úrovni level 1. Povinnosť zverejňovania vybraných informácií cez jednotné európske miesto prístupu (ESAP) je upravené v dvoch osobitných predpisoch:

- (i) vo vzťahu k 19 nariadeniam v nariadení úrovne level 1, ktoré sa niekedy označuje ako ESAP súhrnné nariadenie (z anglického *ESAP Omnibus Regulation*)²¹,
- (ii) vo vzťahu k 16 smerniciam v smernici úrovne level 1, ktoré sa niekedy označuje ako ESAP súhrnná smernica (z anglického *ESAP Omnibus Directive*)²². ESAP súhrnná smernica neupravuje novelizáciu všetkých 17 smerníc vymenovaných v časti B prílohy k ESAP nariadeniu, pretože čl. 17 smernice EP a Rady 2024/1760 CSDDD už v čase prijatia smernice CSDDD obsahovala ustanovenie vo vzťahu k povinnosti zverejňovania určitých údajov cez ESAP.

Povinnosť zverejňovania informácií cez ESAP je upravená v troch fázach:

- (i) **1. fáza** - prístupnosť informácií od **10.07.2026** (nariadenie EP a Rady (EÚ) č. 2017/1129 o prospektoch, nariadenie EP a Rady (EÚ) č. 236/2012 o predaji nakrátko; smernica EP a Rady 2004/109/ES o transparentnosti),
- (ii) **2. fáza** - prístupnosť informácií od **10.01.2028** [nariadenie EP a Rady (ES) č. 1060/2009 (CRAR), nariadenie EP a Rady (EÚ) č. 345/2013 (EuVECA), nariadenie EP a Rady (EÚ) č. 346/2013 (EuSEF), nariadenie EP a Rady (EÚ) č. 596/2014 (MAR), nariadenie EP a Rady (EÚ) č. 1286/2014 (PRIIPS), nariadenie EP a Rady

¹⁹ čl. 1 (1) nariadenia Európskeho parlamentu a Rady (EÚ) 2023/2859 z 13. decembra 2023, ktorým sa zriaďuje jednotné európske miesto prístupu, ktoré poskytuje centralizovaný prístup k verejne dostupným informáciám týkajúcim sa finančných služieb, kapitálových trhov a udržateľnosti

²⁰ článok 1 ods. 1 písm. a) nariadenia Európskeho parlamentu a Rady (EÚ) 2023/2859 z 13. decembra 2023, ktorým sa zriaďuje jednotné európske miesto prístupu, ktoré poskytuje centralizovaný prístup k verejne dostupným informáciám týkajúcim sa finančných služieb, kapitálových trhov a udržateľnosti

²¹ nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2869 z 13. decembra 2023, ktorým sa menia určité nariadenia, pokiaľ ide o zriadenie a fungovanie jednotného európskeho miesta prístupu

²² smernica Európskeho parlamentu a Rady (EÚ) 2023/2864 z 13. decembra 2023, ktorou sa menia určité smernice, pokiaľ ide o zriadenie a fungovanie jednotného európskeho miesta prístupu

(EÚ) 2016/1011 (BMR), nariadenie EP a Rady (EÚ) č. 2019/1238 (PEPP), nariadenie EP a Rady (EÚ) 2019/2088 (SFDR); smernica EP a Rady 2009/65/ES UCITS, smernica EP a Rady 2013/34/EÚ o účtovných závierkach, smernica EP a Rady 2014/65/EÚ (MiFID II)],

- (iii) **3. fáza** - prístupnosť informácií od **10.01.2030** (nariadenie CRAR, nariadenie EP a Rady (EÚ) č. 575/2013 (CRR), nariadenie EP a Rady (EÚ) č. 537/2014 o štatutárnom audite subjektov verejného záujmu, nariadenie EP a Rady (EÚ) č. 600/2014 (MIFIR), nariadenie EP a Rady (EÚ) č. 2015/760 (ELTIF), nariadenie EP a Rady (EÚ) č. 2015/2365 (SFTR), nariadenie EP a Rady (EÚ) č. 2017/1131 (MMR), nariadenie EP a Rady (EÚ) č. 2019/2033 (IFR), nariadenie EP a Rady (EÚ) č. 2023/1114 (MiCA), nariadenie EP a Rady (EÚ) 2023/2631 (EuGBR); smernica EP a Rady 2013/36/EÚ (CRD), smernica EP a Rady 2002/87/ES o finančných konglomerátoch, smernica EP a Rady 2004/25/ES o ponukách na prevzatie, smernica EP a Rady 2006/43/ES o štatutárnom audite, smernica EP a Rady 2007/36/ES o právach akcionárov, smernica EP a Rady 2011/61/EÚ (AIFMD), smernica EP a Rady 2009/138/ES Solventnosť II, smernica EP a Rady 2014/59/EÚ o riešení krízových situácií, smernica EP a Rady č. (EÚ) 2016/97 (IDD), smernica EP a Rady (EÚ) č. 2016/2341 (IZDZ), smernica EP a Rady (EÚ) č. 2019/2034 (IFD), smernica EP a Rady (EÚ) č. 2019/2162 o krytých dlhopisoch).

Dobrovoľne bude možné sprístupniť informácie podľa článku 1 ods. 1 písm. b) nariadenia ESAP až v tretej fáze projektu, a to od 10. januára 2030. Dobrovoľné sprístupnenie budú môcť využiť podniky alebo subjekty, ktoré sa riadia právom členského štátu EÚ. Ak sa tieto subjekty rozhodnú dobrovoľne sprístupniť cez ESAP informácie, nemôže ísť o akékoľvek informácie (napr. marketingový materiál), ale musí ísť o informácie, ktoré sa „*uvádzajú v legislatívnych aktoch Únie uvedených v prílohe alebo v akýchkoľvek ďalších právne záväzných aktoch Únie, v ktorých sa stanovuje centralizovaný elektronický prístup k informáciám*“ cez ESAP. Navyše budú musieť tieto informácie spĺňať technické požiadavky v súlade s článkom 3 ods. 1 nariadenia ESAP.

Orgánom zberu údajov (ďalej len „OZÚ“) je „*orgán Únie, úrad alebo agentúra alebo vnútroštátny orgán, úrad alebo register určený za takýto orgán podľa akýchkoľvek legislatívnych aktov Únie podľa článku 1 ods. 1 písm. a) alebo určený za takýto orgán členským štátom v súlade s článkom 3 ods. 2*“²³. V niektorých prípadoch bude OZÚ priamo ESMA a v niektorých prípadoch musia členské štáty určiť jeden alebo viac národných orgánov. V zmysle článku 3 ods. 2 nariadenia ESAP musia členské štáty určiť aspoň jeden OZÚ na účely zberu dobrovoľne predkladaných informácií a oznámiť to orgánu ESMA do 09.01.2030. Zoznam OZÚ bude viesť ESMA²⁴.

²³ Článok 2 ods. 2 nariadenia ESAP

²⁴ Článok 4 nariadenia ESAP

ESMA bude plniť funkciu OZÚ podľa nasledujúcich nariadení a smerníc: nariadenie CRAR, nariadenie EuVECA, EuSEF, MMR, ELTIF, MIFIR, SFTR, BMR a EuGBR (zdieľané s národnými OZÚ), smernica AIFMD. EBA bude OZÚ podľa nariadenia CRR a IFR. Úrad pre dohľad nad výkonom štatutárneho auditu (ÚDVA) bude OZÚ na základe § 53 ods. 1 písm. l) zákona č. 423/2015 Z.z. o štatutárnom audite vo vzťahu k smernici o štatutárnom audite a nariadeniu o štatutárnom audite subjektov verejného záujmu. Podľa § 23e ods. 1 a ods. 5 zákona o účtovníctve (ZoÚ) určila Slovenská republika za OZÚ Ministerstvo financií SR pre účely zberu údajov na povinnej báze na základe smernice o účtovných závierkach a pre účely zberu údajov na dobrovoľnej báze.

Podľa zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona 187/2025 Z.z. určila Slovenská republika Národnú banku Slovenska za OZÚ pre väčšinu dátových tokov, pri ktorých mal OZÚ určiť členský štát v súvislosti s projektom ESAP. Zákomom 187/2025 Z.z. boli novelizované aj jednotlivé sektorové zákony za účelom určenia povinnosti oznamovania alebo sprístupňovania určitých dát cez ESAP. NBS sa stala OZÚ vo vzťahu k právnym predpisom uvedeným v poznámke pod čiarou 19b v novom § 5a zákona č. 747/2004 Z. z. V zmysle bodu 23.1. Legislatívnych pravidiel vlády Slovenskej republiky „poznámky pod čiarou k príslušným odkazom nie sú súčasťou právneho predpisu; majú informatívnu hodnotu. Preto nesmú obsahovať veci, ktoré majú normatívnu povahu.“ Z uvedeného dôvodu vyvstáva otázka, či určenie NBS za OZÚ touto legislatívnou technikou bola vhodná voľba.

Datafikácia

Datafikáciou rozumieme aplikáciu analytických nástrojov na digitalizované dáta²⁵, ako sú napríklad algoritmy a dátovo riadené aplikácie (napr. strojové učenie).²⁶ Tieto nástroje sú využívané v oblasti udržateľných financií. **Rámec udržateľných financií je vo svojej podstate dátovou stratégiou a projektom datafikácie.**²⁷ Existuje priame spojenie medzi udržateľnými financiami a datafikáciou, pričom existencia predpisov v oblasti udržateľných financií by nebola možná bez digitalizácie.

²⁵ BUCKLEY, Ross P. - ARNER, Douglas W. - ZETZSCHE, Dirk A.: FinTech – Finance, Technology and Regulation. Cambridge University Press, 2023. 330 s. ISBN 9781009086943.

²⁶ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

²⁷ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

Vytváranie, agregovanie, spracovanie, sprístupňovanie a zverejňovanie informácií o udržateľnosti je ústredným prvkom predpisov v oblasti udržateľnosti ako je smernica CSRD, nariadenie o EÚ taxonómii, nariadenia SFDR, nariadenia BMR alebo nariadenia EuGBR, ktoré sú základom Európskeho rámca udržateľných financií.²⁸ Smernica CSRD požaduje, aby vykazované informácie boli porovnateľné, spoľahlivé a aby ich používatelia mohli ľahko vyhľadať a narábať s nimi pomocou digitálnych technológií.²⁹ V minulosti sa údaje uchovávali manuálne, správy sa pripravovali v tabuľkových procesoroch a používali sa papierové systémy na spracovanie údajov o udržateľnosti. Keďže regulácia alebo trhové štandardy požadujú spracovanie množstva veľkého objemu zložitých údajov o udržateľnosti, dátový manažment zostal neúplný a neefektívny. Tieto staré prístupy majú spoločné znaky v tom, že môžu spôsobovať nezrovnalosti v údajoch, neskorší termín vykazovania a problémy s komunikovaním a vysvetlením údajov počas auditu.³⁰

Keďže doterajší prístup prípravy podávania správ o udržateľnosti nie je efektívny a udržateľný z dlhodobého hľadiska, prirodzene sa vytvorila potreba digitalizácie dát a digitalizácie celého procesu podávania správ o udržateľnosti. Zložitosť údajov a informácií si vyžaduje hlboké a podrobné pochopenie obchodných operácií, ktoré môžu mať iba interní zamestnanci.³¹ Preto je nevyhnutné, aby boli do projektu digitalizácie celého procesu podávania správ o udržateľnosti zapojení interní zamestnanci aj v takom prípade, ak podnik využíva služby externých odborných poradcov alebo implementuje moderné digitálne platformy na vykazovanie správ o udržateľnosti.

Moderné digitálne platformy na vykazovanie správ o udržateľnosti sú veľkým zlepšením v dátovom manažmente a zverejňovaní informácií o udržateľnosti.³² Ich

²⁸ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

²⁹ HESEKOVÁ, Simona: Problematika ESG na finančných trhoch. In: V. Slovensko-české dni daňového práva. Daňové právo a nové javy v ekonomike. Recenzovaný zborník vedeckých prác. Univerzita Pavla Jozefa Šafárika. Košice, roč. 5, (2023), s. 105 - 115. <https://doi.org/10.33542/VSCD-0269-5-07>, ISBN 978-80-574-0269-5.

³⁰ IRIANTO, Okto - ADIATMA, Tina - RACHMAN, Adi M.: Digital Platforms for Sustainability Reporting: A Review of Bridging Business Ethics and Economic Transformation. In: Account and Financial Management Journal, roč. 10, č. 2, (2025), s. 3491-3500. <https://doi.org/10.47191/afmj/v10i2.01>

³¹ FORNASARI, Tommaso - TRAVERSI, Marco: The Impact of the CSRD and the ESRS on Non-Financial Disclosure. In: Symphonia. Emerging Issues in Management. New Perspectives in Global Competition, č. 1 (2024), s. 117 - 133. <https://dx.doi.org/10.4468/2024.1.07fornasari.traversi>

³² SALAMZADEH, Aidin - HADIZADEH, Morteza - FEYZABADI, Javad Ghaffari - YASIN, Naveed - PARAMBA, Jumana Nalakam: The Role of Digital Platforms in Transforming Corporate Governance: A Path to Sustainability Through ESG. In S. Ed-Dafali, F. Özşungur, & M. Mohiuddin (Eds.), Modern

pridanou hodnotou je, že umožňujú integráciu rôznych zdrojov údajov, automatizujú zber údajov, niekedy spojenú so schopnosťou zhromažďovať údaje v reálnom čase, pokročilé vizualizačné nástroje a prichádzajú s vylepšenými analytickými schopnosťami.³³ Digitalizované platformy na vykazovanie správ o udržateľnosti zvyčajne zahŕňajú uhlíkové účtovníctvo, sledovanie udržateľnosti v rámci hodnotového (dodávateľského) reťazca a komplexné sledovanie výkonnosti ESG.³⁴ Niektoré pokročilé digitálne platformy na vykazovanie informácií o udržateľnosti zahŕňajú množstvo ďalších funkcií s plne automatizovaným overovaním dát (verifikáciou), s analytickými nástrojmi s podporou AI napríklad na predikovanie trendov v oblasti udržateľnosti, nástroje na analýzu scenárov pre hodnotenie klimatických rizík, alebo moduly zapojenia zainteresovaných strán na riadenie komunikácie s rôznymi zainteresovanými stranami³⁵, niektoré aj s využitím blockchainu³⁶. Mnohé z nich už dokážu integrovať algoritmy pre strojové učenie pre lepšiu presnosť a detekciu príležitostí na zvýšenie výkonu v oblasti udržateľnosti.³⁷ Povinná digitalizácia údajov vedie k zachyteniu dát o rizikách ohrozujúcich udržateľnosť a o vplyvoch na udržateľnosť do štandardizovaných súborov údajov, ktoré možno automaticky analyzovať prostredníctvom rôznych foriem analýzy. Podniky, ktoré povinne zverejňujú alebo vykazujú dáta o udržateľnosti, musia zrevidovať svoje interné procesy za účelom zhromaždenia údajov a vytvorenia správ (reportingu) s tým, že použitie automatizovaných riešení založených na dátach sa môže stať nevyhnutnosťou. Tieto riešenia môžu zahŕňať potrebu vytvorenia dátových skladov, nástrojov na zber dát, nástrojov na vytvorenie správ (výkazov, reportov) ako aj nástrojov na verifikáciu údajov použitú riadením rizík alebo dohľadom. Je zaujímavé, že samotná smernica CSRD alebo ESRS štandardy neukladajú podnikom povinnosť digitalizovať svoje interné procesy vo forme príkazu.

Corporate Governance Strategies for Sustainable Value Creation, 2025. S. 111-136. IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-6750-6.ch006>.

³³ LAGODIYENKO, Oleg: Using Digital Platforms for Reporting in The Implementation And Evaluation of ESG Strategies. In: Economic Scope, roč. 192, (2024). S. 63 – 67. <https://doi.org/10.30838/EP.192.63-67>

³⁴ YUZGENC, Ibrahim Umut - AYDEMIR, Erdal: Sustainable ERP Systems: A Green Perspective. In: International Conference on Pioneer and Innovative Studies, č. 1, (2023). S. 533 – 538. <https://doi.org/10.59287/icpis.886>

³⁵ IRIANTO, Okto - ADIATMA, Tina - RACHMAN, Adi M.: Digital Platforms for Sustainability Reporting: A Review of Bridging Business Ethics and Economic Transformation. In: Account and Financial Management Journal, roč. 10, č. 2, (2025), s. 3491–3500. <https://doi.org/10.47191/afmj/v10i2.01>

³⁶ SARAJOTI, Pattarake - CHATJUTHAMARD, Pattanaporn - PAPANGKORN, Suwongrat - PHIROMSWAD, Piyachart: CSR Reporting and Blockchain Technology. In: Corporate Social Responsibility in the 21st Century, (2023). 376 s. <https://doi.org/10.5772/intechopen.105512>

³⁷ IRIANTO, Okto - ADIATMA, Tina - RACHMAN, Adi M.: Digital Platforms for Sustainability Reporting: A Review of Bridging Business Ethics and Economic Transformation. In: Account and Financial Management Journal, roč. 10, č. 2, (2025), s. 3491–3500. <https://doi.org/10.47191/afmj/v10i2.01>

Digitalizácia a datafikácia procesov sa však stáva potrebou alebo nevyhnutnosťou na splnenie regulačných povinností. Podniky, ktoré budú úspešnejšie v prechode na automatizáciu a digitalizáciu zhromažďovania a zverejňovania dát budú mať **kompetitívnu výhodu**. Tieto podniky, pôsobiace v sektore finančných služieb, by mohli prinášať na trh skôr alebo kvalitnejšie finančné produkty s aspektami udržateľnosti, eventuálne podniky emitujúce dlhopisy by mohli emitovať zelené dlhopisy.³⁸

Záver

Cieľom príspevku je poukázať na to, že prechod na udržateľné podnikanie sa nevyhnutne prelína s digitálnou transformáciou a predstavuje dojitú transformáciu. Vytváranie, agregovanie, spracovanie, sprístupňovanie a zverejňovanie informácií o udržateľnosti je ústredným prvkom predpisov v oblasti udržateľnosti (CSRD, SFDR, BMR, EUTR, EuGBR). Vykazovanie informácií o udržateľnosti vedie nevyhnutne k digitalizácii dát, už len preto, že ich bude potrebné zverejňovať cez ESAP. Digitalizácia a datafikácia procesov sa stáva potrebou alebo nevyhnutnosťou na splnenie regulačných povinností. Rámec udržateľných financií je preto vo svojej podstate dátovou stratégiou a projektom datafikácie, ktorá vykazujúcim podnikom umožňuje využiť komparatívnu výhodu prameniacu z toho, že prešli procesom digitalizácie. Zverejňovanie informácií o udržateľnosti, či už na povinnej alebo dobrovoľnej báze, je indikátorom toho, že podnik má svoje dátové toky pod kontrolou a nevyhnutne musel prejsť procesom digitalizácie.

Podniky, ktoré budú úspešnejšie v prechode na automatizáciu a digitalizáciu zhromažďovania a zverejňovania dát o udržateľnosti budú mať preto kompetitívnu výhodu. Budú ju mať nielen preto, že budú o nich k dispozícii informácie o rôznych aspektoch udržateľnosti a preto budú atraktívnejšie pre inštitucionálnych investorov alebo potenciálnych dodávateľov alebo odberateľov, ale najmä preto, že predpokladom vykazovania informácií o udržateľnosti je digitalizácia a datafikácia procesov v tejto spoločnosti. Tie podniky, ktoré využijú rozumne moderné digitálne platformy na vykazovanie správ o udržateľnosti a zlepšia svoj dátový manažment, môžu navyše ťažiť z výhod, ktoré súvisia s novými funkciami týchto platforiem ako je napríklad plne automatizované overovanie dát (verifikácia) alebo analytické nástroje s podporou umelej inteligencie.

³⁸ ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.

Zoznam použitej literatúry

1. CEZMI OZDEMIR, Alper - PEREZ LUDENA, Miguel: The Impacts of Digitalization: Identifying emerging challenges and opportunities for sustainability reporting. Global Reporting Initiative. 45 s. <https://www.globalreporting.org/media/s5kogs1e/the-impact-of-digitalization-identifying-emerging-challenges-and-opportunities-for-sustainability-reporting.pdf>
2. BRYNJOLFSSON Erikk - MCAFEE, Andrew: The Second Machine Age: Work, Progress, and Prosperity In A Time Of Brilliant Technologies. New York, London: Norton & Company, 2014. 336 s. ISBN 978-0-393-35064-7.
3. ZETZSCHE, Dirk A. - UNTERSTELL, Marian - BUCKLEY, Ross P. - ARNER, Douglas W.: Datafication of Sustainable Finance. In: UNSW Law Research Paper, roč. 24-19 (2024), University of Hong Kong Faculty of Law Research Paper č. 2024/18, FutureFinTech Working Paper Series. 38 s. SSRN: <https://ssrn.com/abstract=4879687> alebo <http://dx.doi.org/10.2139/ssrn.4879687>.
4. MONKIEWICZ, Jan – MONKIEWICZ, Marek: Financial sector supervision in digital age: transformation in progress. In: Foundations of Management, roč. 14, (2022), s. 25 – 36. eISSN 2300-5661, pISSN 2080-7279, DOI: 10.2478/fman-2022-0002..
5. MÄKITIE, Tuukka - HANSON, Jens - DAMMAN, Sigrid - WARDEBERG, Mari: Digital innovation's contribution to sustainability transitions. In: Technology in Society, roč. 73, č. 102255, (2023), s. 1 - 12. ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2023.102255>.
6. EDMANS, Alex: The End of ESG. In: Financial Management, roč. 52, č. 1, (2023), s. 3-17. SSRN: <https://ssrn.com/abstract=4221990> or <http://dx.doi.org/10.2139/ssrn.4221990>
7. OECD (2019) Going Digital: Shaping Policies, Improving Lives. Paríž: OECD Publishing. 18 s. <https://doi.org/10.1787/9789264312012-en>
8. HUSAIN, Shaiara, SOHAG, Kazi, WU, Yanrui: The response of green energy and technology investment to climate policy uncertainty: An application of twin transitions strategy. In: Technology in Society, roč. 71, č. 102132, (2022). ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2022.102132>.
9. FERREIRA, Joao J. - FERNANDES, Cristina I., MOTA VEIGA, Pedro, CAPUTO, Andrea: The interactions of entrepreneurial attitudes, abilities and aspirations in the (twin) environmental and digital transitions? A dynamic panel data approach. In: Technology in Society, roč. 71, č. 102121, (2022), ISSN 0160-791X. <https://doi.org/10.1016/j.techsoc.2022.102121>.

10. BUCKLEY, Ross P. - ARNER, Douglas W. - ZETZSCHE, Dirk A.: FinTech – Finance, Technology and Regulation. Cambridge University Press, 2023. 330 s. ISBN 9781009086943.
11. HESEKOVÁ, Simona: Problematika ESG na finančných trhoch. In: V. Slovensko-české dni daňového práva. Daňové právo a nové javy v ekonomike. Recenzovaný zborník vedeckých prác. Univerzita Pavla Jozefa Šafárika. Košice, roč. 5, (2023), s. 105 - 115. <https://doi.org/10.33542/VSCD-0269-5-07>, ISBN 978-80-574-0269-5.
12. IRIANTO, Okto - ADIATMA, Tina - RACHMAN, Adi M.: Digital Platforms for Sustainability Reporting: A Review of Bridging Business Ethics and Economic Transformation. In: Account and Financial Management Journal, roč. 10, č. 2, (2025), s. 3491–3500. <https://doi.org/10.47191/afmj/v10i2.01>
13. FORNASARI, Tommaso - TRAVERSI, Marco: The Impact of the CSRD and the ESRS on Non-Financial Disclosure. In: Symphonya. Emerging Issues in Management. New Perspectives in Global Competition, č. 1 (2024), s. 117 - 133. <https://dx.doi.org/10.4468/2024.1.07fornasari.traversi>
14. SALAMZADEH, Aidin - HADIZADEH, Morteza - FEYZABADI, Javad Ghaffari - YASIN, Naveed - PARAMBA, Jumana Nalakam: The Role of Digital Platforms in Transforming Corporate Governance: A Path to Sustainability Through ESG. In S. Ed-Dafali, F. Özsungur, & M. Mohiuddin (Eds.), Modern Corporate Governance Strategies for Sustainable Value Creation, 2025. S. 111-136. IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-6750-6.ch006>.
15. LAGODIYENKO, Oleg: Using Digital Platforms for Reporting in The Implementation And Evaluation of ESG Strategies. In: Economic Scope, roč. 192, (2024). S. 63 – 67. <https://doi.org/10.30838/EP.192.63-67>
16. YUZGENC, Ibrahim Umut - AYDEMIR, Erdal: Sustainable ERP Systems: A Green Perspective. In: International Conference on Pioneer and Innovative Studies, č. 1, (2023). S. 533 – 538. <https://doi.org/10.59287/icpis.886>
17. SARAJOTI, Pattarake - CHATJUTHAMARD, Pattanaporn - PAPANGKORN, Suwongrat - PHIROMSWAD, Piyachart: *CSR Reporting and Blockchain Technology*. In: Corporate Social Responsibility in the 21st Century, (2023). 376 s. <https://doi.org/10.5772/intechopen.105512>
18. MACCHIAVELLO, Eugenia: Greenwashing in investment intermediation: investor protection and the difficult role of enforcement. In: EUSFiL Research Working Paper Series, č. 28, (2024), 78 s. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4957242
19. smernica EP a Rady (EÚ) 2022/2464 pokiaľ ide o vykazovanie informácií o udržateľnosti podnikov (CSRD)
20. delegované nariadenie Komisie (EÚ) 2019/815 zo 17. decembra 2018, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2004/109/ES, pokiaľ ide o regulačné technické predpisy o špecifikácii jednotného elektronického formátu

vykazovania (Ú. v. EÚ L 143, 29.5.2019, s. 1) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0815-20250101>

21. nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2859 z 13. decembra 2023, ktorým sa zriaďuje jednotné európske miesto prístupu, ktoré poskytuje centralizovaný prístup k verejne dostupným informáciám týkajúcim sa finančných služieb, kapitálových trhov a udržateľnosti <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02023R2859-20240725>
22. nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2869 z 13. decembra 2023, ktorým sa menia určité nariadenia, pokiaľ ide o zriadenie a fungovanie jednotného európskeho miesta prístupu <https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1705688054648&uri=CELEX%3A32023R2869>
23. smernica Európskeho parlamentu a Rady (EÚ) 2023/2864 z 13. decembra 2023, ktorou sa menia určité smernice, pokiaľ ide o zriadenie a fungovanie jednotného európskeho miesta prístupu https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=OJ%3AL_202302864

Kontaktné údaje

JUDr. Katarína Poliaková, LL.M.

poliakova42@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

TRANSPARENTNOSŤ ALEBO NADBYTOČNÉ DÁTOVÉ STOPY V KYBERPRIESTORE V KONTEXTE KRYPTOAKTÍV¹

TRANSPARENCY OR EXCESSIVE DATA TRACES IN CYBERSPACE IN THE CONTEXT OF CRYPTO-ASSETS

Klaudia Keratová²

Abstrakt: Cieľom tohto príspevku je identifikácia rozsahu informačných povinností, ktoré sú subjekty poskytujúce finančné služby v oblasti kryptoaktív povinné zhromažďovať za účelom zabezpečenia transparentnosti jednotlivých transakčných tokov. Autorka v príspevku, za využitia analýzy a komparácie príslušných regulačných rámcov identifikuje, či legitímny záujem verejnej moci bojovať proti praniu špinavých peňazí nespôsobuje nadbytočné zdieľanie dát v kyberpriestore. Takýto stav totiž môže spôsobovať riziko zraniteľnosti dotknutých údajov, ako aj ich pôvodcov, pretože ich odcudzenie môže viesť k ich zneužitiu na iné nelegálne aktivity. V súčasnosti majú práve regulačné opatrenia zabezpečiť, aby príslušné subjekty finančného trhu, ako osoby v prvej línii boja proti praniu špinavých peňazí overovali legitímnosť každého prevodu kryptoaktív. Tieto opatrenia však majú skôr substantívnu povahu a neponúkajú technické riešenia na ich efektívne zavedenie. Chrániť dáta, ktoré majú charakter osobných údajov, a zároveň byť zárukou transparentnosti pre prípadné zneužitie dotknutých údajov ostáva minimálne výzvou. Najmä, ak je možné niektoré opatrenia plniť len formálne.

Kľúčové slová: transparentnosť, kryptoaktíva, TFR, riziko zraniteľnosti

Abstract: The aim of this paper is to identify the scope of information obligations that financial service providers in the field of crypto-assets are required to collect to ensure the transparency of transaction flows. By employing analysis and comparison of the relevant regulatory frameworks, the author examines whether the legitimate interest of public authorities in combating money laundering results in excessive data sharing online. Such a situation may create risks regarding the vulnerability of the affected data and their originators, as the theft of such information could result in its misuse for

¹ Predložený príspevok je čiastkovým výstupom projektu APVV-22-0482 Financovanie územnej samosprávy – potenciál funkčných mikroregiónov.

² Právnická fakulta Univerzity Komenského v Bratislave, Katedra finančného práva.

other illicit activities. At the present time, regulatory measures are designed to ensure that financial market entities, as front-line actors in the fight against money laundering, verify the legitimacy of each transfer of crypto-assets, albeit without offering technical solutions. These measures are primarily substantive in nature and do not provide technical solutions for their effective implementation. Safeguarding personal data while at the same time guaranteeing transparency to prevent potential misuse of such data remains a considerable challenge, especially when certain measures are fulfilled only formally.

Key words: transparency, crypto-assets, TFR, risk of vulnerability

Úvod

Pretrvávajúca technologická revolúcia a digitalizácia nástrojov finančného trhu menia podobu finančných služieb. Finančné služby dokážu byť efektívnejšie, pretože technologické prvky v zásade podporujú rýchlosť finančných transakcií a znižujú transakčné náklady.³ Pre zachovanie vzájomnej dôvery medzi jednotlivými aktérmi finančného trhu sa však vyžaduje verejnoprávna regulácia⁴, ktorá je potrebná pre adekvátnu informovanosť, transparentnosť a bezpečnosť finančného systému. Od subjektov poskytujúcich (digitálne) finančné služby, akými sú aj služby kryptoaktív⁵, sa vyžaduje vyššia miera obozretnosti vo vzťahu ku svojim klientom (KYC⁶) ako aj k vykonávaným transakciám (KYT⁷).

Finančný sektor je totiž vystavený rizikám, ktoré do veľkej miery spočívajú v legalizácii aktív (výnosov) nadobudnutých trestnou činnosťou (ďalej ako „ML“).⁸ Rôzne analýzy poukazujú na to, že aj keď sú jednotlivé transakcie kryptoaktív detegované ako nelegálne, tieto majú rokmi klesajúci podiel na všetkých prevodoch,

³ V prípade distribuovanej databázy transakcií (ďalej ako „DLT“) to neplatí *en bloc*, nakoľko distribuovaná sieť je v dôsledku zdieľania údajov medzi všetkými účastníkmi siete pomalá a nákladná. K tomu pozri napr.: PUTERA, M.: Kryptoaktíva, ich zdaňovanie a exekúcia. Bratislava: C.H.Beck SK, 2024. s. 11.

⁴ 1. ČUNDERLÍK, Lubomír a kol.: Právo finančného trhu. 1. vyd. Bratislava: Wolters Kluwer, 2017. s. 15.

⁵ Pod pojmom „služba kryptoaktív“ sa rozumejú služby tak, ako sú uvedené v čl. 3 ods. 16 nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937.

⁶ KYC z anglického *know your client*.

⁷ KYT z anglického *know your transaction*.

⁸ ELAD, Barry – KINDER, Kathleen. Cryptocurrency Anti Money Laundering (AML) Statistics 2025: Revealing Illicit Flows & Enforcement. CoinLaw, 2025. Dostupné [online] na: <<https://coinlaw.io/cryptocurrency-anti-money-laundering-statistics/>> [cit. 08.09.2025]

práve aj vďaka regulačným a technickým protiopatreniam.⁹ To však neznamená, že je riziko ML nízke, práve naopak.¹⁰ Preto v záujme mitigácie rizík s tým súvisiacich bol na úrovni Európskej únie (ďalej ako „EÚ“) v období rokov 2022 – 2024 prijatý balík opatrení vzťahujúcich sa aj na kryptoaktíva vrátane pravidiel ich prevodu.¹¹ Ide o sériu legislatívnych aktov, *in concreto* nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1113 z 31. mája 2023 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849 (ďalej ako „TFR“), nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937, ako aj doplnenia v predpisoch zameraných proti praniu špinavých peňazí¹² (ďalej ako „AML predpisy“) a ďalších, zohľadňujúc odporúčania medzinárodnej organizácie FATF, ktoré majú normatívny charakter.¹³ Cieľom jednotlivých pravidiel, ktoré vyplývajú z uvedených predpisov je zabezpečiť, aby subjekty poskytujúce služby kryptoaktív (ďalej ako „CASP“) identifikovali a zhromažďovali údaje o pôvode a celi tých finančných operácií, ktoré sa svojim objemom alebo kvalitou vymykajú legitímnym rámcom.¹⁴

⁹ ELMOUGY, Youssef – LING, Liu. Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23). Association for Computing Machinery, New York, NY, USA, 2023, str. 3979–3990. Dostupné [online] na: <<https://doi.org/10.1145/3580305.3599803>> [cit. 08.09.2025] alebo 6. ROSENQUIST, Hampus – HASSEQUIST, David – ARLITT, Martin – CARLSSON, Niklas: On the Dark Side of the Coin: Characterizing Bitcoin Use for Illicit Activities. In: Richter, P., Bajpai, V., Carisimo, E. (eds) Passive and Active Measurement. PAM 2024. Lecture Notes in Computer Science, vol 14538. Springer, Cham. s. 37 – 66. Dostupné [online] na: <https://doi.org/10.1007/978-3-031-56252-5_3> [cit. 06.09.2025]

¹⁰ K tomu pozri: FSJ. Správa z III. kola národného hodnotenia rizík legalizácie výnosu z trestnej činnosti a financovania terorizmu. Legislatívny proces č. LP/2025/403. Dostupné [online] na: <<https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/403>> [cit. 09.09.2025]

¹¹ K tomu bližšie pozri: European Commission. Digital finance package. Dostupné [online] na: <https://finance.ec.europa.eu/publications/digital-finance-package_en> [cit. 08.09.2025]

¹² V súčasnosti najmä smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu; smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a ich národná implementácia, zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

¹³ Ide najmä o odporúčanie č. 16, označené ako „Payment transparency“. Bližšie pozri: FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris. 2012-2025.

¹⁴ K tomu bližšie pozri napr.: Chainalysis. The 2025 Crypto Crime Report. Dostupné [online] na: <<https://go.chainalysis.com/2025-Crypto-Crime-Report.html>> [cit. 12.09.2025]

Tento článok má za cieľ na základe analýzy a komparácie príslušných prameňov stanoviť rozsah informačných povinností CASP, kvantitu a kvalitu údajov, ktoré CASP zhromažďujú na účely boja proti ML a vyhodnotiť, či riziká spojené s ich zhromažďovaním, teda záujem na ochrane pred ML nepresahuje oprávnený zásah do integrity klientov, a teda či klientov nevystavuje neakceptovateľnému riziku.¹⁵

KYT – sledovanie transakčného toku na základe „*Travel Rule*“

Cezhraničný platobný styk korešponduje s charakterom kryptoaktív. Ich globálna povaha je výzvou pre bezpečnosť a ochranu cezhraničných platieb, najmä ak tieto pochádzajú z nelegálnych aktivít, alebo ak sa nimi má financovať taká aktivita. Identifikácia podozrivej transakcie bez ďalšieho nepostačuje pre príslušné orgány presadzovania práva, ktorí majú za úlohu zabrániť nelegálnemu finančnému toku. Tieto výzvy si uvedomujú aj regulačné authority, ktorí sa snažia prispôbovať obmedzenia adekvátne súčasným trendom.

V júni 2025 aj FATF revidovala medzinárodné štandardy pre transparentnosť platieb zakotvených vo svojom odporúčaní č. 16.¹⁶ Toto odporúčanie predstavuje tzv. princíp *Travel Rule*, z ktorého vyplýva požiadavka na zodpovedný subjekt identifikovať svojho klienta a konečného užívateľa výhod, vykonávať nepretržité monitorovanie transakcií, overovať obsah poskytnutých údajov o pôvodcovi a príjemcovi kryptoaktív a vo vymedzených prípadoch zmraziť alebo zakázať vykonanie určitých transakcií.¹⁷ Tieto zmeny vzhľadom na kryptoaktíva zahŕňajú (i) určenie zodpovednej osoby v rámci platobného reťazca (toho, kto získal a mal zabezpečiť nemennosť informácií v platobných správach, t. j. najčastejšie tzv. povinná osoba podľa AML predpisov¹⁸); (ii) určenie *thresholdu* pre cezhraničné platby, nad ktorú sa majú žiadať príslušné informácie (v súčasnosti ide o sumu nad 1.000 Eur); (iii) požiadavky na

¹⁵ K tomu pozri aj: NBU. Metodika analýzy rizík kybernetickej bezpečnosti. Dostupné [online] na: <<https://www.nbu.gov.sk/riadenie-rizik/>> [cit. 12.09.2025]

¹⁶ FATF. FATF updates Standards on Recommendation 16 on Payment Transparency. 2025. Dostupné [online] na: <<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html>> [cit. 09.09.2025]

¹⁷ DAUDRIKH, Yana: Travel rule v kontexte finančných inovácií: povinnosti týkajúce sa údajov o pôvodcoch a príjemcoch prevodov kryptoaktív a ich vplyv na reguláciu finančného trhu. In: Finančné inovácie – determinant súčasnej a anticipovanej regulácie na finančnom trhu (výzvy a riziká). 1. časť. / Ľubomír Čunderlík, Maroš Katkovčín (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s. 113.

¹⁸ Povinné osoby sa považujú za subjekty v prvej línii boja proti ML. K tomu bližšie pozri: STIERANKA, Jozef a kol.: Legalizácia príjmov z trestnej činnosti a financovanie terorizmu. Bratislava: Wolters Kluwer, 2018. s. 118.

zavedenie automatizovaných technológií na ochranu pred podvodmi a chybovosťou (napr. overovanie bankových informácií príjemcov platby).¹⁹

Podľa zistení FATF, implementácia princípu *Travel Rule* v jednotlivých jurisdikciách postupne rastie.²⁰ Na úrovni EÚ bolo v roku 2023 prijaté zmienené TFR, s cieľom umožniť efektívne trasovanie prevodov kryptoaktív pre zmiernenie rizík súvisiacich s ich (pseudo)anonymitou.²¹ Ide významný nástroj na predchádzanie praniu špinavých peňazí a financovania terorizmu, ich odhaľovanie, vyšetrovanie a prijímanie reštriktívnych opatrení.²²

Okrem usmernenia Európskej bankovej autority č. EBA/GL/2024/11, ktoré môže byť užitočným vodítkom pre zainteresované subjekty, v júni 2025 vydala FATF *Best Practises* k implementácii *Travel Rule* pre oblasť kryptoaktív.²³ Je zjavné, že žiadny z uvedených neposkytuje technické riešenia pre zavedenie efektívnych mechanizmov, ktoré by reflektovali požiadavky regulátora, avšak FATF vyzýva národné authority, aby po vzore iných krajín napr. stanovili komplexné usmernenia a odporúčania pre CASP v súvislosti s implementáciou *Travel Rule*, aby zväžili zavedenie testovacieho *sandboxu* alebo aby stanovili, že podmienkou pre udelenie licencie žiadateľovi – budúcemu CASP je preukázanie potrebnej technickej a operatívnej spôsobilosti na plnenie povinností vyplývajúcich z *Travel Rule* ešte pred začatím svojej činnosti.²⁴

TFR v zásade operuje s dvoma kategóriami subjektov v oblasti kryptoaktív, ktorí podliehajú princípu *Travel Rule*, a to s CASP a sprostredkovateľom služieb kryptoaktív²⁵ (ďalej ako „ICASP“) (ďalej spolu aj ako „povinné subjekty“). Pritom pri

¹⁹ FATF. FATF updates Standards on Recommendation 16 on Payment Transparency. 2025. Dostupné [online] na: <<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html>> [cit. 09.09.2025]

²⁰ V prieskume za rok 2025 uviedlo 73 % krajín (85 zo 117 jurisdikcií, s výnimkou tých, ktoré výslovne zakazujú alebo plánujú zakázať činnosť VASP), že prijali legislatívu implementujúcu *Travel Rule*. Ďalších 14 jurisdikcií uviedlo, že sú v procese implementácie tohto pravidla, v porovnaní s 15 zo 80 jurisdikcií v roku 2024. Bližšie pozri: FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris. 2025. Dostupné [online] na: <<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>> [cit. 10.09.2025]

²¹ Recitál 30 TFR.

²² Recitál 16 TFR.

²³ FATF. Best Practices on Travel Rule Supervision, FATF, Paris. 2025. Dostupné [online] na: <<https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule>> [cit. 10.09.2025]

²⁴ Ibid.

²⁵ Podľa čl. 3 ods. 16 TFR „sprostredkovateľ služieb kryptoaktív je poskytovateľ služieb kryptoaktív, ktorý nie je poskytovateľom služieb kryptoaktív pôvodcu ani prijímateľa a ktorý prijíma a odosiela prevod

prevodoch kryptoaktív (i) medzi osobami bez zapojenia CASP (ďalej ako „samohostované adresy“); (ii) medzi CASP konajúcimi vo vlastnom mene; pri (iii) nezameniteľných kryptoaktívach (NFT); a pri (iv) osobách poskytujúcich výhradne služby posielania správ alebo doplnkovú infraštruktúru umožňujúcu fungovanie CASP sa toto nariadenie neuplatní.^{26 27}

Z uvedených výnimiek je potom zaujímavý vzťah CASP a osoby so samohostovanou adresou. V prípade prevodu kryptoaktív na samohostovanú adresu, ktorá presahuje daný *threshold* alebo sa vyznačuje inými rizikovými faktormi²⁸, CASP pôvodcu získava a uchováva požadované údaje od svojho klienta a zabezpečuje, aby takýto prevod mohol byť individuálne posúdený, a to, či túto adresu vlastní alebo kontroluje práve pôvodca.²⁹

V konkrétnom prípade však vzniká otázka, či politika zavedená povinnou osobou na zistenie údajov prijímateľa takejto platby plní svoj účel, a či nejde len skôr o formálne splnenie povinnosti. CASP totiž aj keď má povinnosť získavať a uchovávať vybrané údaje o pôvodcovi alebo prijímateľovi, ktorý je reprezentovaný samohostovanou adresou, a tiež údaje individuálne identifikovať a overovať, nedisponuje praktickými možnosťami overenia informácií o pôvodcovi alebo prijímateľovi, keďže u osoby so samohostovanou adresou nie je možné vykonať KYC, nakoľko údaje v DLT nepostačujú na identifikovanie samohostovanej adresy pôvodcu alebo prijímateľa. Takéto údaje je možné získať zložitým trasovaním kryptoaktív³⁰ a napr. za predpokladu, že osoba na samohostovanú adresu získala kryptoaktíva prostredníctvom CASP, ktorá podlieha AML predpisom, a teda vykonala KYC vo vzťahu ku klientovi. Obdobne platí, že CASP musí prijať také opatrenia, aby dokázal posúdiť, či samohostovanú adresu pôvodcu alebo prijímateľa vlastní alebo kontroluje klient. CASP správnosť údajov overuje prostredníctvom spoľahlivého a nezávislého zdroja. Čo sa považuje za spoľahlivý a nezávislý zdroj však z materiálneho hľadiska jednoznačne nemožno určiť. Môže sa tak jednať o databázy identifikovaných samohostovaných adries spravodajských, policajných a justičných orgánov alebo súkromných spoločností zaoberajúcimi sa ušľachťovaním samohostovaných adries, resp. databázy zistených údajov CASP pri vykonávaní

kryptoaktív v mene poskytovateľa služieb kryptoaktív pôvodcu alebo prijímateľa alebo iného sprostredkovateľa služieb kryptoaktív“.

²⁶ NBS. Prezentácia ku TFR. Dostupné [online] na: <<https://nbs.sk/dohlad-nad-financnym-trhom/dohlad/kryptoaktiva/regulacia/>> [cit. 10.09.2025]

²⁷ Bližšie k jednotlivým výnimkám pozri čl. 2 TFR.

²⁸ Čl. 14 ods. 5 v spojení s recitálom 39 TFR.

²⁹ Ibid.

³⁰ K tomu bližšie pozri: ŠANTA, Ján – LIPTÁK, Andrej – ŠANTA, Ivo: Virtuálne meny, ich trasovanie a procesnoprávne aspekty. Trestní právo, 3/2024. Dostupné [online] na: <https://www.researchgate.net/publication/384861454_Virtualne_meny_ich_trasovanie_a_procesnopravne_aspekty_-_Trestni_pravo_032024_-_ISSN_2788-3787> [cit. 12.09.2025]

opatrení z AML predpisov, ktoré budú v tomto ponímaní medzi sebou zdieľané. CASP však v zmysle TFR nesmie žiadny prevod kryptoaktív vykonať bez splnenia uvedených opatrení. Pravdivosť overených údajov však dnes nemožno po materiálnej stránke uspokojivo zabezpečiť.³¹

Zdanlivá duplicita KYC

Regulované subjekty finančného trhu pravidelne vykonávajú tzv. starostlivosť vo vzťahu ku klientom, a to či už základnú, zvýšenú alebo zjednodušenú, vzhľadom na rizikové faktory klienta.³² Politika a samotné mechanizmy KYC sú nástrojom včasného detegovania potenciálnych legalizačných zámerov, a preto je opodstatnené, aby požiadavkám KYC podliehali i subjekty v oblasti kryptoaktív. Na úrovni EÚ patria tieto subjekty medzi povinné osoby od účinnosti smernice Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu.³³

Starostlivosť vo vzťahu ku klientovi zahŕňa okrem iného identifikáciu a overenie totožnosti klienta a konečného užívateľa výhod, pričom všetky dotknuté údaje a písomné doklady získané počas týchto procesov je povinná osoba povinná uchovávať v zákonom stanovenej lehote.³⁴ Tieto údaje predstavujú v zásade totožné údaje, ktoré má CASP získavať v rámci TFR za účelom transparentnosti transakcie.

TFR v recitáli 31 pamätá na administratívne zaťaženie regulovaných subjektov a pre konzistentnosť stanovených postupov nevyžaduje od povinných osôb, aby duplicitne zhromažďovali dotknuté údaje, nakoľko ich už vo svojich databázach uchovávajú a spracúvajú. Absenciu tejto povinnosti preto možno hodnotiť vysoko pozitívne.

³¹ LIPTÁK, Andrej: Cryptoasset Service Providers and DEFI Systems Identification within the scope of Examination of Distributed Ledger of Cryptoassets. Dostupné [online] na: <https://www.researchgate.net/publication/393631742_Cryptoasset_Service_Providers_and_DEFI_Systems_Identification_within_the_scope_of_Examination_of_Distributed_Ledger_of_Cryptoassets> [cit. 12.09.2025]

³² Podľa § 13 slovenského zákona o AML povinná osoba môže i prevziať plnenie (údaje) tretími stranami.

³³ Je na mieste spomenúť, že EÚ prijala prvé nariadenie o AML, a to nariadenie Európskeho Parlamentu a Rady (EÚ) 2024/1624 z 31. mája 2024 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorá sa v zásade uplatňuje od 10. júla 2027, a ktorá rovnako radí medzi tzv. povinné osoby CASP, ktoré terminologicky spadajú už pod finančné inštitúcie. Dostupné [online] na: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=OJ:L_202401624>

³⁴ Podľa slovenského zákona o AML ide o 5 rokov, pričom sa táto lehota môže predĺžiť, avšak nie viac, ako 5 rokov. K tomu pozri: ustanovenie § 19 zákona o AML.

Rozsah údajov sprevádzajúcich prevody kryptoaktív

Informačné povinnosti, na základe ktorých povinné subjekty získavajú, držia a zabezpečujú prenos požadovaných údajov je možné vymedziť nasledovne:

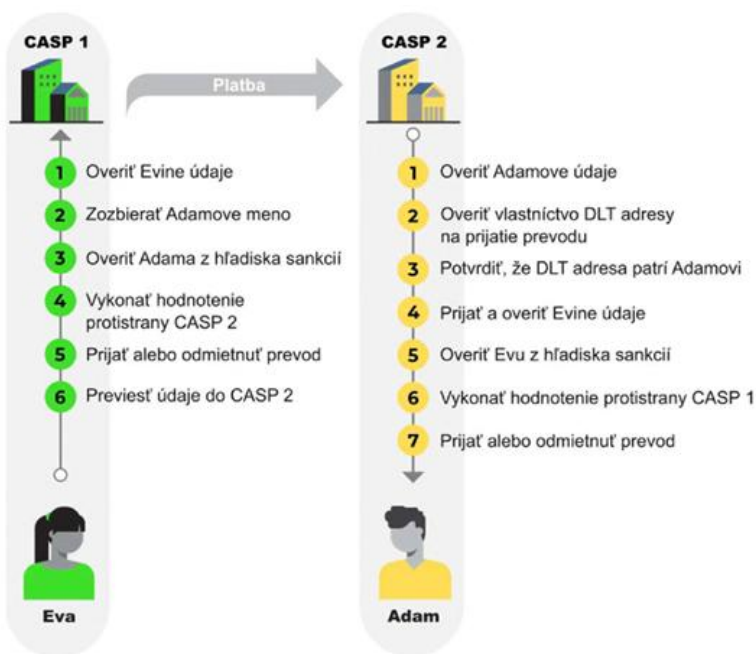
Údaje pôvodcu (odosielateľa) kryptoaktív, a to

- (i) Meno a priezvisko fyzickej osoby/ názov právnickej osoby;
- (ii) DLT adresa pôvodcu (verejná adresa);
- (iii) Číslo účtu kryptoaktív pôvodcu;
- (iv) Adresa
 - miesto obvyklého pobytu platiteľa alebo pôvodcu alebo, ak nie je určená adresa bydliska, poštová adresa, na ktorej možno fyzickú osobu zastihnúť,
 - registrované alebo úradné sídlo platiteľa alebo pôvodcu v prípade právnickej osoby;
- (v) Číslo osobného dokladu;
- (vi) Identifikačné číslo klienta;
- (vii) LEI alebo jeho rovnocenný identifikátor.

Na opačnej strane údaje prijímateľa kryptoaktív, a to

- (i) Meno a priezvisko fyzickej osoby/ názov právnickej osoby;
- (ii) DLT adresa prijímateľa (verejná adresa);
- (iii) Číslo účtu kryptoaktív prijímateľa;
- (iv) LEI alebo jeho rovnocenný identifikátor.³⁵

³⁵ Bližšie pozri čl. 14 a nasl. TFR, pričom tieto boli špecifikované v EBA: Guidelines on information requirements in relation to transfers of funds and certain crypto assets transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines). EBA/GL/2024/11, str. 11 a nasl. Dostupné [online] na: <<https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>> [cit. 10.09.2025]



Obrázok č. 1
Informačné povinnosti CASP podľa TFR
 Zdroj: NBS³⁶

Zároveň je potrebné dodať, že v prípade, ak chýba niektorý z uvedených údajov o pôvodcovi alebo prijímateľovi transakcie podľa čl. 16 a nasl. TFR, povinné subjekty po zohľadnení vyhodnotenej miery rizika podľa AML predpisov si bez zbytočného odkladu opätovne vyžiadajú údaje o pôvodcovi a prijímateľovi pred sprístupnením kryptoaktív prijímateľovi alebo takúto transakciu zamietnu alebo ju vrátia. Ak sa tak nestane, povinné subjekty sú *ultima ratio* oprávnené s partnerským CASP alebo ICASP obmedziť či ukončiť svoj obchodný vzťah.³⁷

Zraniteľnosť osôb v dôsledku zhromažďovania údajov

Ako uvádza i Daudrikh, existujú obavy z nedostatočného zohľadňovania základného práva na súkromie, digitálnej bezpečnosti občanov EÚ, keďže sú títo vystavení najmä zvýšenému riziku kybernetických hrozieb.³⁸

³⁶ NBS. Prezentácia ku TFR. Dostupné [online] na: <<https://nbs.sk/dohlad-nad-financnym-trhom/dohlad/kryptoaktiva/regulacia/>> [cit. 10.09.2025]

³⁷ K tomu bližšie pozri: čl. 17 a 21 TRF.

³⁸ DAUDRIKH, Yana: Travel rule v kontexte finančných inovácií: povinnosti týkajúce sa údajov o pôvodcoch a príjemcoch prevodov kryptoaktív a ich vplyv na reguláciu finančného trhu. In: Finančné inovácie – determinant súčasnej a anticipovanej regulácie na finančnom trhu (výzvy a riziká). 1. časť. /

Reakciou na vzrastajúce kybernetické útoky malo byť aj nariadenie DORA³⁹, ktorá má za cieľ posilňovať bezpečnosť finančného trhu, aby sa v čo najväčšej miere zabránilo neoprávnenému úniku (aj tých) dát, ktoré sú v kontexte kryptoaktív CASP povinní zhromažďovať.⁴⁰

Všeobecne je ochrana osobných údajov pretavená do nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej ako „GDPR“), ktoré bolo navrhnuté tak, aby sa zhromažďovanie obmedzilo na rozsah, ktorý je nevyhnutný na svoj účel.⁴¹ V súlade s GDPR aj TFR zakazuje ďalšie spracúvanie osobných údajov na obchodné účely a špecifikuje účel takého spracovania. Týmto účelom je boj proti praniu špinavých peňazí a financovaniu terorizmu, ktoré uznávajú všetky členské štáty ako vec dôležitá verejnému záujmu,⁴² čo možno považovať za absolútne legitímne. Dokonca pri postupe podľa TFR je CASP povinný v plnej miere rešpektovať znenie GDPR a napr. pri prevodoch kryptoaktív má CASP pôvodcu posúdiť schopnosť CASP prijímateľa registrovaného mimo EÚ prijímať a uchovávať osobné údaje v súlade s ustanoveniami GDPR upravujúcimi prenos osobných údajov do tretích krajín.⁴³ Predmetné požiadavky sú zodpovednosťou každého povinného subjektu aj napriek tomu, že príslušné predpisy opäť neponúkajú technické riešenia.

Záver

Informačné povinnosti vzťahujúce sa na subjekty poskytujúce finančné služby v oblasti kryptoaktív, sú nastavené pomerne striktné. Tieto subjekty sú povinné podľa TFR zhromažďovať údaje a zabezpečiť, aby sprevádzali konkrétnu transakciu kryptoaktív, spadajúcu pod regulačný rámec. Na opačnej strane každá osoba (klient) poskytuje svoje osobné údaje v rozsahu, v akej povinný, regulovaný subjekt od nej požaduje.

Ľubomír Čunderlík, Maroš Katkovčín (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. s. 118.

³⁹ Nariadenie Európskeho Parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011

⁴⁰ Na ilustráciu takého útoku pozri napr.: State Data Protection Inspectorate. The State Data Protection Inspectorate has Initiated an Investigation Regarding Personal Data Breach in “Revolut” Dostupné [online] na: <<https://vdai.lrv.lt/en/news/the-state-data-protection-inspectorate-has-initiated-an-investigation-regarding-personal-data-breach-in-revolut/>> [Navštívené dňa 11.09.2025]

⁴¹ Ide o zásadu minimalizácie údajov podľa čl. 5 ods. 1 písm. c) GDPR. K tomu bližšie pozri napr.: HANOUSEK, Daniela: Blockchain z pohľadu ochrany osobných údajov. Bratislava: C. H. Beck, 2022. s. 71.

⁴² Recitál 19 TFR.

⁴³ V súlade s čl. 44 a nasl. GDPR.

Pozitívne možno hodnotiť konzistentnosť opatrení v predpisoch AML a TFR, čím sú povinné subjekty odbremenené od ďalšej administratívnej záťaže, vzhľadom na totožný rozsah informácií, ktoré majú zhromažďovať za účelom KYC a *Travel Rule*. Ide o postupy, ktoré síce často zťažujú obe strany, no mali by byť opodstatnené vzhľadom najmä na dôslednú reakciu orgánov presadzovania práva v prípade podozrenia alebo naplnenia podozrenia z trestnej činnosti. V tomto smere sa boj proti ML presúva na CASP a ich schopnosť implementovať normy *Travel Rule*. Samotný koncept regulácie prostredníctvom TFR posilňuje transparentnosť finančných tokov v oblasti kryptoaktív a prispieva k ochrane pred ML a financovaním terorizmu.

Ďalej treba zdôrazniť, že DLT prináša nový systém prevodu aktív, pri ktorom už nie je potrebná ingerencia sprostredkovateľa (CASP). Doposiaľ, tradičné finančné subjekty uskutočňovali prevody aktív výlučne medzi sebou, na účet klienta a vykonávali KYC a KYT v zmysle AML predpisov. Tieto informácie si potom zdieľali medzi sebou, čo predstavovalo dostatočný systém monitorovania transakcií a identifikácie pôvodcov a prijímateľov. Dnes, pri technologickom pokroku, teda pri využívaní DLT, dokáže tento klient vykonať prevod aj „samohostovane“, teda absolútne decentralizovane, bez potreby sprostredkovateľa, čo vylučuje AML záruky, ktoré by inak zabezpečoval tradičný finančný subjekt. V kontexte boja proti ML prináša samotná identifikácia samohostovanej entity veľké výzvy, rovnako potom overovanie už identifikovaných dát ostáva viac formálne ako materiálne. Pri prevode aktív medzi CASP a samohostovanou adresou v DLT, kedy podľa princípu *Travel Rule* má CASP povinnosť overiť príjemcu resp. odosielateľa, takúto informáciu získava (primárne) od svojho klienta. Tieto informácie následne overuje prostredníctvom tretieho (externého) subjektu alebo vlastnou činnosťou za využitia metód ako je skúmanie DLT alebo OSINT, ktorých relevancia však nie je zaručená. Informácie poskytnuté klientom teda nie je možné fakticky hodnoverne overiť, aj keď je podmienka ich overenia formálne naplnená.

Komparáciou noriem príslušných právnych predpisov bolo zistené, že existuje odôvodnený zámer zabezpečovať informácie, po ktorých je možné v prípade naplnenia podozrení z ML siahnuť. Preto by takýto zber údajov mal byť akceptovateľný aj napriek zásahu do integrity klientov. Na druhej strane, akákoľvek agregácia dát predstavuje riziko odcudzenia a ich využite na iné nelegálne aktivity. K tomu môže dôjsť i za predpokladu, že povinné osoby len formálne plnia povinnosti a nepodložia ich efektívnymi technickými a organizačnými opatreniami vyplývajúcimi najmä z DORA a GDPR. Treba ale uznať, že DLT nie je navrhnutý ako systém viazaný na jurisdikciu. Preto niektoré opatrenia, ako napríklad práve plnenie informačných povinností CASP, budú prakticky existovať (aspoň dnes) len formálne. Na záver možno konštatovať, že finančný sektor je skutočne postavený na robustnosti a resiliencii, avšak často bez štandardizovaných technických riešení,

ktoré by účinne sprevádzali reguláciu. Preto nie len regulačné výzvy, o to viac technologické môžu byť paralyzujúce pre subjekty finančného trhu.

Zoznam použitej literatúry

1. ČUNDERLÍK, Ľubomír a kol.: Právo finančného trhu. 1. vyd. Bratislava: Wolters Kluwer, 2017. 260 s. ISBN 978-80-8168-753-2.
2. DAUDRIKH, Yana: Travel rule v kontexte finančných inovácií: povinnosti týkajúce sa údajov o pôvodcoch a príjemcoch prevodov kryptoaktív a ich vplyv na reguláciu finančného trhu. In: Finančné inovácie – determinant súčasnej a anticipovanej regulácie na finančnom trhu (výzvy a riziká). 1. časť. / Ľubomír Čunderlík, Maroš Katkovčín (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024. 135 s. ISBN 978-80-7160-736-6.
3. HANOUSEK, Daniela: Blockchain z pohľadu ochrany osobných údajov. Bratislava: C. H. Beck, 2022. 122 s. ISBN 978-80-8232-023-0
4. ELAD, Barry – KINDER, Kathleen. Cryptocurrency Anti Money Laundering (AML) Statistics 2025: Revealing Illicit Flows & Enforcement. CoinLaw, 2025. Dostupné [online] na: <<https://coinlaw.io/cryptocurrency-anti-money-laundering-statistics/>> [cit. 08.09.2025]
5. ELMOUGY, Youssef – LING, Liu. Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23). Association for Computing Machinery, New York, NY, USA, 2023, str. 3979–3990. Dostupné [online] na: <https://doi.org/10.1145/3580305.3599803> [cit. 08.09.2025]
6. LIPTÁK, Andrej: Cryptoasset Service Providers and DEFI Systems Identification within the scope of Examination of Distributed Ledger of Cryptoassets. Dostupné [online] na: <https://www.researchgate.net/publication/393631742_Cryptoasset_Service_Providers_and_DEFI_Systems_Identification_within_the_scope_of_Examination_of_Distributed_Ledger_of_Cryptoassets> [cit. 12.09.2025]
7. PUTERA, Marko: Kryptoaktíva, ich zdaňovanie a exekúcia. Bratislava: C.H.Beck SK, 2024. 176 s. ISBN: 978-80-8232-057-5.
8. ROSENQUIST, Hampus – HASSEQUIST, David – ARLITT, Martin – CARLSSON, Niklas: On the Dark Side of the Coin: Characterizing Bitcoin Use for Illicit Activities. In: Richter, P., Bajpai, V., Carisimo, E. (eds) Passive and Active Measurement. PAM 2024. Lecture Notes in Computer Science, vol 14538. Springer, Cham. s. 37 – 66. Dostupné [online] na: <https://doi.org/10.1007/978-3-031-56252-5_3> [cit. 06.09.2025]

9. STIERANKA, Jozef a kol.: Legalizácia príjmov z trestnej činnosti a financovanie terorizmu. Bratislava: Wolters Kluwer, 2018. 196 s. ISBN: 978-80-8168-912-3.
10. ŠANTA, Ján – LIPTÁK, Andrej – ŠANTA, Ivo: Virtuálne meny, ich trasovanie a procesnoprávne aspekty. In: Trestní právo, 3/2024. Wolters Kluwer ČR, 2024. ISSN 2788-3787.

Internetové zdroje

1. EBA: Guidelines on information requirements in relation to transfers of funds and certain crypto assets transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines). EBA/GL/2024/11, str. 11 a nasl. Dostupné [online] na: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers> [cit. 10.09.2025]
2. European Commission. Digital finance package. Dostupné [online] na: https://finance.ec.europa.eu/publications/digital-finance-package_en [cit. 08.09.2025]
3. FATF. Best Practices on Travel Rule Supervision, FATF, Paris. 2025. Dostupné [online] na: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule> [cit. 10.09.2025]
4. FATF. FATF updates Standards on Recommendation 16 on Payment Transparency. 2025. Dostupné [online] na: <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html> [cit. 09.09.2025]
5. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris. 2012-2025.
6. FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris. 2025. Dostupné [online] na: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html> [cit. 10.09.2025]
7. FSJ. Správa z III. kola národného hodnotenia rizík legalizácie výnosu z trestnej činnosti a financovania terorizmu. Legislatívny proces č. LP/2025/403. Dostupné [online] na: <https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/403> [cit. 09.09.2025]
8. NBS. Prezentácia ku TFR. Dostupné [online] na: <https://nbs.sk/dohlad-nad-financnym-trhom/dohlad/kryptoaktiva/regulacia/> [cit. 10.09.2025]

Právne predpisy

1. Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES
2. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011
3. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1113 z 31. mája 2023 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849
4. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937
5. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2024/1624 z 31. mája 2024 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu
6. Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu
7. Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a ich národná implementácia
8. Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov

Kontaktné údaje

Mgr. Klaudia Keratová

keratova6@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

DIGITALIZÁCIA V PROSTREDÍ CROWDFUNDINGU

DIGITALIZATION IN THE CROWDFUNDING ENVIRONMENT

Matej Krkoška¹

Abstrakt: Digitalizácia a crowdfunding inú spolu ruka v ruka, crowdfunding ako ho poznáme v súčasnosti vznikol v dôsledku digitalizácie ako jeden z mnohých jej produktov digitalizácie. Crowdfunding je tak fenoménom spojených s digitalizáciou. Umožňuje široký prístup k financovaniu, ktorý sa stal dostupným pre širšie skupiny subjektov na základe tzv. princípu zdola nahor (*bottom-up principle*) s využitím digitálnych nástrojov. Zároveň aktuálna regulácia pre crowdfunding v európskom prostredí, ktorým je Európske nariadenie o poskytovateľoch služieb hromadného financovania pre podnikanie a na neho nadväzujúce právne predpisy, zaviedla reguláciu pre crowdfunding, ktorá v sebe zahŕňa povinnosť vykonávať crowdfunding prostredníctvom digitálnej platformy a aj požiadavky na technické zabezpečenie pre prevádzkovateľov platforiem hromadného financovania. Technické zabezpečenie prevádzkovateľa príslušnej platformy musí zabezpečovať ochranu pred rizikami, ktoré sa vyskytujú v digitálnom prostredí, osobitne zabezpečiť ochranu údajov a transakcií klientov, ale aj odolnosť platformy hromadného financovania. Crowdfunding zároveň zostáva digitálnym fenoménom, nakoľko je možné ho vykonávať výhradne elektronicky digitálnou formou. Je to produkt digitalizácie, ktorý zostáva umiestnený len v digitálnom prostredí.

Kľúčové slová: crowdfunding, digitalizácia, online platforma, technické zabezpečenie

Abstract: Digitalization and crowdfunding go hand in hand, crowdfunding as we know it today emerged as a result of digitization as one of its many products of digitization. Crowdfunding is thus a phenomenon associated with digitization. It enables broad access to financing, which has become available to wider groups of entities based on the so-called bottom-up principle using digital tools. At the same time, the current regulation for crowdfunding in the European environment, which is the European Regulation on Crowdfunding Service Providers for business and related legal regulations, has introduced a

¹ Externý doktorand Právnická fakulta Univerzity Komenského

regulation for crowdfunding, which also includes the obligation to conduct crowdfunding through a digital platform as well as the requirements for technical capability for the operators of crowdfunding platforms. The technical measures of the operator of the applicable platform must ensure the protection against risks that occur in the digital environment, in particular ensuring the protection of client data and transactions, as well as the resilience of the crowdfunding platform. Crowdfunding also remains a digital phenomenon, since it can be carried out exclusively electronically in digital form. It is a product of digitization, which remains located only in the digital environment.

Key words: crowdfunding, digitalization, online platform, technical capability

Úvod

Digitalizácia je fenomén, ktorý prichádza od začiatku 90-tych rokov s masívnym nástupom internetu a výpočtovej techniky. V rámci digitalizácie sa rôzne spoločenské vzťahy, ktoré existovali vo fyzickom priestore dostali do digitálneho priestoru. Ide o ekonomické, kultúrne, mediálne, ale aj ďalšie iné vzťahy, ktoré začali fungovať digitálne. Rovnako, popri spoločenských vzťahoch existujúcich aj pred nástupom digitalizácie, prepojenie medzi širokou verejnosťou prostredníctvom digitálnych komunikačných prostriedkov umožnilo vznik úplne nových spoločenských fenoménov. Dobrým príkladom sú napríklad digitálne sociálne siete, ktoré vôbec pred nástupom digitalizácie neexistovali a dnes bežne existujú po celej planéte a vstupujú do našich životov z rôznych aspektov (zábava, práca, média, informovanie o veciach verejných či komunikácia v profesionálnej sfére). Crowdfunding je tiež jedným z fenoménov, ktoré vznikli vďaka alebo v dôsledku digitalizácie.

Vo všeobecnosti, digitálna infraštruktúra napomáha tzv. kolektívnej akcii alebo činom smerovaným zdola nahor (*bottom-up*) rýchlejšie ako v období pred digitalizáciou a taktiež aj činnosť trhov, ktoré by inak mali ťažkosti dosiahnuť na zákazníkov bez prítomnosti alebo významného zapojenia usmerňujúcich sprostredkovateľov (*gatekeeper intermediaries*²). To sa v plnom rozsahu vzťahuje aj na crowdfunding, ktorý jednoznačne predstavuje činnosť, ktorá vzniká zdola nahor, teda spontánne z iniciatívy subjektu zo širokej verejnosti. Typicky nevzniká pôsobením štátu, orgánov verejnej moci, či existujúcich inštitúcií alebo elít, ktoré inak typicky pôsobia ako usmerňovači toku informácií a prostriedkov medzi účastníkmi trhu. Absencia týchto usmerňujúcich sprostredkovateľov je významná pre

² Dalla Chiesa, C. (2020). From digitalization to crowdfunding platforms: fomenting the cultural commons. In E. Macri (Ed.), *Cultural Commons and Urban Dynamics* (pp. 173-186) https://doi.org/10.1007/978-3-030-54418-8_11

demokratickosť crowdfundingu ako finančnej inovácie existujúcej v technologickom prostredí. Crowdfunding ako taký totiž autor nepovažuje za technológiu, vo svojej podstate neprináša žiadny nový druh technológie, ale za inováciu využívajúcu technológiu.

Definičným znakom demokracie je hlasovanie a rovnako hlasujú aj účastníci trhu o projekte, ktorý sa uchádza o ich podporu cez crowdfunding. Digitalizácia umožnila aby tento fenomén existoval.

Digitálnym nástrojom, ktorý crowdfunding využíva je crowdfundingová platforma, teda digitálny – online priestor, v ktorom sa stretáva ponuka s dopytom ako ich vzájomný prepájač a ako tzv. dvojstranná platforma, ktorá umožňuje prepojenie medzi zákazníkom a dodávateľom obidvoma smermi³. Využitie tejto platformy zároveň umožňuje obchádzať usmerňovačov, ktorí na danom trhu pôsobia⁴.

Crowdfunding ako fenomén, ktorý je digitálny, demokratický a zároveň fenomén ktorý pôsobí spôsobom smerom zdola na hor, sa prejavuje aj ako fenomén, ktorý prispieva k digitálnej inklúzií. Digitálnou inklúziou sa myslí poskytnutie služieb finančných služieb častiam populácie, ktorým tieto chýbajú⁵. Medzi subjekty, ktoré sú vylúčené z dostatočného prístupu k finančným službám patria aj malé a stredné podniky, ktoré môžu mať prístup k finančným službám avšak tento nie je dostatočný. Je potrebné podotknúť, že takýmto subjektom v rámci obchodných modelov⁶, ktoré sú im k dispozícii, zahŕňajú popri investovaní do tzv. ekvity (nadobúdanie podiel) aj tzv. peer-to-peer lending, ktorý v sebe zahŕňa aj poskytovanie pôžičiek podnikateľom, financovanie realitných projektov alebo poskytovanie pôžičiek zabezpečených majetkom dlžníka. Všetky tieto činnosti predstavujú rôzne modely crowdfundingu. Každopádne, crowdfunding vznikol mimo regulovaného prostredia, spôsobom ako už bolo uvedené vyššie. Postupne však potom ako najprv okrajový fenomén prenikal do širšej komerčnej sféry, začal výkon crowdfundingu dochádzať do kontaktu s finančnou reguláciou. Tu je však potrebné odlíšiť tzv. nekomerčný crowdfunding, teda crowdfunding zameraný na podporu humanitárnych, sociálnych alebo umeleckých aktivít, bez cieľa priniesť komerčný prospech, resp. zisk osobám, ktoré poskytnú peňažné prostriedky v rámci crowdfundingu. Cieľom ďalšieho skúmania

³ Dalla Chiesa, C. (2020). From digitalization to crowdfunding platforms: fomenting the cultural commons. In E. Macri (Ed.), *Cultural Commons and Urban Dynamics* (pp. 173-186) https://doi.org/10.1007/978-3-030-54418-8_11

⁴ Dalla Chiesa (2020), ako vyššie

⁵ Md. Abdul Halim, Does crowdfunding contribute to digital financial inclusion?, *Research in Globalization*, Volume 9, 2024, ISSN 2590-051X, <https://doi.org/10.1016/j.resglo.2024.100238>, (<https://www.sciencedirect.com/science/article/pii/S2590051X24000479>)

⁶ European crowdfunding market report 2023, Rotem Shneor, Karsten Wenzlaff, Konstantin Boyko, Prince Baah-Pepurah, Ana Odorović, Olga Okhrimenko, University of Agder, School of Business, str. 24

crowdfundingu a digitalizácie je crowdfunding zameraný na podnikateľské účely – investičný crowdfunding.

Európska regulácia investičného crowdfundingu a digitalizácia

Na európskej úrovni je investičný crowdfunding upravený Nariadením Európskeho parlamentu a Rady (EÚ) 2020/1503 o európskych poskytovateľoch služieb hromadného financovania pre podnikanie z 7. októbra 2020 (*Regulation ... on European crowdfunding service providers for business*) (**ECSP Nariadenie**). ECSP Nariadenie zadefinovalo činnosť crowdfundingu investičného crowdfundingu, teda takého ktorý je vykonávaný s cieľom dosiahnuť zisk ako tzv. hromadné financovanie pre podnikanie.

ECSP Nariadenie (článok 2(1)(a)) zadefinovalo pojem „*služba hromadného financovania*“, ktorá znamená *spárovanie záujmov investorov a vlastníkov projektov o financovanie podnikania prostredníctvom využívania platformy hromadného financovania, ktorá zahŕňa ktorúkoľvek z týchto činností:*

- *uľahčenie poskytovania pôžičiek; a*
- *umiestňovanie finančných nástrojov bez pevného záväzku v súvislosti s prevoditeľnými cennými papiermi a prijatými nástrojmi na účely hromadného financovania, ktoré emitovali vlastníci projektov alebo účelovo vytvorený subjekt, a prijímanie a postúpenie pokynov klientov v súvislosti s uvedenými prevoditeľnými cennými papiermi a prijatými nástrojmi na účely hromadného financovania*⁷.

Pre účely tohto článku, je dôležité, že hromadné financovanie je definované ako činnosť vykonávanú prostredníctvom online platformy, ktorá je definovaná ako „*verejne prístupný internetový informačný systém, ktorý prevádzkuje alebo spravuje poskytovateľ služieb hromadného financovania*“.

Uľahčovanie poskytovania pôžičiek je vo špecifický koncept vytvorený pre poskytovanie služieb hromadného financovania. Vo svojej podstate ide o sprostredkovanie poskytnutie pôžičiek, keď sú tieto pôžičky poskytnuté hromadne, veľkou skupinou veriteľov voči jednému dlžníkovi. K tejto činnosti dochádza prostredníctvom digitálnej platformy. V prípade sprostredkovania poskytovania pôžičiek je potrebné spomenúť aj ďalšiu formu crowdfundingu, ktorá je prípustná mimo rámca ECSP Nariadenia, ktorou je peer-to-peer lending. V rámci tejto formy sú prostredníctvom online platformy poskytované pôžičky od fyzických osôb –

⁷ Text definície uvedený vyššie je zjednodušením, presné znenie je: *umiestňovanie finančných nástrojov bez pevného záväzku uvedené v bode 7 oddielu A prílohy I k smernici 2014/65/EÚ v súvislosti s prevoditeľnými cennými papiermi a prijatými nástrojmi na účely hromadného financovania, ktoré emitovali vlastníci projektov alebo účelovo vytvorený subjekt, a prijímanie a postúpenie pokynov klientov uvedené v bode 1 uvedeného oddielu v súvislosti s uvedenými prevoditeľnými cennými papiermi a prijatými nástrojmi na účely hromadného financovania.*

nepodnikateľom iným fyzickým osobám, resp. spotrebiteľom. Funkcia peer-to-peer lendingu spočíva v sprostredkovaní pôžičiek medzi dlžníkom a veriteľom, pričom k týmto obchodom dochádzalo na anonymnej báze a prevádzkovateľ príslušnej platformy vystupoval vo svojom mene a na účet veriteľov⁸. Aj táto forma crowdfundingu sa vykonáva prostredníctvom digitálnej platformy. Tzv. peer-to-peer lending je oblasť, ktorá je aj pokrytá pomerne dobre v slovenskej odbornej literatúre⁹, mám však za to, že menej ako oblasť crowdfundingu, v rámci ktorej dochádza k poskytovaniu investičných služieb týkajúcich sa cenných papierov. Sprostredkovanie pôžičiek ako také však je činnosťou, ktorá nemusí byť vykonávaná prostredníctvom online platformy aby ako také bolo možné ju vykonávať. Nemusí byť taká efektívna, nemusí zasahovať širšiu verejnosť a ani využívať moderné nástroje digitalizácie.

Rovnako aj investičné služby, ktoré predstavujú obsah hromadného financovania nemusia byť nevyhnutne vykonávané digitálnym spôsobom (aj keď to v súčasnosti je málo praktické). Tieto činnosti vznikli a boli vykonávané dávno pred nástupom digitalizácie. Digitalizácia nesporne napomohla rozvoju poskytovania investičných služieb, umožnila ich dostupnosť širokej verejnosti a nepochybne napomohla demokratizácii poskytovania a využívania investičných služieb. Zákon však nevyžaduje pre investičné služby aby boli poskytované určitou formou, teda prostredníctvom online platformy ako je to v prípade crowdfundingu. Treba dodať, že poskytovanie služieb hromadného financovania (pôžičiek a aj príslušných investičných služieb) je limitované vzhľadom na výšku investície pre jeden príslušný projekt na celkovo 5 000 000 EUR v priebehu 12 mesiacov¹⁰. Toto obmedzenie sa netýka digitalizácie, avšak je uvedené pre porozumenie kontextu v akých objemoch je možné vykonávať investičný crowdfunding v porovnaní s poskytovaním investičných služieb alebo pôžičiek (úverov) inak.

Kľúčovým pojmom pre crowdfunding vo vzťahu k digitalizácii je teda elektronická, resp. online platforma. Online platforma slúži na spárovanie potenciálnych investorov alebo veriteľov s podnikmi, ktoré sa snažia získať finančné prostriedky, alebo uľahčiť ich spárovanie. Táto platforma je otvorená verejnosti¹¹, ECSP

⁸ Čunderlík, L., Čunderlík, Čerbová, V., Daudrikh, Y., Heseková, S., Katkovčín, M., Mazúr, J. Inovatívne a atypické modely správy majetku na finančnom trhu a súvisiace otázky. Vedecká monografia. Praha: Leges, 2019. 183 s. ISBN 978-80-7502-405-3, str. 106-111

⁹ Heseková Bojmírová, S.-Katkovčín, M.: Právne vzťahy v rámci peer to peer lendingu; Justičná revue, 73, 2021, č. 11, s. 1312-1326

Simona Heseková, Andrea Szakács, Služby hromadného financovania založené na požíčianí a ich daňové aspekty, 2021

¹⁰ Článok 1(2)(C) ECSP Nariadenia

¹¹ ECSP Nariadenie, čl. 2(1)(d) "*platforma hromadného financovania*" je verejne prístupný internetový informačný systém, ktorý prevádzkuje alebo spravuje poskytovateľ služieb hromadného financovania; špecifikáciu platformy obsahuje recitál 1 ECSP Nariadenia.

Nariadenie vyžaduje dokonca aby táto platforma bola prístupná verejnosti na nediskriminačnom základe. Túto online platformu môžeme z funkčného hľadiska zadefinovať ako digitálny systém prístupný online prostredníctvom internetu, ktorý na jednej strane slúži na propagáciu cieľov pre crowdfundingové investovanie, tzv. projekty hromadného financovania a na druhej strane slúži na prepojenie potenciálnych investorov a investorov s daným investičným projektom. Toto prepojenie v sebe zahŕňa aj identifikáciu a verifikáciu investora, informovanie o investícií o jej rizikách a ich vyhodnotenie, poskytnutie dokumentov spojených s investíciou, ktoré po odsúhlasení zo strany investora sa stanú v určitom momente právne záväznými. Zároveň prostredníctvom tohto systému je investor vyzvaný aby poukázal peňažné prostriedky svojej investície na bankový účet špecifikovaný prevádzkovateľom tohto online systému – platformy.

Celý proces získania klienta a poskytnutia služby klientovi – investorovi prebieha digitálne. Samozrejme, v rámci praktického života sa môžu vyskytnúť situácie, ktoré si vyžadujú aj ne-digitálne riešenie, podstatným pre účely tohto článku je, že hromadné financovanie je vykonávané a musí byť vykonávané digitálne. Ponuka na investovanie a všetky informácie k nej sú poskytované prostredníctvom online platformy¹². Vstupný test vedomostí investora a tzv. simulácia schopnosti znášať stratu na strane investora sa musia uskutočniť prostredníctvom platformy¹³. Zároveň sú poskytovatelia služieb hromadného financovania povinný uchovávať najmenej 5 rokov všetky záznamy o ich službách a transakciách, rovnako aj zmluvy uzavreté s klientami, pričom klienti musia mať vždy okamžitý prístup k týmto záznamom o službách¹⁴.

Požiadavky na crowdfunding z hľadiska digitalizácie

Zákon na prevádzkovateľov crowdfundingových platforiem pre investičný crowdfunding, resp. poskytovanie služieb hromadného financovania stanovuje určité podmienky pre účely získania licencie na poskytovanie uvedených služieb v oblasti digitalizácie.

ECSP Nariadenie ako príslušný sektorový právny predpis pre oblasť investičného crowdfundingu spolu s tzv. Level 2, resp. delegovanými nariadeniami stanovuje pre získanie povolenia na poskytovanie služieb hromadného financovania aj podmienky v oblasti digitalizácie, teda podmienky, ktoré musí žiadateľ o povolenie splniť vzhľadom na technické zabezpečenie. Sú to Delegované Nariadenie Komisie (EÚ) 2022/2112 ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2020/1503, pokiaľ ide o regulačné technické predpisy, ktorými sa spresňujú

¹² Čl. 19(5) ECSP Nariadenia

¹³ Čl. 21 ECSP Nariadenia

¹⁴ Čl. 26 ECSP Nariadenia

požiadavky a podmienky žiadosti o udelenie povolenia na výkon činnosti poskytovateľa služieb hromadného financovania (ďalej **Nariadenie o podmienkach žiadosti**) a taktiež aj Delegované Nariadenie Komisie (EÚ) 2022/2116 ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2020/1503, pokiaľ ide o regulačné technické predpisy, ktorými sa spresňujú opatrenia a postupy týkajúce sa plánu na zabezpečenie kontinuity činností poskytovateľov služieb hromadného financovania (ďalej **Nariadenie o politike kontinuity**).

Nariadenie o podmienkach žiadosti vzhľadom na požiadavky z oblasti digitalizácie stanovuje¹⁵, že žiadateľ o povolenie je v rámci žiadosti povinný predložiť určité informácie o platforme hromadného povolenia. Sú to informácie ohľadom toho ako budú sprístupnené informácie vyžadované pre účely vykonávania hromadného financovania na základe čl. 19 ECSP Nariadenia¹⁶. Ako bolo uvedené vyššie, sú to tie informácie, ktoré musí poskytovateľ služieb hromadného financovania poskytovať pri výkone crowdfundingu prostredníctvom svojej online platformy, t.j. digitálnym spôsobom. Poskytovanie týchto informácií je súčasťou vykonávania crowdfundingu. Žiadateľ je ďalej povinný preukázať v rámci žiadosti o licenciu opatrenia, ktoré majú zabezpečiť, že platforma je prístupná verejne a nediskriminačným spôsobom¹⁷. Rovnako je žiadateľ o povolenie povinný preukázať aké má zavedené postupy pre spravodlivé a pohotové vykonávanie služieb hromadného financovania, aké má postupy na prijímanie a postúpenie pokynov klientov, spracúvanie pokynov klientov, ako aj mechanizmy na uľahčenie tokov informácií medzi tzv. vlastníkami projektov (projekty, ktoré sú financované prostredníctvom crowdfundingu) a investormi alebo medzi investormi. Z hľadiska digitalizácie je žiadateľ o povolenie povinný rovnako špecifikovať opis operačných rizík, a to rizík súvisiacich s IT infraštruktúrou a postupmi. Žiadateľ je povinný preukázať identifikáciu týchto rizík a aj opis postupov na účel riadenia týchto operačných rizík, t.j. na zabezpečenie spoľahlivosti IT systému, jeho zabezpečenia, integrity a ochrany súkromia¹⁸.

¹⁵ Oddiel 5 Nariadenia o podmienkach žiadosti

¹⁶ Opatrenia na sprístupnenie informácií uvedených v článku 19 nariadenia (EÚ) 2020/1503 na webovom sídle platformy hromadného financovania žiadateľa vrátane príslušných opatrení v oblasti IT

¹⁷ Opatrení zameraných na to, aby sa platforma hromadného financovania stala internetovým informačným systémom, ktorý je verejne dostupný a bez diskriminačného prístupu.

¹⁸ Opis identifikovaných zdrojov operačných rizík a opis postupov, systémov a kontrol prijatých žiadateľom na účely riadenia týchto operačných rizík (spoľahlivosť systému, zabezpečenie, integrita, súkromie atď.) vrátane:

- a) postupov na zabránenie prerušeniu operácií;
- b) zavedených záložných zariadení;
- c) opatrení, pokiaľ ide o záruky proti útokom hackerov.

Ďalšie požiadavky v oblasti digitalizácie, ktoré stanovuje regulácia vzťahujúca sa na poskytovateľa služieb hromadného financovania vyplývajú z Nariadenia o politike kontinuity. Cieľom tohto nariadenia je zabezpečiť aby poskytovateľ služieb hromadného financovania bol spôsobilý zabezpečiť fungovanie kritických služieb (vrátane služieb, ktoré sú predmetom outsourcingu. Rovnako požaduje od poskytovateľa služieb hromadného financovania aby mal pripravený plán na pokrytie situácií, ktoré môžu mať škodlivý vplyv na vykonávanie kritických služieb¹⁹. Podstatnou je povinnosť poskytovateľa služieb hromadného financovania byť pripravený, mať plán na riešenie situácií keď z nejakého dôvodu dôjde k prerušeniu poskytovania týchto služieb, typicky z dôvodu nejakej mimoriadnej udalosti, prírodnej katastrofy alebo nejakej technickej chyby. Tento plán musí obsahovať opatrenia aj pre prípad prerušenie poskytovania kritických služieb aj v oblasti informačných technológií a to ohľadom prístupu k informáciám klientov a prípadne k aktívam klientov²⁰ (to je viac relevantné ak by poskytovateľ služieb hromadného financovania mal oprávnenie aj na poskytovanie platobných služieb alebo úschovy cenných papierov, inak sú totiž aktíva klientov uložené u poskytovateľov iných služieb). To znamená, že poskytovateľ služieb hromadného financovania musí mať pripravené postupy pre prípad ak by jeho online platforma prestala fungovať spôsobom ako predpokladá zákon. Z hľadiska digitalizácie je to ochrana údajov klientov, zmlúv klientov avšak vnímam to aj ako zabezpečenie funkčnosti platformy ako takej. Teda jej spôsobilosti digitálne prepájať investorov so subjektami, ktoré sa snažia získať financovanie (vlastníci projektov) ako spôsobilosť zhromažďovať peňažné prostriedky investorov.

Vyššie uvedené požiadavky takto predstavujú požiadavky z oblasti digitalizácie vyžadované pre účely získania licencie. Môžeme tak konštatovať, že regulácia, ktorá vyžaduje aby bol investičný crowdfunding vykonávaný digitálnym spôsobom, rovnako aj stanovuje technické požiadavky v oblasti digitalizácie pre výkon tejto činnosti. Tieto technické požiadavky musia byť pri každej platforme individuálne nadizajnované, naprogramované a technicky zabezpečené v príslušnej platforma hromadného financovania. Zároveň regulácia vyžaduje aby poskytovateľ služieb hromadného financovania bol spôsobilý udržiavať svoju online platformu v prevádzke a bol spôsobilý sa vysporiadať s rizikami prerušenia bežnej prevádzky platformy v digitálnej sfére.

Záver

Záverom môžeme skonštatovať, že crowdfunding je príslušnou právnou reguláciou definovaný prostredníctvom digitálneho nástroja – elektronickej, resp. online

¹⁹ Recitál 2 a 3 Nariadenia o politike kontinuity

²⁰ Čl. 5 Nariadenia o politike kontinuity

platformy, pričom finančná regulácia vyžaduje aby bol vykonávaný prostredníctvom tejto platformy. Môžeme tak hovoriť o umiestnení crowdfundingu do čisto digitálneho prostredia, keď ho ani nie je možné vykonávať inak ako digitálnym spôsobom.

V slovenskom právnom kontexte toto digitálne nastavenie ilustruje aj neprípustnosť využívania finančných agentov pre účely sprostredkovania služieb poskytovateľa služieb hromadného financovania. ECSP Nariadenie neumožňuje využívať tzv. viazaných finančných agentov, ako je umožnené v rámci regulácie upravujúcej investičné služby vo všeobecnosti Smernica MiFID²¹, z ktorej ECSP Nariadenie vychádza. V slovenskom kontexte, podľa zákona č. 186/2009 Z.z., o finančnom sprostredkovaní a finančnom poradenstve (ďalej **Zákon o finančnom poradenstve**). Tento zákon upravuje tzv. poskytovanie finančného sprostredkovania v sektore kapitálového trhu²², ktoré pozostáva z poskytovania investičnej služby prijímanie a postupovanie pokynov klienta týkajúcich sa prevoditeľných cenných papierov a z poskytovania investičnej služby finančného poradenstva²³. Poskytovanie finančného poradenstva v tomto rozsahu by bolo teoreticky možné aj vo vzťahu k prevoditeľným cenným papierom, ktoré sú emitované vlastníkom projektu rámci hromadného financovania, avšak Zákon o finančnom sprostredkovaní neumožňuje finančnému agentovi poskytovať služby poskytovateľovi služieb hromadného financovania²⁴. Teda inému subjektu ako je finančná inštitúcia, pričom poskytovateľ služieb hromadného financovania definíciu finančnej inštitúcie nespĺňa. Finančný agent tak nie oprávnený poskytovať finančné sprostredkovanie pre poskytovateľa služieb hromadného financovania. Z pohľadu autora článku toto obmedzenie znemožňuje vykonávať crowdfunding inak ako prostredníctvom online platformy a teda digitálne.

Crowdfunding z pohľadu digitalizácie je možné vnímať aj ako nadstavbu na existujúce digitálne systémy a činnosti vykonávané v oblasti finančného sektora digitálnym spôsobom. Týmto ďalšími činnosťami sú platobné služby a úschova cenných papierov (cenných papierov v dematerializovanej forme). ECSP Nariadenie dokonca umožňuje získať poskytovateľovi služieb hromadného financovania

²¹ Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi

²² §2 ods. 2 Zákona o finančnom sprostredkovaní

²³ Definícia tých služieb: (i) poskytovanie investičnej služby prijímanie a postupovanie pokynov klienta⁵ týkajúcich sa prevoditeľných cenných papierov a cenných papierov a majetkových účastí vo fondoch kolektívneho investovania a ich propagácia a poskytovanie investičnej služby investičného poradenstva⁵ vo vzťahu k prevoditeľným cenným papierom a cenným papierom a majetkovým účastiam vo fondoch kolektívneho investovania

²⁴ §6 a §4 písm. b) Zákona o finančnom sprostredkovaní

oprávnenie na vykonávanie týchto služieb²⁵, avšak za splnenia podmienok podľa príslušnej sektorovej regulácie.

Zaujímavou otázkou smerom do budúcnosti crowdfundingu a digitalizácie, bude skúmať ako bude tento fenomén digitalizácie fungovať s novším fenoménom digitalizácie, ako sú kryptoaktíva. Vzhľadom na aktuálny stav finančnej regulácie a regulácie kryptoaktív, tieto nie sú prepojené. Avšak nemusí byť ťažké si predstaviť ako crowdfunding môže fungovať aj v oblasti kryptoaktív, za podmienky regulatórnej konvergencie upravujúcich tieto produkty digitalizácie.

Zoznam použitej literatúry

1. Čunderlík, Ľ., Čunderlík, Čerbová, V., Daudrikh, Y., Heseková, S., Katkovčin, M., Mazúr, J. Inovatívne a atypické modely správy majetku na finančnom trhu a súvisiace otázky. Vedecká monografia Praha: Leges, 2019. 183 s. ISBN 978-80-7502-405-3, str. 106-111
2. Dalla Chiesa, C. (2020). From digitalization to crowdfunding platforms: fomenting the cultural commons. In E. Macri (Ed.), Cultural Commons and Urban Dynamics (pp. 173-186) https://doi.org/10.1007/978-3-030-54418-8_11
3. Md. Abdul Halim, Does crowdfunding contribute to digital financial inclusion?, Research in Globalization, Volume 9, 2024, ISSN 2590-051X, <https://doi.org/10.1016/j.resglo.2024.100238>
4. Heseková Bojmírová, S.-Katkovčin, M.: Právne vzťahy v rámci peer to peer lendingu; Justičná revue, 73, 2021, č. 11, s. 1312-1326
5. Simona Heseková, Andrea Szakács, Služby hromadného financovania založené na požičiavaní a ich daňové aspekty, 2021
6. Rotem Shneor, Karsten Wenzlaff, Konstantin Boyko, Prince Baah-Peprah, Ana Odorović, Olga Okhrimenko, European crowdfunding market report 2023, University of Agder, School of Business

Kontaktné údaje

Mgr. Matej Krkoška LL.M.

matej.krkoska@gmail.com

Právnická fakulta Univerzity Komenského

²⁵ Čl. 10 ECSP Nariadenia

ELEKTRONICKÁ FAKTURÁCIA V OBLASTI DPH Z POHĽADU ORGÁNOV VEREJNEJ MOCI

ELECTRONIC INVOICING IN THE FIELD OF VAT FROM THE PERSPECTIVE OF PUBLIC AUTHORITIES

Filip Richter¹

Abstrakt: Autor v predkladanom príspevku, opierajúc sa o vnútroštátne právo, ako aj o právo EÚ, analyzuje dopad návrhov legislatívnych zmien v oblasti elektronickej fakturácie, obsiahnutých v návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa menia dopĺňajú niektoré zákony, na povinnosti orgánov verejnej moci vo vzťahu k vyhotovovaniu faktúry na účely dane z pridanej hodnoty. Cieľom príspevku je vo všeobecnosti poukázať na postavenie orgánov verejnej moci z hľadiska uplatňovania spoločného systému dane z pridanej hodnoty, ďalej v stručnosti predstaviť návrhy zmien týkajúcich sa elektronickej fakturácie v oblasti dane z pridanej hodnoty, ktoré sa dotknú orgánov verejnej moci s účinnosťou od 1. januára 2027 a 1. júla 2030 a tie, so zameraním na povinnosť vyhotoviť faktúru na účely dane z pridanej hodnoty, porovnať so súčasnou právnou úpravou. Autor v tejto súvislosti využíva analytickú metódu na správne uchopenie navrhovaných zmien v oblasti elektronickej fakturácie, ďalej metódu komparácie s cieľom porovnať tieto zmeny so súčasnou právnou úpravou a metódu syntézy na formulovanie záverov. Stručný priestor bude venovaný aj povinnosti oznamovania údajov z tuzemských a cezhraničných transakcií.

Kľúčové slová: DPH, faktúra, elektronickej faktúra, orgán verejnej moci

Abstract: In this paper, the author, relying on both national law and European Union law, analyses the impact of proposed legislative changes in the field of electronic invoicing, as set out in the draft Act amending and supplementing Act No. 222/2004 Coll. On Value Added Tax as amended, and amending and supplementing certain other acts, on the obligations of public authorities with respect to invoice issuance for VAT purposes. The aim of the paper is, in general, to highlight the position of public authorities in the context of the

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra trestného práva, kriminológie a kriminalistiky.

application of the common system of VAT, to briefly present the proposed amendments concerning electronic invoicing in the field of VAT that will affect public authorities as of 1 January 2027 and 1 July 2030, and to compare these proposals, with a particular focus on the obligation to issue an invoice for VAT purposes, with the current legal framework. In this context, the author applies the analytical method to appropriately interpret the proposed changes in the field of electronic invoicing, the comparative method to assess these changes in relation to the existing legal framework, and the method of synthesis to draw relevant conclusions. A concise part of the paper will also address the obligation to report information from domestic and cross-border transactions.

Key words: VAT, invoice, electronic invoice, public authority

Úvod

Typickým charakteristickým znakom kontinuálne rozvíjajúcej sa spoločnosti je, okrem iného, výrazný trend digitalizácie naprieč širokým spektrom oblastí. Jednou z nich je prirodzene aj oblasť dokumentovania transakcií, teda oblasť fakturácie, ktorá zastáva významné miesto v rámci uplatňovania spoločného systému DPH. Konkrétnu podobu snahy o digitalizáciu procesu fakturácie na účely DPH bolo možné badať už v marci 2025, kedy došlo k dlho očakávanému prijatiu smernice Rady (EÚ) 2025/516 z 11. marca 2025, ktorou sa mení smernica 2006/112/ES, pokiaľ ide o pravidlá DPH pre digitálny vek (Ú. v. EÚ L, 2025/516, 25.3.2025) [ďalej len „smernica Rady (EÚ) 2025/516“],² na základe ktorej sa, okrem iného,³ zavádza elektronická fakturácia ako predvolená metóda dokumentovania transakcií na účely DPH. V nadväznosti na prijatie citovanej smernice a na ciele deklarované v programovom vyhlásení vlády SR na roky 2023 – 2027 začalo Ministerstvo financií SR pracovať na návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej

² Európska komisia iniciovala iniciatívu DPH v digitálnom veku s cieľom modernizovať systém DPH v EÚ a zvýšiť jeho odolnosť voči podvodom a podnikateľskú priateľnosť využitím príležitostí, ktoré prináša digitalizácia. Iniciatíva DPH v digitálnom veku má svoj pôvod v Akčnom pláne pre spravodlivé a jednoduché zdaňovanie na podporu stratégie obnovy. MERKX, M. – GRUSON, J. – VERBAAN, N. – VAN DER DOEFL, B.: VAT in the Digital Age Package: Viva La ViDA or LivinMadeleine, Merckx and Gruson, John and Verbaan, Naomie and van der Doef, Bart, VAT in the Digital Age Package: Viva La ViDA or Livin' La ViDA Loca? [online]. In: EC Tax Review, 2023, ročník 32, č. 3, s. 127 [cit. 2025-11-08]. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4437300

³ Iniciatíva DPH v digitálnom veku sa skladá z troch častí: (i) digitálne oznamovanie v reálnom čase na základe elektronickej fakturácie, (ii) zmeny v DPH zaobchádzaní v rámci platformovej ekonomiky a (iii) zavedenie konceptu jednotnej registrácie na účely DPH. MERKX, M. – GRUSON, J. – VERBAAN, N. – VAN DER DOEFL, B.: VAT in the Digital Age package: Singling out the Single VAT Registration [online]. In: EC Tax Review, 2023, ročník 32, č. 4, s. 172 [cit. 2025-11-08]. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4504784

hodnoty v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „novela zákona o DPH“), a to s cieľom transponovať čl. 1 a čl. 5 citovanej smernice. Hlavným dôvodom prijatia smernice (EÚ) 2025/516 bolo zavedenie harmonizovaných pravidiel týkajúcich sa digitálneho oznamovania údajov vyplývajúcich z nárastu digitálneho hospodárstva, ktorý výrazne ovplyvnil fungovanie systému DPH v rámci Európskej únie, keďže súčasná právna úprava neumožňuje plnohodnotné využívanie údajov vychádzajúcich z nových digitálnych obchodných modelov. Smernica Rady (EÚ) 2006/112/ES z 28. novembra 2006 o spoločnom systéme dane z pridanej hodnoty (Ú. v. EÚ L 347 11.12.2006) v platnom znení (ďalej len „smernica o DPH“) bola zmenená tak, aby sa v nej zohľadnil tento vývoj. S cieľom zvýšiť výber daní z cezhraničných transakcií, ako aj z dôvodu diverzifikácie prostredia, kedy členské štáty majú zavedené rozdielne systémy oznamovania, bolo potrebné stanoviť jednotné únieové požiadavky na digitálne oznamovanie spočívajúce v tom, že transakcie, ktoré sa majú daňovým správam oznamovať, sa budú dokumentovať elektronicky. Používanie elektronickej fakturácie sa preto stane predvoleným systémom vyhotovovania faktúr.⁴ Keďže do spoločného systému DPH sú v určitej miere zapojené aj orgány verejnej moci, ktorým však vo všeobecnosti nebýva venovaný výrazný priestor v akademickej, vedeckej či odbornej spisbe týkajúcej sa problematiky DPH, tak cieľom tohto príspevku je vo všeobecnosti poukázať na postavenie orgánov verejnej moci z hľadiska uplatňovania spoločného systému DPH, ďalej v stručnosti predstaviť návrhy zmien týkajúcich sa elektronickej fakturácie v oblasti DPH, ktoré sa dotknú orgánov verejnej moci s účinnosťou od 1. januára 2027 a 1. júla 2030 a tie, so zameraním na povinnosť vyhotoviť faktúru na účely DPH, porovnať s právnou úpravou *de lege lata*. Východiskovým bodom metodického postupu, pokiaľ ide o postavenie orgánov verejnej moci, je analýza únieového a vnútroštátneho normatívneho právneho rámca so zreteľom na zásadu neutrality DPH, na základe ktorej bude možné ozrejmiť postavenie týchto subjektov v rámci spoločného systému DPH a ich participáciu na ňom. Z hľadiska elektronickej fakturácie metodika vychádza z obsahovej analýzy ustanovení navrhovanej právnej úpravy v novele zákona o DPH, ktorá predstavuje nevyhnutný základ pre následné porovnanie navrhovaných zmien s platnou právnou úpravou. Príspevok vychádza z verzie novely zákona o DPH, ktorá bola doručená poradným orgánom vlády SR. Keďže téma elektronickej fakturácie v kontexte smernice Rady (EÚ) 2025/516 predstavuje na Slovensku pomerne novú oblasť výskumu, a zároveň vzhľadom k tomu, že samotný legislatívny proces k novele zákona o DPH ešte nie je

⁴ Dôvodová správa k návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Všeobecná časť [online]. Legislatívny proces č. LP/2025/396 [cit. 2025-09-15]. Dostupné na internete: <https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/396/sprievodne-dokumenty?stadiumUuid=f5c7b0b3-059e-4bc8-afad-52ad5b1af5b9>

ukončený, tak k predmetnej oblasti v súčasnosti existuje len veľmi obmedzené množstvo vedeckej či odbornej literatúry.⁵

Orgány verejnej moci ako (ne)zdaniteľné osoby

Smernica o DPH, ako vyplýva z jej článku 1 ods. 1, ustanovuje spoločný systém DPH, vo vzťahu ku ktorému ďalej stanovuje, že tento sa uplatňuje až po maloobchodný stupeň vrátane a je založený na zásade, že na tovar a služby sa uplatňuje všeobecná daň zo spotreby presne úmerná cene tovaru a služieb bez ohľadu na počet transakcií uskutočnených vo výrobnom a distribučnom procese pred stupňom, na ktorom sa daň účtuje. Na každú transakciu sa uplatní DPH vypočítaná z ceny tovaru alebo služieb podľa sadzby platnej pre tento tovar alebo služby po odpočítaní sumy DPH, ktorou boli priamo zaťažené rôzne nákladové prvky. Uvedené ustanovenie vyjadruje základnú zásadu spoločného systému DPH, ktorou je zásada neutrality. DPH ako všeobecná nepriama daň zo spotreby sa v tejto súvislosti vyberá na každom hospodárskom stupni.⁶ DPH je v nadväznosti na uvedené skutočnosti nepochybne širokospektrálnou daňou, ktorá sa uplatňuje na každom stupni výrobného a distribučného procesu až po maloobchodný stupeň vrátane.

Jedným z ústredných pojmov spoločného systému DPH je práve pojem „zdaniteľná osoba“. Pokiaľ ide o definíciu pojmu zdaniteľná osoba, predmetný pojem je definovaný vo vzťahu k nezávislému vykonávaniu ekonomickej činnosti. Pojem „ekonomická činnosť“ je pritom potrebné vykladať extenzívne, ako každú nezávislú činnosť, z ktorej sa dosahuje príjem na pokračujúcom základe. Napriek objektívnemu poňatiu uvedeného pojmu z dôvodu čo najširšieho možného zdanenia spotreby tovarov a služieb, smernica o DPH pri splnení určitých presne stanovených podmienok jednoznačne nepovažuje istú kategóriu osôb, ktoré vykonávajú činnosť za poplatok, za zdaniteľné osoby.⁷ Túto kategóriu osôb predstavujú orgány verejnej moci. Pre úplnosť treba však upozorniť, že orgány verejnej moci – ako „nekomerčné subjekty“ zabezpečujúce výkon verejnej moci, nie sú v celistvosti vylúčené z uplatňovania spoločného systému DPH, avšak požívajú osobitný režim vzhľadom na povahu činností, ktoré vykonávajú z titulu verejnej moci im zverenej príslušným zákonom alebo na základe zákona. Uvedené má aj normatívny základ priamo v smernici o DPH. V tejto súvislosti sa žiada poukázať na článok 13 ods. 1 smernice o DPH, ktorý ustanovuje, za akých podmienok sa orgán verejnej moci považuje za

⁵ Napr. DANCÁK, J.: Elektronická fakturácia a digitálne oznamovanie v kontexte smernice ViDA. In: Bulletin Slovenskej komory daňových poradcov. 2025, číslo 3, s. 10-18.

⁶ RICHTER, F.: Podvod na dani z pridanej hodnoty verzus trestný čin daňového podvodu. In: Bratislavské právnické fórum 2023 : aktuálne výzvy trestného práva. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, s. 323.

⁷ BEŇO, M. – KAČALJAK, M. – ORDA ORAVCOVÁ, A. – RICHTER, F. – SÁBO, J. – VARGAN, M.: Zákon o dani z pridanej hodnoty. Komentár. Bratislava : Wolters Kluwer SR, 2024, s. 24.

zdaniteľnú osobu.⁸ Podľa citovaného ustanovenia totiž platí, že: „*Štáty, regionálne a miestne orgány, ako aj iné subjekty, ktoré sa spravujú verejným právom, sa nepovažujú za zdaniteľné osoby vzhľadom na činnosti alebo transakcie, ktorých sa zúčastňujú ako orgány verejnej moci ani vtedy, keď v súvislosti s týmito činnosťami alebo transakciami vyberajú dávky, poplatky, príspevky alebo platby. Keď však uskutočňujú takéto činnosti alebo transakcie, považujú sa za zdaniteľné osoby v súvislosti s týmito činnosťami alebo transakciami, ak by zaobchádzanie s nimi ako s nezdaniiteľnými osobami viedlo k závažnému narušeniu hospodárskej súťaže. Subjekty, ktoré sa spravujú verejným právom, sa v každom prípade považujú za zdaniteľné osoby v súvislosti s činnosťami uvedenými v prílohe I za predpokladu, že uvedené činnosti nevykonávajú v zanedbateľnom rozsahu.*“

Skôr uvedené ustanovenie smernice o DPH je kogentnej povahy, teda nepripúšťajú sa od neho odchýlky. V tejto súvislosti bolo transponované aj do zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon o DPH“), a to konkrétne do § 3 ods. 4 tohto zákona, podľa ktorého štátne orgány a ich rozpočtové organizácie, štátne fondy, orgány územnej samosprávy a ich rozpočtové organizácie a iné právnické osoby, ktoré sú orgánmi verejnej moci, sa nepovažujú za zdaniteľné osoby, keď konajú v rozsahu svojej hlavnej činnosti, a to ani v prípade, ak prijímajú v súvislosti s touto činnosťou platby, s výnimkou, ak táto činnosť výrazne narušuje alebo môže výrazne narušiť hospodársku súťaž, a s výnimkou, ak vykonávajú činnosti uvedené v prílohe č. 8 a tieto činnosti nevykonávajú v zanedbateľnom rozsahu. Správa štátnych hmotných rezerv Slovenskej republiky je zdaniteľnou osobou v rozsahu nákupu a predaja štátnych hmotných rezerv.

Orgány verejnej moci teda nie sú v absolútnej rovine vylúčené z uplatňovania DPH. V kontexte § 3 ods. 4 zákona o DPH platí duálna koncepcia nazerania na skúmanie postavenia orgánov verejnej moci na účely zákona o DPH, teda či sú zdaniteľnými osobami alebo ide v danom prípade o nezdaniiteľné osoby. Uvedené sa však vyhodnocuje vo vzťahu ku konkrétnej činnosti. Pre lepší kontext sa žiada začať rovinou, ktorá je v normatívnom texte uvedená až ku koncu ustanovenia. Ide teda o rovinu spočívajúcu v tom, že orgány verejnej moci sa považujú za zdaniteľné osoby, ak vykonávajú činnosti uvedené v prílohe č. 8 k zákonu o DPH v inom ako zanedbateľnom rozsahu. V prílohe č. 8 k zákonu o DPH sú taxatívnym spôsobom vymedzené činnosti, ktoré ak sú vykonávané ako ekonomická činnosť akýmkoľvek inými osobami ako orgánmi verejnej moci, tak niet pochyb, že tieto osoby sa na účely zákona o DPH pri výkone týchto činností považujú za zdaniteľné osoby. Ide o (i) telekomunikačné služby, (ii) dodanie vody, plynu, elektriny a tepla, (iii) prepravu

⁸ BERGER, W. – KINDL, C. – WAKOUNIG, M.: Smernice ES o dani z pridanej hodnoty. Praktický komentár. Praha : 1. VOX, 2010, s. 159.

tovaru, (iv) prístavné a letiskové služby, (v) prepravu osôb, (vi) dodanie nového tovaru vyrobeného na predaj, (vii) činnosti pôdohospodárskych sprostredkovateľských agentúr týkajúce sa pôdohospodárskych produktov vykonávané podľa predpisov o spoločnej organizácii trhu s týmito produktmi, (viii) organizovanie obchodných veľtrhov a výstav, (ix) skladovanie, (x) reklamné služby, (xi) služby cestovného ruchu, (xii) prevádzkovanie predajní pre zamestnancov, prevádzkovanie jedální pre zamestnancov a prevádzkovanie podobných prevádzok a (xiii) činnosti verejnoprávnej televízie a verejnoprávneho rozhlasu iné ako tie, ktoré sú oslobodené od dane podľa § 36 zákona o DPH. Ak teda niektorú z týchto činností vykonáva orgán verejnej moci v inom ako zanedbateľnom rozsahu, považuje sa tento orgán za zdaniteľnú osobu v tomto rozsahu.

Druhá rovina sa týka činností iných ako tých uvedených v prílohe č. 8 k zákonu o DPH, čo vyplýva z logického kontextu § 3 ods. 4 zákona o DPH, keďže podľa zákona o DPH sa orgány verejnej moci nepovažujú za zdaniteľné osoby, keď konajú v rozsahu svojej hlavnej činnosti, a to ani v prípade, ak prijímajú v súvislosti s touto činnosťou platby, s výnimkou, ak táto činnosť výrazne narušuje alebo môže výrazne narušiť hospodársku súťaž. Ide teda o činnosti hospodárskej povahy, výkonom ktorých by sa pri ponechaní vylúčenia orgánov verejnej moci z mechanizmu DPH výrazne narušovala alebo mohla výrazne narušiť hospodárska súťaž. V zásade však treba doplniť, že ide o také činnosti, ktoré môžu byť vykonávané paralelne tak orgánmi verejnej moci, ako aj súkromno-právnymi subjektmi.⁹

Uplatňovanie zákona o DPH orgánmi verejnej moci

Pokiaľ ide o uplatňovanie zákonných pravidiel v oblasti DPH z pohľadu orgánov verejnej moci, na úvod je dôležité sa vysporiadať s postavením orgánu verejnej moci pri vykonávaní konkrétnej činnosti. V prípade, že orgán verejnej moci na účely výkonu konkrétnej činnosti nemá postavenie zdaniteľnej osoby, teda je nezdaniteľnou osobou (bez registrácie podľa § 7 zákona o DPH), na účely zákona o DPH mu nevznikajú žiadne povinnosti, avšak pri vstupných činnostiach môže za istých okolností vzniknúť povinnosť podať žiadosť o registráciu pre daň podľa § 7 zákona o DPH, a následne aj povinnosť platiť daň. Naopak, ak má v súvislosti s výkonom konkrétnej činnosti orgán verejnej moci postavenie zdaniteľnej osoby, môžu mu na účely zákona o DPH vzniknúť práva a povinnosti, avšak pokiaľ ide o rozsah týchto práv a povinností, všetko závisí od konkrétnych skutkových okolností prípadu. Jedným z druhov zákonných povinností, ktoré zákon o DPH ukladá osobám povinným platiť daň, je aj povinnosť vyhotovovať faktúry. Zákon o DPH v § 72 ustanovuje osoby, ktoré sú povinné na účely zákona o DPH vyhotoviť faktúru. Vo

⁹ BEŇO, M. – KAČALJAK, M. – ORDA ORAVCOVÁ, A. – RICHTER, F. – SÁBO, J. – VARGAN, M.: Zákon o dani z pridanej hodnoty. Komentár. Bratislava : Wolters Kluwer SR, 2024, s. 25.

väčšine prípadov pôjde o osoby, ktoré sú platiteľmi dane, avšak za určitých okolností majú povinnosť vyhotoviť faktúru aj iné osoby – zdaniteľné osoby, zahraničné osoby alebo napr. aj akákoľvek osoba. Pokiaľ má orgán verejnej moci postavenie platiteľa dane, tak pri výkone určitej konkrétnej činnosti (dodanie tovaru alebo služby inej zdaniteľnej osobe alebo právnickej osobe, ktorá nie je zdaniteľnou osobou) s miestom dodania v tuzemsku, v súvislosti s ktorou má uvedené postavenie platiteľa dane, mu vzniká, okrem iného, povinnosť vyhotoviť faktúru pri dodaní tovaru alebo služby podľa § 72 ods. 1 písm. a) zákona o DPH. V súčasnosti je bežné, že orgány verejnej moci majú postavenie platiteľov dane, pričom ide predovšetkým o obce a mestá,¹⁰ ale postavenie platiteľa dane má napr. aj Ministerstvo obrany Slovenskej republiky.¹¹ Pre orgány verejnej moci je ale typická aj registrácia podľa § 7 zákona o DPH.

Navrhované zmeny v oblasti fakturačných pravidiel

Novelou zákona o DPH sa navrhujú rozsiahle zmeny v oblasti fakturačných pravidiel v oblasti DPH. Tieto zmeny však možno veľmi zjednodušene rozdeliť na dve veľké oblasti – prvou je zavedenie povinnej elektronickej fakturácie a druhou zase zavedenie digitálneho oznamovania údajov o dodaniach tovarov a služieb finančnej správe. Iniciatíva návrhov týchto zmien pramení v podstate z dvoch rovín. Vychádzajúc zo všeobecnej časti dôvodovej správy k novele zákona o DPH a zamerajúc sa na vnútroštátne aspekty, vláda SR sa vo svojom programovom vyhlásení na roky 2023 – 2027 zaviazala zefektívniť boj proti daňovým únikom a čo najefektívnejšie využiť existujúce opatrenia, ako aj prijať nové s cieľom dosiahnuť minimalizáciu počtu a objemu daňových únikov a zníženie daňovej medzery. V tomto kontexte, v rámci strednodobých priorít, je jej snahou zaviesť povinnú elektronickú fakturáciu a digitálne oznamovanie údajov o dodaniach tovarov a služieb finančnej správe. Táto prvá rovina ale vychádza zároveň z druhej roviny, ktorou je transpozícia smernice Rady (EÚ) 2025/516.¹²

¹⁰ Napr. obec Bajtava, obec Horná Ves, mesto Nitra, mesto Hurbanovo. Pozri Zoznam daňových subjektov registrovaných pre DPH [online] [cit. 2025-08-24]. Dostupné na internete: https://www.financnasprava.sk/sk/elektronicke-sluzby/verejne-sluzby/zoznamy/detail/_101c6128-e1f6-4a48-81ed-ad3c01220e03/?q=Tv6nMSlnOdlagGbaZ9Wr8l_EGpQVsaJ3iYUC8oFTydjMmWNBmJVDzPoJXCpnIEfMuMclBfe6iif_KmTfD4hzsBYWmiWoTO7lsz3KoFWD2dSEXghSchoif-Bwocxp1Rc6wbaA4neTSobzBgjSWC6CRS8ZGuCrmi6LWxwYfX1X-mSmc2bkhMorMvOyYbqrNoadKXG3olzBv8lCsvrl3FGkfPFQhoY=

¹¹ Tamže.

¹² Dôvodová správa k návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Všeobecná časť

Zamerajúc sa už ďalej na obsah samotných navrhovaných zmien zákona o DPH, z vlastného materiálu k novele zákona o DPH vyplýva, že zmeny v oblasti fakturačných pravidiel sa navrhujú s účinnosťou od 1. januára 2027 a potom od 1. júla 2030. Uvedené sa odvíja od transpozičných lehôt k príslušným článkom smernice Rady (EÚ) 2025/516. S účinnosťou od 1. januára 2027 sa navrhuje zaviesť povinnú elektronickú fakturáciu pre tuzemských platiteľov dane (registrácia pre daň podľa § 4, § 4b alebo §4c zákona o DPH), ktorá sa má vzťahovať na tuzemské transakcie. Zároveň sa navrhuje ustanoviť aj požiadavky, ktoré musí doklad alebo oznámenie spĺňať, aby bolo považované za elektronickú faktúru. Elektronickou faktúrou bude teda len taký doklad alebo oznámenie, ktoré obsahuje náležitosti podľa § 74 ods. 1 zákona o DPH a je vyhotovené, zaslané a prijaté vo formáte elektronického dokumentu, ktorý umožňuje jeho automatizované a elektronické spracovanie, a v dátovej štruktúre v súlade s technickou normou pre elektronickú fakturáciu a so zoznamom jej syntaxí podľa vykonávacieho rozhodnutia Komisie (EÚ) 2017/1870 zo 16. októbra 2017 o uverejnení odkazu na európsku normu pre elektronickú fakturáciu a zoznamu syntaxí podľa smernice Európskeho parlamentu a Rady 2014/55/EÚ (Ú. v. EÚ L 266, 17. 10. 2017)[ďalej len „vykonávacie rozhodnutie Komisie (EÚ) 2017/1870“]. Novelou zákona o DPH sa tiež navrhuje s účinnosťou od 1. januára 2027 zaviesť povinnosť oznámiť vybrané údaje finančnej správe z tuzemských transakcií, ak je platiteľ dane povinný vyhotoviť elektronickú faktúru, ktorú zasiela príjemcovi doručovacou službou. Táto povinnosť sa navrhuje zaviesť aj platiteľovi dane, ktorý je príjemcom plnenia a prijal elektronickú faktúru prostredníctvom doručovacej služby. Povinnosť oznamovať vybrané údaje z elektronickej faktúry prostredníctvom kontrolného výkazu týmto nie je dotknutá. Všetky tieto zmeny sa navrhujú upraviť v príslušnom prechodnom ustanovení zákona o DPH.

Pokiaľ ide o zmeny s účinnosťou od 1. júla 2030, tieto sa navrhuje upraviť do systémových ustanovení zákona o DPH, pričom v zásade zostáva zachovaná povinnosť elektronickej fakturácie pre tuzemských platiteľov dane, ako aj povinné oznamovanie údajov z tuzemských transakcií, avšak dochádza k rozšíreniu povinnosti elektronickej fakturácie a oznamovania údajov aj na oblasť cezhraničných transakcií, pričom povinnosť cezhraničnej elektronickej fakturácie a povinnosť oznamovať údaje o cezhraničných transakciách sa budú vzťahovať už aj na platiteľov dane registrovaných pre daň podľa § 5 zákona o DPH a v zákonom ustanovených prípadoch aj na zdaniteľné osoby registrované pre daň podľa § 7 alebo § 7a zákona o DPH. Elektronickou faktúrou bude aj s účinnosťou od 1. júla 2030 len taký doklad alebo oznámenie, ktoré obsahuje náležitosti podľa § 74 ods. 1 zákona o DPH a je

[online]. Legislatívny proces č. LP/2025/396 [cit. 2025-09-15]. Dostupné na internete: <https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/396/sprievodne-dokumenty?stadiumUuid=f5c7b0b3-059e-4bc8-afad-52ad5b1af5b9>

vyhotovené, zaslané a prijaté vo formáte elektronického dokumentu, ktorý umožňuje jeho automatizované a elektronické spracovanie, a v dátovej štruktúre v súlade s technickou normou pre elektronickú fakturáciu a so zoznamom jej syntaxí podľa vykonávacieho rozhodnutia Komisie (EÚ) 2017/1870. S účinnosťou od 1. júla 2030 sa zároveň navrhuje úplné vypustenie povinnosti podávať kontrolný výkaz a súhrnný výkaz. Novelou zákona o DPH sa zároveň s účinnosťou od 1. januára 2027 navrhuje ustanoviť, že každá osoba, ktorej je v tuzemsku dodaný tovar alebo služba, pri ktorej je zdaniteľná osoba povinná vyhotoviť elektronickú faktúru podľa zákona o DPH, je povinná zabezpečiť, aby mohla prijať elektronickú faktúru zaslanú doručovacou službou.

Vo všeobecnosti možno k navrhovaným zmenám uviesť, že novela zákona o DPH je formulovaná mimoriadne komplikovaným a legislatívno-technicky náročným spôsobom. Orientáciu v jednotlivých zmenách sťažuje aj skutočnosť, že sa navrhujú rôzne dátumy nadobudnutia účinnosti, čo znásobuje mieru nejasnosti. Pre orgány verejnej moci, ale aj pre iné subjekty, tak môže byť problematické vôbec identifikovať, či a ako sa ich určité nové povinnosti týkajú.

Vplyv legislatívnych zmien v oblasti fakturácie na orgány verejnej moci

S ohľadom na navrhovanú techniku nadobudnutia účinnosti novely zákona o DPH možno pristúpiť k sumarizácii vplyvov legislatívnych zmien v oblasti fakturácie na orgány verejnej moci do dvoch skupín. Prvá skupina sa týka vplyvu legislatívnych zmien, pri ktorých sa navrhuje, aby nadobudli účinnosť 1. januára 2027 – ide o tuzemskú elektronickú fakturáciu a oznamovanie údajov z tuzemských transakcií. V rámci dotknutých legislatívnych zmien je teda možné skonštatovať, že orgán verejnej moci, ktorý je nezdaniteľnou osobou, nebude mať povinnosť od 1. januára 2027 vyhotoviť elektronickú faktúru pri tuzemskom dodaní tovaru alebo služby, ako ani povinnosť oznamovať údaje z takejto tuzemskej transakcie, keďže nevyhotovuje elektronickú faktúru. Takýto orgán verejnej moci však bude mať povinnosť zabezpečiť, aby bol schopný prijať elektronickú faktúru od platiteľa dane, ktorému vznikla povinnosť vyhotoviť elektronickú faktúru. Z prijatej elektronickej faktúry ale takémuto orgánu verejnej moci tiež nevznikne povinnosť oznamovať údaje. V prípade, ak ide o orgán verejnej moci, ktorý má postavenie platiteľa dane a zároveň v posudzovanom prípade aj koná ako platiteľ dane, tak tomuto orgánu verejnej moci pri dodaní tovaru alebo služby s miestom dodania v tuzemsku zdaniteľnej osobe so sídlom, miestom podnikania, prevádzkarňou, bydliskom v tuzemsku, alebo ktorá sa v tuzemsku obvykle zdržiava, alebo nezdaniteľnej právnickej osobe so sídlom alebo miestom charakterizovaným dostatočným stupňom stálosti a vhodnou štruktúrou, ak ide o ľudské a technické zdroje potrebné na výkon jej činnosti, vzniká povinnosť vyhotoviť elektronickú faktúru. Povinnosť vyhotoviť faktúru má dotknutý orgán

verejnej moci aj podľa aktuálnej právnej úpravy, avšak s tým rozdielom, že nemusí ísť o elektronickú faktúru. Okrem toho orgánu verejnej moci zároveň vzniká povinnosť oznámiť vybrané údaje z dotknutej transakcie. V prípade, ak je orgán verejnej moci, ktorý je platiteľom dane a koná ako platiteľ dane, v postavení príjemcu plnenia, tomuto orgánu verejnej moci vzniká tak povinnosť prijať elektronickú faktúru, ako aj povinnosť oznámiť vybrané údaje. Pokiaľ ide o druhú skupinu legislatívnych zmien, pri ktorých sa navrhuje účinnosť od 1. júla 2030 a týkajú sa rozšírenia elektronickej fakturácie a oznamovania údajov aj na cezhraničné transakcie, možno skonštatovať, že v tejto oblasti platia rovnaké závery ako pri prvej skupine.

Záver

Novela zákona o DPH prináša niekoľko zmien do oblasti fakturácie z pohľadu orgánov verejnej moci. Najvýraznejšou zmenou je skutočnosť, že faktúra sa bude vyhotovovať ako elektronická faktúra v súlade so zákonnými požiadavkami. Odhliadnuc od toho, aktuálne pravidlá určenia osôb, ktoré sú povinné vyhotoviť faktúru, sa ale v zásade nemenia. Orgány verejnej moci, ktoré majú postavenie platiteľov dane a aj konajú v rámci konkrétnej transakcie ako platitelia dane, budú mať aj podľa novely zákona o DPH povinnosť vyhotoviť faktúru, hoci už ako elektronickú faktúru. Naopak, orgány verejnej moci, ktoré sú nezdaniteľnými osobami, takúto povinnosť mať nebudú, rovnako ako podľa aktuálnej právnej úpravy. Takéto orgány verejnej moci však budú mať povinnosť byť spôsobilé prijať elektronickú faktúru. Keďže v prípade povinnej elektronickej fakturácie ide o oblasť, ktorá v súčasnosti nepredstavuje bežnú prax všetkých orgánov verejnej moci, samotné prijatie legislatívnych zmien nebude postačovať na zabezpečenie ich efektívnej a jednotnej aplikácie. *De lege ferenda* je preto nevyhnutné uvažovať o vydaní minimálne metodických pomôcok, ktoré umožnia plynulý a bezproblémový prechod orgánov verejnej moci do digitálneho fakturačného prostredia.

Zoznam použitej literatúry

1. BEŇO, M. – KAČALJAK, M. – ORDA ORAVCOVÁ, A. – RICHTER, F. – SÁBO, J. – VARGAN, M.: Zákon o dani z pridanej hodnoty. Komentár. Bratislava : Wolters Kluwer SR, 2024, 884 s. ISBN 978-80-571-0688-3.
2. BERGER, W. – KINDL, C. – WAKOUNIG, M.: Smernice ES o dani z pridanej hodnoty. Praktický komentár. Praha : 1. VOX, 2010, 736 s. ISBN 978-80-86324-83-8.
3. DANCÁK, J.: Elektronická fakturácia a digitálne oznamovanie v kontexte smernice ViDA. In: Bulletin Slovenskej komory daňových poradcov. 2025, číslo 3, s. 10-18. ISSN 2644-688X.

4. Dôvodová správa k návrhu zákona, ktorým sa mení a dopĺňa zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Všeobecná časť [online] . Legislatívny proces č. LP/2025/396 [cit. 2025-09-15]. Dostupné na internete: <https://www.slovlex.sk/elegislativa/legislativne-procesy/SK/LP/2025/396/sprievodne-dokumenty?stadiumUuid=f5c7b0b3-059e-4bc8-afad-52ad5b1af5b9>
5. MERKX, M. – GRUSON, J. – VERBAAN, N. – VAN DER DOE, F.: VAT in the Digital Age Package: Viva La ViDA or Livin' La ViDA Loca? [online]. In: EC Tax Review, 2023, ročník 32, č. 3, s. 127-141 [cit. 2025-11-08]. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4437300
6. MERKX, M. – GRUSON, J. – VERBAAN, N. – VAN DER DOE, F.: VAT in the Digital Age package: Singling out the Single VAT Registration [online]. In: EC Tax Review, 2023, ročník 32, č. 4, s. 172-182 [cit. 2025-11-08]. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4504784
7. RICHTER, F.: Podvod na dani z pridanej hodnoty verzus trestný čin daňového podvodu. In: Bratislavské právnické fórum 2023 : aktuálne výzvy trestného práva. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, s. 322-331. ISBN 978-80-7160-696-3.
8. TERRA, B. – KAJUS, J.: A Guide to the European VAT Directives 2022. Volume 1: Introduction to European VAT. Amsterdam : IBFD, 2022, 1565 s. ISBN 978-90-8722-756-2.
9. Zoznam daňových subjektov registrovaných pre DPH [online] [cit. 2025-08-24]. Dostupné na internete: https://www.financnasprava.sk/sk/elektronicke-sluzby/verejne-sluzby/zoznamy/detail/_101c6128-e1f6-4a48-81ed-ad3c01220e03/?q=TV6nMSlnOdlaqGbaZ9Wr8l_EGpQVsaJ3iYUC8oFTyjdjMmWNBmJvDzPoJXCpnIEfMuMcIBfe6iiF_KmTfD4hZsBYWmiWoTO7lsz3KoFWD2dSEXghSchoif-Bwocxp1Rc6wbaA4neTSobzBgjSWC6CRS8ZGuCrmi6LWxwYfX1X-mSmc2bkhMorMvOyYbqrNoadKXG3olzBv8lCsvrl3FGkfPFQhoY=

Kontaktné údaje

JUDr. Filip Richter

richter20@uniba.sk

Katedra trestného práva, kriminológie a kriminalistiky

Univerzita Komenského v Bratislave

Právnická fakulta

MICA VS. PSD2: REGULAČNÝ PRIENIK A APLIKAČNÉ PROBLÉMY

MICA VS. PSD2: REGULATORY OVERLAP AND ENFORCEMENT CHALLENGES

Mária Potančoková¹

Abstrakt: Stanovisko Európskeho orgánu pre bankovníctvo (EBA) z júna 2025 k vzťahu medzi smernicou (EÚ) 2015/2366 o platobných službách (PSD2) a nariadením (EÚ) 2023/1114 o trhoch s kryptoaktívami (MiCA) otvára zásadné otázky (aj) pre správne trestanie v sektore finančného trhu. EBA odporúča, aby určité služby v oblasti kryptoaktív súvisiace s tokenmi elektronických peňazí (EMT) – najmä poskytovanie služieb prevodu kryptoaktív v mene klienta a úschova a správa kryptoaktív v mene klientov prostredníctvom úschovnej peňaženky – boli považované za platobné služby podľa PSD2, a teda podliehali povinnosti dodatočného povolenia na poskytovanie platobných služieb. Zároveň však EBA odporúča obmedziť uplatňovanie niektorých ustanovení PSD2 a navrhuje legislatívne riešenie buď v rámci pripravovanej smernice PSD3 a nariadenia o platobných službách (PSR), alebo prostredníctvom posilnenia MiCA.

Príspevok sa zameria na tento regulačný prienik z pohľadu slovenského finančného práva, najmä má za cieľ poukázať, že aktuálny stav prináša riziko dvojitej regulácie a nejasností pre právnu istotu adresátov, pričom v slovenskom prostredí bude Národná banka Slovenska zohrávať kľúčovú úlohu pri vyváženom výkone dohľadu a správneho trestania.

Kľúčové slová: MiCA. PSD2. tokeny elektronických peňazí (EMT). služby v oblasti kryptoaktív. platobné služby.

Abstract: The June 2025 Opinion of the European Banking Authority (EBA) on the interplay between Directive (EU) 2015/2366 on payment services (PSD2) and Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA) raises fundamental questions for administrative enforcement in the financial market sector. The EBA recommends that certain crypto-asset services related to e-money tokens (EMTs) – in particular the provision of transfer services of crypto-

¹ Univerzita Komenského v Bratislave, Právnická fakulta

assets on behalf of clients and the custody and administration of crypto-assets on behalf of clients through a custodial wallet – should be regarded as payment services under PSD2 and thus subject to an additional authorization requirement for the provision of payment services. At the same time, however, the EBA advises limiting the application of certain PSD2 provisions and proposes a legislative solution either within the forthcoming PSD3 and Payment Services Regulation (PSR), or through a strengthening of MiCA. The paper focuses on this regulatory overlap from the perspective of Slovak financial law and aims to demonstrate that the current framework creates the risk of double regulation and uncertainties for legal certainty of market participants, while in the Slovak context the National Bank of Slovakia will play a crucial role in ensuring a balanced approach to supervision and administrative enforcement.

Key words: MiCA. PSD2. EMTs. crypto-asset services. payment services.

Úvod

Regulácia finančného trhu v Európskej únii sa v poslednom desaťročí vyznačuje výraznou dynamikou, ktorá odráža nielen technologický pokrok, ale aj snahu zákonodarcu reagovať na nové riziká a potreby trhu. Jedným z najzásadnejších krokov je prijatie **nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1114 o trhoch s kryptoaktívami (ďalej v texte aj ako „MiCA“)**, ktoré nadobúda účinnosť v priebehu rokov 2024 a 2025². MiCA má ambíciu harmonizovať fragmentovanú právnu úpravu v oblasti kryptoaktív a vytvoriť jednotný európsky rámec pre poskytovanie súvisiacich služieb.

Popri tom však naďalej platí **smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 o platobných službách na vnútornom trhu (ďalej v texte aj ako „PSD2“)**, ktorá bola v Slovenskej republike transponovaná **zákonom č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej v texte aj ako „Zákon o platobných službách“)**³. PSD2 upravuje poskytovanie platobných služieb a udeľovanie povolení platobným inštitúciám a inštitúciám elektronických peňazí. Vzniká tak otázka, do akej miery sa tieto dva rámce – MiCA a PSD2 – môžu v praxi prekrývať a viesť k tzv. *dual licensing* efektu, teda povinnosti získať popri licencií podľa MiCA aj povolenie podľa PSD2.

² Nariadenie (EÚ) 2023/1114 (MiCA), Ú. v. EÚ L 150, 9. 6. 2023

³ Smernica (EÚ) 2015/2366 (PSD2), Ú. v. EÚ L 337, 23. 12. 2015; zákon č. 492/2009 Z. z. o platobných službách v znení neskorších predpisov

Dôležitú úlohu v tejto diskusii zohráva aj nedávne stanovisko **Európskeho orgánu pre bankovníctvo (ďalej v texte aj ako „EBA“)**. V júni 2025 EBA publikovala tzv. „No-Action Letter“, ktorým odporučila príslušným vnútroštátnym orgánom do marca 2026 nevymáhať požiadavku na povolenie podľa PSD2 pri určitých činnostiach súvisiacich s tokenmi elektronických peňazí (ďalej v texte aj ako „EMT“)⁴. Na prvý pohľad ide o pozitívny krok k zníženiu regulačného tlaku. Pri bližšom pohľade však vyvstáva otázka jeho účelnosti: obdobie do marca 2026 je čas, ktorý v praxi neumožňuje väčšine subjektov získať povolenie platobnej inštitúcie, keďže podľa skúseností EBA a praxe jednotlivých orgánov dohľadu proces povoľovania často presahuje jeden rok⁵. Toto „odkladné opatrenie“ tak v skutočnosti nerieši podstatu problému a prispieva k prehlbovaniu právnej neistoty.

Slovenská odborná literatúra sa doteraz problematike prieniku MiCA a PSD2 venovala len okrajovo. Je to prirodzené, keďže ide o novú tému a ešte neexistuje judikatúra ani ustálená doktrínálna interpretácia. Absencia vedeckých reflexií kladie zvýšené nároky na výklad právnych predpisov a vyžaduje metodologický prístup založený na právnej analýze, komparácii a kritickej reflexii.

Cieľom tohto článku je preto analyzovať regulačný prienik medzi MiCA a PSD2, identifikovať aplikačné problémy, ktoré môžu vzniknúť najmä v slovenskom právnom prostredí, a upozorniť na riziká pre právnu istotu dohliadaných subjektov. Zároveň článok poukazuje na špecifiká slovenského rámca, ktoré môžu viesť k disproporciám voči európskemu štandardu.

MiCA: základné východiská a regulačné ambície

Nariadenie (EÚ) 2023/1114 o trhoch s kryptoaktívami (MiCA) predstavuje prvý ucelený právny rámec Európskej únie, ktorý sa sústreďí na kryptoaktíva, ktoré dovtedy unikali jednotnej regulácii. Cieľom MiCA je odstrániť fragmentáciu právnej úpravy v členských štátoch a posilniť právnu istotu subjektov pôsobiacich na trhu. Ide o reakciu na prudký rozvoj krypto-ekosystému, ktorý sa dovtedy pohyboval na hrane medzi regulovanými finančnými nástrojmi (napr. cenné papiere podľa MiFID II⁶) a neregulovanými digitálnymi aktívami.

⁴ EBA, No-Action Letter on the interplay between PSD2 and MiCA, EBA/Op/2025/08

10. 6. 2025. dostupné: [https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-](https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bc0a28db7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf)

[bc0a28db7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf](https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bc0a28db7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf)

⁵ EBA, Peer Review Report on authorisation under PSD2, EBA/REP/2023/01

11. 1. 2023. dostupné:

https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1050744/Peer%20Review%20Report%20on%20authorisation%20under%20PSD2.pdf

⁶ Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ

MiCA má tri kľúčové ambície:

1. **Ochrana investorov a spotrebiteľov** – zvýšenie transparentnosti prostredníctvom povinných white papers pre emitentov a informačných povinností pre poskytovateľov služieb.
2. **Finančná stabilita** – zavedenie prísnejších pravidiel pre tzv. *stablecoiny*, t. j. asset-referenced tokens (ďalej v texte aj ako „ART“) a e-money tokens (EMT), ktoré môžu mať systémový význam pre platobný styk⁷.
3. **Jednotný trh** – harmonizácia podmienok pre poskytovanie služieb s kryptoaktívami (crypto-asset services) naprieč členskými štátmi, čím sa odstraňuje potreba viacnásobného povolenia v rôznych jurisdikciách.

MiCA zavádza licenčný režim pre **poskytovateľov služieb s kryptoaktívami (ďalej v texte aj ako „CASP“)**. Podľa čl. 3 ods. 1 bod (15) MiCA je „*crypto-asset service provider*“ (CASP) *a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59*⁸

Medzi regulované služby patrí najmä úschova a správa kryptoaktív, prevody kryptoaktív, prevádzka obchodných platforiem, výmena kryptoaktív za fiat meny alebo iné kryptoaktíva, prijímanie a vykonávanie pokynov klienta.

Každý CASP musí splniť (najmä, nie však výlučne) kapitálové požiadavky, zaviesť riadenie rizík, politiky AML/CFT⁹, systém ochrany klientskych aktív a zabezpečiť transparentnosť voči klientom. Mimoriadny dôraz sa kladie na **segregáciu aktív klientov od aktív samotného poskytovateľa**, čo má predchádzať stratám v prípade insolvenzie alebo zneužitia.

Najdiskutovanejšou časťou MiCA je úprava tzv. *stablecoinov*. MiCA v čl. 3 ods. 1 (6) definuje **asset-referenced token (ART)** ako „*a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies*“¹⁰. Naopak, čl. 3 ods. 1 (7) MiCA definuje **e-money token (EMT)** ako „*a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency*“.¹¹

Pre obe kategórie platia osobitné režimy: emitenti ART musia preukazovať rezervy a mechanizmy stabilizácie, zatiaľ čo emitenti EMT podliehajú režimu podobnému inštitúciám elektronickým peňazí. To vytvára priestor na prekryvy s PSD2, čo je jedna z najostrejších diskutovaných otázok.

⁷MiCA, časť III (ART), časť IV (EMT)

⁸ MiCA čl. 3 ods. 1 bod (15)

⁹ Ochrany pred praním špinavých peňazí a financovaním terorizmu

¹⁰ MiCA, čl. 3 ods. 1 bod (6)

¹¹ MiCA, čl. 3 ods. 1 bod (7)

Slovenský zákonodarca prijal **zákon č. 248/2024 Z. z. o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív a o zmene a doplnení niektorých zákonov**. Tento predpis plní dve úlohy:

1. vytvára procesnoprávny rámec pre udeľovanie povolení a dohľad zo strany Národnej banky Slovenska (NBS),
2. novelizuje súvisiace zákony, vrátane zákona č. 747/2004 Z. z. o dohľade nad finančným trhom, aby sa zabezpečilo efektívne sankčné konanie a dohľadová koordinácia.¹²

Slovenský trh s kryptoaktívami je relatívne menší, ale MiCA tu bude mať pre subjekty na ňom pôsobiace zásadný dopad. Kľúčovým prínosom je zavedenie licencie CASP, ktorá umožní poskytovateľom služieb využívať tzv. „passporting“ – teda pôsobiť po udelení povolenia v celej EÚ. Na druhej strane však vznikajú otázky, ako zosúladiť povinnosti CASP podľa MiCA s požiadavkami PSD2, najmä pri EMT, čo je hlavná téma tohto článku.

PSD2: účel, transpozícia a aplikačné výzvy

Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 o platobných službách na vnútornom trhu (PSD2) predstavuje základný právny rámec pre reguláciu platobných služieb v Európskej únii. Nahradila pôvodnú PSD1 z roku 2007 a reagovala na prudký rozvoj digitálnych platieb, internetového bankovníctva a nových fintech riešení. Cieľom PSD2 je posilniť integráciu trhu platobných služieb, zvýšiť úroveň ochrany spotrebiteľa a podporiť inováciu prostredníctvom otvoreného bankovníctva.

Čl. 4 bod 3 PSD2 definuje „**payment service**“ ako „*any business activity listed in Annex I*“¹³. Medzi tieto služby patrí vydávanie platobných nástrojov, prevod finančných prostriedkov, inkasá, správa platobných účtov a ďalšie kategórie.

Na národnej úrovni bol rámec PSD2 transponovaný **do zákona č. 492/2009 Z. z. o platobných službách**, ktorý v § 2 ods. 1 definuje „*platobnú službu*“ ako taxatívne vymenované činnosti.¹⁴

¹² Zákon č. 248/2024 Z. z. o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív a o zmene a doplnení niektorých zákonov

¹³ PSD2, čl. 4 bod 3; Annex I

¹⁴ § 2 ods. 1 Zákona o platobných službách: „*Platobnou službou sa rozumie*

a) *vkład finančných prostriedkov v hotovosti na platobný účet a vykonávanie všetkých úkonov súvisiacich s vedením platobného účtu,*

b) *výber finančných prostriedkov v hotovosti z platobného účtu a vykonávanie všetkých úkonov súvisiacich s vedením platobného účtu,*

c) *vykonávanie platobných operácií vrátane prevodu finančných prostriedkov z platobného účtu alebo na platobný účet vedený u poskytovateľa platobných služieb*

1. úhradou,

Zároveň tento zákon ustanovuje dohľad nad poskytovaním platobných služieb, ktorý vykonáva Národná banka Slovenska. Jednou z kľúčových otázok spojených s PSD2 je proces udeľovania povolení platobným inštitúciám a inštitúciám elektronických peňazí. Autorizácia vyžaduje najmä (nie však výlučne):

- preukázanie minimálneho počiatočného kapitálu (od 20 000 EUR pri niektorých službách po 125 000 EUR),
- detailný podnikateľský plán,
- vnútorné kontrolné mechanizmy a systém riadenia rizík,
- splnenie požiadaviek na odbornú spôsobilosť a bezúhonnosť členov štatutárnych orgánov (fit & proper test).¹⁵

Európsky orgán pre bankovníctvo (EBA) vydal 10. júna 2025 tzv. *No-Action Letter* vo forme „Opinion“ na základe žiadosti Európskej komisie z decembra 2024. Dokument vychádza z čl. 9c nariadenia (EÚ) č. 1093/2010 o zriadení EBA a jeho účelom bolo poskytnúť jednotné usmernenie vnútroštátnym orgánom dohľadu počas tzv. intervenčného obdobia pred účinnosťou PSD3/PSR.

EBA uvádza konkrétny zoznam činností, pri ktorých majú vnútroštátne orgány dohľadu uplatniť rámec PSD2:

- **Transfer EMT** ako platobná služba, „*where they entail EMTs and are carried out... on behalf of their clients*“¹⁶.
- **Custody and administration of EMTs** – správa a úschova sa majú chápať ako poskytovanie platobnej služby.
- **Custodial wallets** – ak sa vedú na meno klientov a umožňujú prijímať a posilať EMT tretím stranám, majú sa kvalifikovať ako **platobné účty** v zmysle PSD2.

2. prostredníctvom platobnej karty alebo iného platobného prostriedku,

3. inkasom,

d) vykonávanie platobných operácií z úveru poskytnutého používateľovi platobných služieb

1. formou povoleného prečerpania platobného účtu, a to

1a. úhradou,

1b. prostredníctvom platobnej karty alebo iného platobného prostriedku,

1c. inkasom, alebo

2. formou úverového rámca prostredníctvom platobnej karty alebo iného platobného prostriedku,

e) vydávanie platobného prostriedku alebo prijímanie platobných operácií,

f) poukazovanie peňazí,

g) platobná iniciálna služba,

h) služba informovania o platobnom účte“

¹⁵ PSD2, čl. 7 – kapitálové požiadavky; § 64 (2) Zákona o platobných službách

¹⁶ Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens. EBA/Op/2025/08. 10/06/2025. str. 1-2 Dostupné: <https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bcba0a28dbe7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf>

Týmto výkladom EBA fakticky subsumovala významnú časť CASP pod platobné služby, hoci ide o entity primárne licencované podľa MiCA. Na druhej strane EBA výslovne uviedla, že určité služby zostávajú výlučne pod MiCA a PSD2 sa na ne nevzťahuje:

- „exchange of crypto-assets for funds“ a „exchange of crypto-assets for other crypto-assets“ nie sú platobnými službami,
- ani prípady, keď CASP sprostredkuje nákup kryptoaktív s použitím EMT.

Toto vymedzenie je dôležité pre zachovanie rozdielu medzi „exchange“ funkciami CASP a skutočnými platobnými službami. Kľúčovým praktickým bodom je, že EBA odporučila, aby povinnosť mať PSD2 povolenie vznikla až od **marca 2026**:

„...grant applicants a transition period until 1 March 2026 before the authorisation needs to be held. After that date, NCAs are advised to prevent entities that are not licenced as a PSP or... partnered with a PSP, from providing EMT-related services that qualify as a payment service.“¹⁷

Dovtedy majú orgány dohľadu používať zjednodušené postupy autorizácie, pričom majú využiť informácie, ktoré CASP poskytl pri autorizácii podľa MiCA. Súčasne EBA umožňuje, aby sa CASP dočasne spoliehali na partnerstvá s existujúcimi poskytovateľmi platobných služieb. EBA zároveň poskytla detailné pokyny, ktoré ustanovenia PSD2 majú byť v tomto období „neprioritizované“:

- safeguarding podľa čl. 10 PSD2,
- informačné povinnosti o poplatkoch,
- maximálne lehoty na vykonanie platobnej transakcie,
- používanie jedinečného identifikátora (IBAN),
- požiadavky otvoreného bankovníctva (AISP, PISP).

Naopak, medzi ustanoveniami, ktoré sa majú plne uplatňovať, sú:

- strong customer authentication (SCA),
- fraud reporting
- vlastné zdroje (own funds) a ich kumulatívny výpočet.

EBA sama v závere konštatuje, že nejde o trvalo udržateľný stav a že povinnosť dvojitého povolení je nežiaduca. Problém prieniku MiCA a PSD2 možno teda zhrnúť ako **normatívny konflikt** medzi dvomi režimami:

MiCA – regulačný rámec pre kryptoaktíva, ktorý mal harmonizovať a zjednodušiť reguláciu.

PSD2 – regulačný rámec pre platobné služby, ktorý subsumuje aj EMT.

¹⁷ Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens. EBA/Op/2025/08. 10/06/2025. str. 2 Dostupné: <https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bcba0a28dbe7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf>

Aplikačné problémy na slovenskom trhu

Popri priamom uplatňovaní nariadení EÚ (napr. MiCA) existujú aj osobitné vnútroštátne zákony, ktoré implementujú alebo dopĺňajú európske predpisy. Vzájomná interakcia týchto noriem môže viesť k viacerým aplikačným problémom. Podľa Zákona o platobných službách je súčasťou povoľovacích procesov aj posudzovanie **odbornej spôsobilosti členov štatutárnych orgánov**. Konkrétne § 2 ods. 30 tohto zákona ustanovuje, že:

*„Odbornou spôsobilosťou sa na účely tohto zákona rozumie **ukončené vysokoškolské vzdelanie druhého stupňa a trojročné riadiace skúsenosti v oblasti poskytovania platobných služieb, bankovníctva alebo inej oblasti finančného trhu**. Za odborne spôsobilú osobu môže Národná banka Slovenska uznať aj*

a) fyzickú osobu, ktorá má ukončené vysokoškolské vzdelanie druhého stupňa a má trojročné riadiace skúsenosti v inej ekonomickej oblasti alebo
b) fyzickú osobu, ktorá má ukončené úplné stredné vzdelanie s maturitou a má sedemročnú prax v oblasti poskytovania platobných služieb, bankovníctva, v inej oblasti finančného trhu alebo v inej ekonomickej oblasti a najmenej trojročné riadiace skúsenosti v oblasti poskytovania platobných služieb, bankovníctva, v inej oblasti finančného trhu alebo v inej ekonomickej oblasti.“

MiCA v čl. 18 vyžaduje, aby členovia riadiaceho orgánu CASP boli mali „dostatočne dobrú povest“ a mali „primerané vedomosti, zručnosti a skúsenosti“ na výkon svojej funkcie, pričom sa hodnotí aj reálna schopnosť venovať výkonu funkcie dostatok času. Ide teda o princípovo formulovanú požiadavku, ktorá ponecháva vnútroštátnym orgánom dohľadu značnú mieru diskrečnej právomoci. Táto rozdielnosť vedie v praxi k potenciálnym kolíziám. Osoba, ktorá by spĺňala flexibilné kritériá MiCA (napr. špecialista na technológie distribuovanej databázy s dvojročnou praxou v sektore kryptoaktív), nemusí spĺňať rigidné slovenské požiadavky podľa Zákona o platobných službách. V prípade subjektov, ktoré budú súčasne potrebovať licenciu CASP podľa MiCA aj povolenie platobnej inštitúcie podľa PSD2 (resp. Zákona o platobných službách), to môže viesť k situácii, že rovnaký člen orgánu bude prijateľný v jednom licenčnom konaní, no neprijateľný v druhom. Tento rozpor oslabuje právnu istotu subjektov finančného trhu a vytvára tlak na zosúladenie vnútroštátnej legislatívy so zásadou proporcionality.

Osobitnú pozornosť si zaslúžia aj možné dôsledky v oblasti sankčného konania. Ak by sa určité činnosti poskytovateľov kryptoaktív považovali zároveň za služby regulované podľa MiCA aj podľa PSD2, vzniká reálne riziko, že orgán dohľadu bude viesť **dve samostatné sankčné konania** – jedno za porušenie povinností podľa MiCA a druhé podľa rámca platobných služieb. Takýto postup by mohol viesť k **duplicitnému postihu za rovnaké konanie**, čo je problematické z pohľadu zásady *ne bis in idem*.

Ďalšou oblasťou neistoty je skutočnosť, že EBA vo svojom No-Action Letter odporučila vnútroštátnym orgánom dohľadu „deprioritizovať“ **uplatňovanie niektorých povinností PSD2**, napríklad v oblasti open bankingu či niektorých informačných povinností. Na druhej strane však nie je jasné, či takéto odporúčanie EBA postačuje na zabezpečenie **riadnej právnej istoty** pre regulované subjekty. V praxi totiž platí, že kým legislatíva formálne zostáva v platnosti, subjekty musia počítať s tým, že dohľadový orgán môže – či už v budúcnosti alebo v konkrétnych prípadoch – rozhodnúť inak.

Právna istota je základným princípom európskeho finančného práva. V rozhodovacej praxi Súdneho dvora EÚ bola viackrát zdôraznená potreba jasnosti a predvídateľnosti právnych povinností adresátov práva¹⁸.

Odkladné opatrenie EBA do marca 2026 nie je dostatočné – nejde o systémové riešenie, iba o dočasné „pozastavenie“ vymáhania povinností. Keďže licenčné konania podľa PSD2 bežne trvajú viac než rok, väčšina subjektov nemá reálnu šancu povolenie získať včas, nehovoriac o rozdielnych formálnych podmienkach licenčného konania, tak, ako bolo opísané vyššie.

Záver

Diskusia o prieniku MiCA a PSD2 patrí medzi aktuálne otázky európskeho práva finančného trhu. MiCA mala priniesť harmonizáciu a jasný rámec pre trh s kryptoaktívami, no jej praktické uplatňovanie odhalilo prienik s existujúcou reguláciou platobných služieb. V oblasti EMT sa tieto dva režimy pretínajú takým spôsobom, že poskytovatelia môžu čeliť požiadavke dvojitej autorizácie, odlišným požiadavkám na odbornú spôsobilosť riadiaceho orgánu či riziku paralelných sankčných konaní.

EBA sa pokúsila reagovať prostredníctvom No-Action Letteru, ktorý dočasne zmiernuje tlak na subjekty trhu, no nerieši jadro problému. Výsledkom je predlžovanie obdobia právnej neistoty, ktorá oslabuje základný cieľ MiCA, a to vytvoriť jednotný a predvídateľný trh pre kryptoaktíva.

Záverom možno povedať, že ide o oblasť v štádiu formovania. Chýbajú skúsenosti z aplikačnej praxe, judikatúra aj metodické usmernenia. Tento článok preto nepredstavuje riešenie, ale príspevok do širšej diskusie, ktorá by mala prebiehať tak na akademickej úrovni, ako aj medzi regulátormi a účastníkmi trhu. Len otvorená odborná debata môže napomôcť tomu, aby sa regulácia kryptoaktív nestala prekážkou, ale skutočnou podporou ich rozvoja v Európskej únii.

¹⁸ Rozsudok Súdneho dvora EÚ vo veci C-17/03 *VEMW a i.*, bod 80

Zoznam použitej literatúry

1. Nariadenie (EÚ) 2023/1114 (MiCA), Ú. v. EÚ L 150, 9. 6. 2023
2. Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ
3. Smernica (EÚ) 2015/2366 (PSD2), Ú. v. EÚ L 337, 23. 12. 2015
4. EBA, No-Action Letter on the interplay between PSD2 and MiCA, EBA/Op/2025/08
10. 6. 2025. dostupné: <https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bcb0a28dbe7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf>
5. EBA, Peer Review Report on authorisation under PSD2, EBA/REP/2023/01
11. 1. 2023. dostupné: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1050744/Peer%20Review%20Report%20on%20authorisation%20under%20PSD2.pdf
6. Zákon č. 248/2024 Z. z. o niektorých povinnostiach a oprávneniach v oblasti kryptoaktív a o zmene a doplnení niektorých zákonov
7. Zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
8. Rozsudok Súdneho dvora EÚ vo veci C-17/03 *VEMW a i.* dostupné: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2005%3A362>

Kontaktné údaje

JUDr. Mária Potančoková
potancokova11@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

PRIENIK DIGITALIZÁCIE A KYBERNETICKEJ BEZPEČNOSTI V REGULAČNOM SANDBOXE

THE NEXUS OF DIGITALIZATION AND CYBERSECURITY WITHIN THE REGULATORY SANDBOX

Dávid Kis¹

Abstrakt: Príspevok sa komplexne zameriava na proces identifikácie a analýzy výskytu pojmov digitalizácia a kyberbezpečnosť v prostredí regulačných sandboxov, ktoré predstavujú moderný mechanizmus podpory inovácií v digitálnej ekonomike. Hlavným cieľom práce je presne definovať, ako a v akých kontextoch sa digitalizácia a kyberbezpečnosť objavujú a navzájom ovplyvňujú v rámci realizácie sandboxov, s dôrazom na ich reálny vplyv na trhové správanie, regulačné politiky a ochranu spotrebiteľov. Metodologický prístup vychádza z komparatívnej analýzy implementácií sandboxov vo vybraných jurisdikciách, pričom osobitná pozornosť je venovaná digitálnym procesom, automatizovanému spracovaniu údajov, využívaniu umelej inteligencie a aplikácii bezpečnostných opatrení. Príspevok analyzuje aj špecifické mechanizmy eliminácie rizík, možnosti dátovej ochrany či testovania nových štandardov kyberbezpečnosti v kontrolovanom prostredí sandboxu. Výsledky potvrdzujú schopnosť sandboxov efektívne identifikovať a riešiť digitálne aj bezpečnostné riziká a súčasne zdôrazňujú význam intenzívnej spolupráce medzi regulátormi a inovátormi pre optimalizáciu regulácie a nastavenie pružných pravidiel. Vedecký prínos práce spočíva v systematizácii poznatkov o fungovaní sandboxov a precizovaní ich úlohy pri formovaní moderných regulačných procesov. Praktické poznatky článku sú využiteľné pri navrhovaní konkrétnych postupov na znižovanie bariér vstupu na trh pre inovatívne podniky, podporu kyberbezpečnosti a ochrany spotrebiteľov v digitálnej ekonomike. Článok komparuje singapurský regulačný sandbox s britským.

Kľúčové slová: Regulačný sandbox, Digitalizácia, Kyberbezpečnosť, Inovácie, FinTech

Abstract: The paper comprehensively focuses on the process of identifying and analyzing the occurrence of the concepts of digitalization and cybersecurity within regulatory sandboxes, which represent a modern mechanism

¹ Právnická fakulta Univerzity Komenského v Bratislave, Katedra finančného práva.

supporting innovation in the digital economy. The main objective of the work is to precisely define how and in what contexts digitalization and cybersecurity appear and interact within the implementation of sandboxes, emphasizing their real impact on market behavior, regulatory policies, and consumer protection. The methodological approach is based on a comparative analysis of sandbox implementations in selected jurisdictions, with particular attention to digital processes, automated data processing, the use of artificial intelligence, and the application of security measures. The paper also analyzes specific mechanisms for risk elimination, options for data protection, and testing of new cybersecurity standards within the controlled environment of the sandbox. The results confirm the ability of sandboxes to effectively identify and address digital and security risks, while highlighting the importance of intensive cooperation between regulators and innovators for optimizing regulation and setting flexible rules. The scientific contribution of the work lies in the systematization of knowledge about the functioning of sandboxes and refining their role in shaping modern regulatory processes. The practical insights of the article are applicable in designing specific procedures to reduce market entry barriers for innovative enterprises, supporting cybersecurity, and protecting consumers in the digital economy. The article compares Singapore's regulatory sandbox with British.

Key words: Regulatory sandbox, Digitalization, Cybersecurity, Innovation, FinTech

Úvod

V súčasnej dobe sa svet ekonomiky a podnikania nachádza v období výrazných transformácií, ktoré sú úzko späté so zrýchlenou digitalizáciou a rozvojom nových technológií. Tento dopyt po inováciách kladie zvýšené nároky na regulačné mechanizmy, ktoré majú za úlohu zabezpečiť rovnováhu medzi podporou technologického pokroku a ochranou spotrebiteľov či stability trhu. Regulácia sa tak musí prispôbovať dynamike trhu a novým formám podnikania, ktoré menia nielen obchodné modely, ale často aj celé odvetvia.

Jedným z nástrojov, ktorý sa v tomto kontexte objavil ako inováčná a flexibilná odpoveď na tieto výzvy je regulačný sandbox. Jeho význam spočíva v tom, že poskytuje podnikateľským subjektom možnosť testovať svoje nové produkty, služby alebo obchodné modely v reálnych podmienkach trhu, a to za príspevku a dohľadu regulátora, pričom im dočasne uľahčuje niektoré regulačné povinnosti. Takéto prostredie umožňuje rýchlejšie zavedenie inovácií bez toho, aby bolo ohrozené právo

spotrebiteľa na ochranu alebo stabilita trhového prostredia. Tento článok sleduje uvedené aspekty v kontexte finančného trhu.

Prínosy, ktoré tento inštitút prináša, sú mnohostranné. Po prvé, významne znižuje vstupné bariéry pre malé a stredné inovatívne firmy a startupy, ktoré by inak mohli čeliť zložitým a nákladným regulačným požiadavkám. Po druhé, umožňuje oveľa rýchlejšiu iteráciu a zlepšovanie produktov na základe spätnej väzby zo samotného trhu a správania sa reálnych spotrebiteľov. Tým sa podporuje konkurencieschopnosť a dynamika v sektore, ktorá je kľúčová pre udržateľný rozvoj.

Regulačný sandbox zároveň podporuje vzájomné učenie sa – na jednej strane inovátori získavajú cenné poznatky o regulačnom rámci, v ktorom pôsobia, a na druhej strane regulátori lepšie chápu mechanizmy nových technológií a trhových modelov. Tento dialóg následne vedie k možnosti úpravy legislatívnych rámcov tak, aby boli efektívnejšie a zároveň rešpektovali potrebu bezpečnosti a ochrany spotrebiteľov.

Okrem toho, v oblasti digitálnych technológií, kde riziká kybernetických útokov a zneužívania dát rastú, sa regulačné sandboxy stávajú dôležitou platformou na testovanie a zavádzanie opatrení kyberbezpečnosti, nakoľko pomáhajú anticipovať potenciálne hrozby a zároveň podporujú vznik nových bezpečnostných štandardov v digitálnom priestore.

V širšom meradle teda možno regulačné sandboxy vnímať ako kľúčový mechanizmus modernej regulácie, ktorý reflektuje potrebu pružnej a zároveň zodpovednej adaptácie regulačných prístupov na nové výzvy digitálnej ekonomiky a podnikania. Význam sandboxov presahuje rámec jednotlivých právnych odvetví, nakoľko prispievajú až k budovaniu celospoločenských podmienok pre bezpečné a udržateľné využívanie inovácií v prospech trhu aj spotrebiteľov.

Hypotézou tohto článku je, že : „*Regulačný sandbox predstavuje efektívny nástroj na podporu inovácií v digitálnej ekonomike, ktorý zároveň zabezpečuje primeranú ochranu spotrebiteľov a stabilitu trhu prostredníctvom vyváženej a adaptívnej regulácie na finančnom trhu.*“ V článku využívame metódy komparácie, analýzy, syntézy. Na verifikáciu tejto hypotézy sme zvolili komparáciu singapurského a britského regulačného sandboxu nakoľko sú protikladmi. V článku vysvetľujeme aj jednotlivé odlišnosti vybraných sandboxov.

Regulačný sandbox ako pojem FinTech inovácií

Regulačný sandbox alebo aj regulačné pieskovisko predstavuje nástroj regulátora alebo orgánu vykonávajúceho dohľad nad finančným trhom, ktorý umožňuje podnikateľským subjektom testovať ich inovácie alebo inovatívne modely podnikania bez nutnosti splnenia platných regulačných požiadaviek, ktoré by sa na nich inak vzťahovali. Regulačnými požiadavkami myslíme platné a účinné právo,

v súlade s ktorým by mohli tieto subjekty inak vykonávať podnikateľskú činnosť na tom ktorom finančnom trhu v národných podmienkach, alternatívne aj v nadnárodných podmienkach. Medzi najbežnejšie regulačné požiadavky patrí potreba udelenia licencie na výkon danej podnikateľskej činnosti. Takáto výnimka z platnej legislatívy nie je nekončiaca a vo väčšine prípadov zaniká v momente skončenia takzvaného testovacieho štádia, ktoré môže nastať fakticky a to tak, že je overená možnosť vstupu inovácie alebo inovatívneho podnikateľského modelu na trh alebo skončením dovolenej doby participácie v sandboxe. V oboch prípadoch sa následne už vyžaduje súlad danej inovácie s platnou legislatívou, ak má inovátor záujem o vstup na trh alebo môže alternatívne upustiť od tohto zámeru napríklad z dôvodu zistenia, že poskytovanie inovatívnych služieb by pre neho nebolo lukratívne. Dôvody sa však môžu líšiť, samozrejme nami opísaná exempcia z platnej legislatívy je zovšeobecnením reálneho fungovania benefitov, ktoré čerpá participant v sandboxe a jednotlivé formy benefitu alebo exempcií sa líšia v závislosti od toho ktorého sandboxu, avšak hlbšia analýza daného javu nie je predmetom tohto článku.²

Prvým štátom, ktorý takýto regulačný sandbox zaviedol bolo Spojené kráľovstvo (ďalej len „UK“) a regulátorom v tomto prípade bola Financial Conduct Authority (ďalej len „FCA“). Tento štát sme zvolili nakoľko predstavuje takzvaný prvý model fungovania sandboxu a všetky následné modely sandboxov sú len akýmsi derivátom tohto FCA modelu. V prípade UK je regulačný sandbox poňatý ako bezpečný priestor, v ktorom môžu podniky testovať ich inovatívne produkty, služby, podnikateľské modely a formy poskytovania služieb bez okamžitej nutnosti spĺňať inak platné požiadavky na danú činnosť. Tento model by sa teda dal označiť za regulačný sandbox spočívajúci v čerpaní výnimky z inak platnej legislatívy, pričom dôležitá je tu dočasnosť. Za tri kľúčové úlohy tohto sandboxu označuje FCA skrátenie času, ktorý je potrebný pre uvedenie na trh, vylepšenie možnosti financovania a poslednou úlohou je podpora inovácií. Okrem týchto úloh vieme vyčítať obdobne dôležité znaky aj v samotnom procese posudzovania prihlášok do tohto sandboxu. Demonštratívne sme zvolili podporu domácej ekonomiky, ochranu stability finančného trhu a podporu a ochranu spotrebiteľov. Sumár týchto úloh alebo aj znakov sandboxu nám dáva pomerne jasný obraz a celkovom poslaní regulačných sandboxov. Ich poslaním nie je bezhlavá podpora akejkoľvek inovácie, podporené sú len inovácie určené pre trh danej krajiny, ktoré budú benefitom pre daný trh aj spotrebiteľov, pričom platí že celkovo musí byť inovácia bezpečná. Bezpečnosť preukáže daný

² BROMBERG, Lev – GODWIN, Andrew – RAMSAY, Ian: Fintech Sandboxes: Achieving a Balance between Regulation and Innovation. In: SSRN Electronic Journal [online]. 2017. S.4-6. Dostupné na internete:

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3090844_code178811.pdf?abstractid=3090844&mirid=1

participant vtedy, ak výhody prevážia potenciálne hrozby v prípade, že by danej inovácii bol umožnený vstup na trh.³

V prípade FCA modelu sandboxu je prameňom kreovania tohto sandboxu *Financial Services and Markets Act* z roku 2000, ktorý splnomocňuje FCA aby vykonávala kroky smerujúce k zaisteniu ochrany spotrebiteľa, ochrany integrity trhu a zabezpečeniu konkurencieschopnosti domácej ekonomiky. Tieto tri body predstavujú takzvané operačné ciele vymedzené v kapitole 1 časť 1B odsek 3 písmená a až c. Okrem operačných cieľov pozná zákon aj strategické ciele vymedzené v rovnakej časti v odseku 2, kde je vymedzené, že týmto strategickým cieľom je zabezpečenie správneho fungovania relevantných trhov, v našom prípade finančného trhu. V rovnakej časti odseku 1 je vymedzený príkaz, že FCA musí konať spôsobom, ktorý je kompatibilný s jej strategickým cieľom a súčasne posúva jeden alebo viac jej operačných cieľov vpred.⁴

Následne s využitím vyššie uvedenej kompetencie za účelom plnenia predmetných cieľov FCA na svojom webovom sídle komplexne vymedzila fungovanie FCA regulačného sandboxu⁵ a zároveň vypracovala aj dokument pod názvom *FCA regulatory sandbox guide*.⁶

Vo všeobecnosti je úlohou regulačných sandboxov umožnenie záujemcom z daného trhu otestovať FinTech služby na reálnom trhu so skutočnými spotrebiteľmi, avšak pod prísny dohľad regulátora. Implicitne je pomerne dôležitý aj aspekt takzvaného vzájomného učenia sa. Ten v praxi znamená, že sa na strane inovátora odstraňuje informačná asymetria, spočívajúca v prirodzenom stave, že logicky subjekt finančného trhu nebude disponovať rovnakým množstvom a kvalitou informácií ako regulátor, ktorý je na čele trhu a vykonáva dohľad. Na druhej strane sa odstraňuje informačná asymetria v tej rovine, že sa zároveň aj regulátor učí o novej inovácii, ktorá má potenciál vstúpiť na trh. Následkom tohto učenia môže byť zmena legislatívy, ktorá sa môže vplyvom informovanosti zmierniť alebo sprísniť. V praktickej rovine môže teda regulátor dospieť k záveru, že v prípade predmetnej inovácie sú riziká väčšie ako potenciálne benefity pre trh aj spotrebiteľov, a vykoná tak apel na zákonodarcu výsledkom čoho bude legislatíva, ktorá do budúca

³ ARNER, Douglas W. – BARBERIS, Janos – BUCKLEY, Ross P.: *FinTech and RegTech in a nutshell, and the future in a sandbox*. [s.l.]: CFA Institute Research Foundation, 2017. S. 16-17. Dostupné na internete:

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3088303_code468680.pdf?abstractid=3088303

⁴ *Financial Services and Markets Act 2000*. Chapter 8. UK Public General Acts. 2000. Dostupné na internete: <https://www.legislation.gov.uk/ukpga/2000/8/part/1A/chapter/1>

⁵ Financial Conduct Authority. *Regulatory Sandbox*. [online]. Dostupné na internete: <https://www.fca.org.uk/firm...ox>

⁶ *FCA Regulatory Sandbox Guide*. In: Financial Conduct Authority [online]. 2022. Dostupné na internete: [fca-regulatory-sandbox-guide.pdf](https://www.fca.org.uk/regulatory-sandbox-guide.pdf)

neumožní vstup takýmto inováciám na finančný trh. Opakom môže byť situácia, kedy regulátor posúdi inováciu ako dostatočne pozitívnu a odobrí jej vstup na trh, následkom čoho sa prispôsobí legislatíva tak, aby podporila túto, ako aj obdobné inovácie, pretože nevykazujú žiadnu hrozbu, a teda sú hodnotené ako bezpečné pre spotrebiteľov aj stabilitu trhu.⁷

Napriek tomu, že by sa mohlo zdať, že takýto právny režim, ktorý so sebou nesie riziko umožnenia vstupu nebezpečnej hrozby na finančný trh bude len akousi dočasnou záležitosťou, dáta odôvodňujú opačný záver. Konkrétne nami uvedený regulačný sandbox v podmienkach UK vznikol v roku 2015 a za nasledovných 10 rokov sa nielenže postupnou modifikáciou dostal do právneho poriadku takmer v každej jurisdikcii ale zároveň sa trh posunul o ďalší krok vpred a bolo iniciované vytvorenie nadnárodných regulačných sandboxov, v prípade ktorých by vznik inovácií nerozoznával štátne hranice a každá jedna inovácia by mohla byť prínosná pre medzinárodné spoločenstvo. Tento krok je označovaný rôznymi autormi za globalizačnú reguláciu alebo aj regulačný kapitalizmus, v podmienkach ktorého sa regulačné normy, modely a hodnoty šíria hranicami rôznych jurisdikcií prostredníctvom rôznych mechanizmov. Takéto iniciatívy vznikli najprv v menšom rozsahu, teda formou spolupráce susediacich štátov a následne sa rozšírili na prakticky globálne meritum.⁸

Digitalizácia a kyberbezpečnosť v podmienkach regulačných sandboxov

V predchádzajúcej kapitole sme naznačili, že regulačný sandbox predstavuje súčasť FinTech inovácií, teda je nástrojom, ktorý umožňuje kreovanie a testovanie iných inovácií v oblasti finančných technológií. FinTech je hybnou silou, ktorá rapídne mení svet financií, čím dochádza k vývoju finančného trhu. K napredovaniu by nedochádzalo takouto rýchlosťou, ak by súčasťou FinTech nebol aj presun do digitálneho sveta. Pod záštitou tejto metamorfózy do digitálneho sveta sa neustále posilňuje aj význam kyberbezpečnosti, nakoľko čím jednoduchší je prístup k osobným údajom, platobným údajom a podobne, tak tým viac narastá možnosť

⁷ RINGE, Wolf-Georg – RUOF, Christopher: Regulating Fintech in the EU: the Case for a Guided Sandbox. In: European Journal of Risk Regulation [online]. 2020, vol. 11, no. 3, s. 605. Dostupné na internete:

<https://www.cambridge.org/core/services/aop-cambridge-core/content/view/3EE71CEEBC22E57A1BF08023073A6F/S1867299X20000082a.pdf/div-class-title-regulating-fintech-in-the-eu-the-case-for-a-guided-sandbox-div.pdf>

⁸ JOHNSON, Walter G.: Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. In: Regulation & Governance [online]. 2022, vol. 17, no. 3, s. 709. Dostupné na internete: <https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/rego.12487>

zneužitia v dôsledku kybernetického útoku.⁹ Pre lepšiu predstavu uvádzame, že v prvej polovici roku 2025 v dôsledku podvodov v súvislosti s kryptomenami prišli investori súhrne o 3,1 miliardy amerických dolárov. Význam digitalizácie podporenej dostatočne silnými kyberopatreniami by mal byť podčiarknutý samotnou skutočnosťou, že v digitálnom prostredí vzniká potenciál na rádovo vyššie škody než v reálnom fyzickom svete, čo je spôsobené digitalizáciou financií.¹⁰

Okrem vyššie uvedených foriem digitalizácie sa regulačných sandboxov dotýkajú aj mnohé iné iniciatívy. Na účely demonštrácie dopadov digitalizácie sme zvolili iniciatívu *Smart city* v Singapure z roku 2014. Táto iniciatíva predstavuje okrem iného masívne inkorporovanie umelej inteligencie do rozhodovacích procesov. Pre nás je obzvlášť zaujímavý podprogram tejto iniciatívy, a to digitálna ekonomika a jej rozšírenie vo forme *digital government*. Tieto podprogramy viedli priamo ku kreovaniu singapurského FinTech regulačného sandboxu, ktorý je považovaný za jeden z najúspešnejších na svete.¹¹ Singapurský FinTech regulačný sandbox sme zvolili za účelom značného kontrastu medzi ním a takzvaným FCA modelom, nakoľko singapurský model síce predstavuje derivát modelu FCA ale je jeho vylepšenou verziou, ktorá dosiahla celosvetové uznanie a označuje sa superlatívom „najúspešnejší“ sandbox.

Právnym základom kreovania singapurského sandboxu je *Monetary Authority of Singapore Act (Cap. 186)* z roku 1970, ktorý vo svojej druhej časti odseku 4 s názvom kľúčové úlohy a funkcie Authority (autoritou sa rozumie Monetary Authority of Singapore, tento pojem je skrátenejší v prvej časti zákona) v bode 1 písmeno d hovorí, že kľúčovým poslaním Monetary Authority of Singapore (ďalej len „MAS“) je podporovať Singapur ako medzinárodne konkurencieschopné finančné centrum.¹² V súlade s touto úlohou MAS vytvorilo *Fintech regulatory sandbox guidelines*, ktoré ako podzákonný predpis komplexne upravuje fungovanie singapurského regulačného sandboxu.¹³

⁹ KAMUANGU, Paulin K.: A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends. In: Journal of Economics, Finance and Accounting Studies [online]. 2024, vol. 6, no. 1, s. 47-53. Dostupné na internete: <https://al-kindipublishers.org/index.php/jefas/article/view/6768>

¹⁰ LEDGER: The state of crypto scams in 2025. In: Ledger [online]. Dostupné na internete: <https://www.ledger.com/academy/topics/security/the-state-of-crypto-scams-in-2025>

¹¹ TENG, Huei-Wen et al.: Mitigating digital asset risks. In: SSRN Electronic Journal [online]. 2023, s. 69. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4594467

¹² Monetary Authority of Singapore Act 1970. Chapter 186. Singapore Statutes Online. Dostupné na internete: <https://sso.agc.gov.sg/Act/MASA1970?Provs=P12-#pr4->

¹³ Monetary Authority of Singapore. FinTech Regulatory Guidelines. November 2016. Dostupné na internete:

https://www.rajahtannasia.com/~media/Files/Asia%20Pacific%20Publications/2016/MAS_Fintech_RegulatorySandbox_Guidelines.pdf

Pre zdôraznenie dodávame, že integrovanie umelej inteligencie do rozhodovacích procesov v podmienkach regulačného sandboxu nepredstavuje prejav čisto digitalizácie. V tomto prípade ide už o vyšší vývojový stupeň, ktorý prevyšuje bežný FinTech regulačný sandbox, a teda sa jedná o nadradený regulačný sandbox, ktorý ponúka odlišné možnosti a nástroje na rozdiel od bežného sandboxu.¹⁴

Ako sme uviedli, digitalizácia sa prejavuje v plnom rozsahu v prípade singapurského sandboxu. Možno ju vnímať od počiatočného štádia podania žiadosti, kedy primárne vyhodnotenie inovácie vykonáva umelá inteligencia a priamo eliminuje prihlášky, pri ktorých by bolo možné riziko v prípade vstupu na trh. V tejto rovine sa digitalizáciou myslí forma realizácie sandboxu, teda konkrétne, že sú v ňom integrované digitálne a elektronické procesy bez nutnosti fyzických konzultácií, stretnutí a podobne. V tomto zmysle môže byť sandbox fyzický, digitálny alebo zmes oboch. Singapurský sandbox by sme teda zaradili pod čisto digitálny.¹⁵ Okrem toho sa digitalizácia prejavuje v rovine urýchlenia celého procesu, nakoľko je deklarované, že záujemcova prihláška bude vyhodnotená v priebehu 21 pracovných dní.¹⁶ Digitalizácia sa prejavuje aj po zaradení inovácie do regulačného sandboxu v administratívnom odbremenení a v zrýchlení celého procesu, čo má za pozitívny následok aj skvalitnenie samotného testovania danej inovácie, nakoľko sa participant, teda inovátor, môže plne venovať testovaniu životaschopnosti svojej inovácie v reálnych trhových podmienkach. Pozitívum digitálnosti v tomto prípade možno vnímať aj v možnosti investovania do úkonov, ktoré majú potenciál prispieť k rozvoju danej inovácie. Participant teda nemusí investovať do materiálneho zabezpečenia, ktoré by sa inak vyžadovalo hoci by nijak nepomohlo v procese verifikácie toho, či by inovácia skutočne mala potenciál byť prínosnou.¹⁷

Protiváhou tohto pomerne liberálneho sandboxu je skutočnosť, že na rozdiel od britského sandboxu sa participantovi neposkytuje akási imunita od nežiadúcich následkov. V prípade Británie sa tým myslí poskytnutie možnosti procesnej ochrany, kedy sa spotrebiteľ nemôže domáhať ochrany svojho nároku v prípade, ak druhá strana participovala v sandboxe (toto sa nazýva aj no-action letter). Singapurský

¹⁴ QIU, Yingpeng – YAO, Han – REN, Ping – TIAN, Xueqing – YOU, Mao: Regulatory sandbox expansion: Exploring the leap from fintech to medical artificial intelligence. In: Health Policy and Technology [online]. 2025, s. 121. Dostupné na internete: <https://www.sciencedirect.com/science/article/pii/S2950261625000202>

¹⁵ NOVELLI, Claudio – HACKER, Philipp – MCDUGALL, Simon – MORLEY, Jessica – ROTOLO, Antonino – FLORIDI, Luciano: Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act. In: SSRN Electronic Journal [online]. 2025, s. 3. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5332161

¹⁶ ACCLIME: Singapore's Fintech Regulatory Sandbox and Incentives. In: Acclime [online]. Dostupné na internete: <https://singapore.acclime.com/guides/fintech-sandbox-incentives/#part1>

¹⁷ ACCLIME: Singapore's Fintech Regulatory Sandbox and Incentives. In: Acclime [online]. Dostupné na internete: <https://singapore.acclime.com/guides/fintech-sandbox-incentives/#part1>

sandbox poskytuje len možnosť zníženia kapitálových požiadaviek. V prípade ak sa vyžaduje napríklad základné imanie alebo iné poplatky, teda v pravom slova zmysle nemôžeme hovoriť o čerpaní exempcie z platnej legislatívy iba o akomsi benefite vo forme znížených kapitálových požiadaviek na inovátora.¹⁸

Prienik digitalizácie samozrejme nie je raritou v podmienkach sandboxov. Regulačné sandboxy sú označované pomerne bežne aj za experimentálne režimy na kreovanie digitálnych inovácií. Vstup do regulačného sandboxu nie je predeterminovaný formou v akej inovácia vznikla. Môže sa jednať aj o digitálne inovácie, ktoré však nepredstavujú raritnú formu, nakoľko väčšina inovácií existuje práve v tejto podobe a sú určené na digitálne používanie.¹⁹ Digitálne inovácie ako také priamo obsahujú nutnosť existencie miernejších pravidiel v podmienkach, kedy by prísna regulácia predstavovala odstrašenie od aplikácie nových technológií na finančnom alebo aj akomkoľvek inom trhu. Zároveň by to malo za následok neprimerané spomalenie rozvoja týchto sektorov. Kľúčovým poslaním sandboxov je teda skĺbenie digitálnych inovácií s ochranou spotrebiteľov a trhu.²⁰

Jednou z kritik digitalizácie v tomto kontexte je aj takzvané *zmyývanie rizík*, ktoré hovorí o tom, že aj napriek objektívnej skutočnosti, že riziká mnohokrát prevážia reálne benefity sandboxu, tak vďaka akejsi selektívnej slepote zastávame názor, že je sandbox bezrizikový. Zástancovia tohto postoja tvrdia, že digitalizácia procesov spojených s rozhodovaním v procese participácie v sandboxe môže mať za následok oslabenie sociálnych väzieb, ktoré by inak mohli zmeniť priebeh participácie. Jedná sa teda o akési odosobnenie, kedy úradník vykonávajúci dohľad neberie ohľad na osoby participujúce v sandboxe ale vníma ich iba ako akési dáta. Taktiež sa uvádza, že tento jav následne smeruje k nerovnomernej a nepriaznivej redistribúcii bohatstva. Rovnako môže viesť digitalizácia k narušeniu súkromia, k narušeniu bežnej rozhodovacej praxe a v konečnom dôsledku môže podryvať dôveru verejnosti

¹⁸ CHEN, Christopher: Regulatory Sandbox and InsurTech: A Preliminary Survey in Selected Countries. In: SSRN Electronic Journal [online]. 2018, s. 10. Dostupné na internete: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3275929_code1582025.pdf?abstractid=3275929&mirid=1

¹⁹ GROMOVA, Elizaveta A. – KONEVA, Natalia S. – TITOVA, Elena V.: Legal barriers to the implementation of digital industry (Industry 4.0) components and ways to overcome them. In: The Journal of World Intellectual Property [online]. S. 198. Dostupné na internete: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/jwip.12215?msocid=2037eboe892d65173eefff5988e664a7>

²⁰ BOLDINI, Marco: A New Strategic Approach Towards Financial Regulation: A Comparative Overview of the English and Italian Legal System between Regulatory Needs and Technology Innovations. In: Bratislava Law Review [online]. 2022, roč. 6, č. 2, s. 11. Dostupné na internete: <https://blr.flaw.uniba.sk/index.php/BLR/article/view/276>

v rozhodovacie procesy vo verejnej správe.²¹ Pripúšťame možnosť vzniku skepticizmu vo vzťahu k zavedeniu digitalizácie v značnej miere, avšak uvedené negatíva podľa nášho názoru skôr prispievajú k objektivizovaniu rozhodovacích procesov. Tým myslíme, že úlohou regulačného sandboxu nie je vytvorenie sociálnych väzieb medzi regulátorom a inovátorom, úlohou sandboxu je rýdze overenie dát a životaschopnosti inovácie.²²

K téme zberu a vyhodnocovania dát uvádzame, že pre regulátorov je nevyhnutné mať kvalitné dáta, pretože nesprávne alebo skreslené vstupy vedú k nespoľahlivým výsledkom („garbage in, garbage out“). Pri strojovom učení môžu zle označené alebo zmanipulované dáta spôsobiť chybné rozhodnutia. Aj keď technológie ako automatizované reportovanie znižujú ľudský zásah, stále hrozí možné obídenie systému. Regulátori by preto mali využívať špecificky vyvinuté riešenia a byť pri zavádzaní nových technológií ostražití. Nedostatok dát či ich limitácie tiež obmedzujú efektívnosť týchto systémov, najmä pri predikcii výnimočných udalostí. Preto je dôležité zbierať čo najkomplexnejšie dáta a v opačnom prípade zvážiť samotné použitie technológií.²³

Teda súhrnne môžeme v kontexte digitalizácie konštatovať, že regulačný sandbox predstavuje moderný inštitucionálny koncept, ktorý reflektuje digitalizáciu ako jeden z fundamentálnych spoločenských a ekonomických fenoménov súčasnosti. Jeho kľúčovým cieľom je vytváranie kontrolovaného experimentálneho prostredia, v ktorom je možné overovať digitálne inovácie v podmienkach nedostatočnej alebo absentujúcej tradičnej regulácie. V tomto kontexte sandbox slúži nielen ako akceleračný digitálnych procesov, ale zároveň podporuje transformáciu hospodárskych a spoločenských štruktúr prostredníctvom digitálnych technológií.²⁴ Kyberbezpečnosť možno vnímať rôznymi optikami v podmienkach sandboxov, obdobne ako aj digitalizáciu. Jednu z možností sme už naznačili v predchádzajúcom texte. Túto možnosť by sme označili ako možnosť vzniku kybernetických hrozieb

²¹ MARKELOS, Raphael N. – ENNIS, Sean F. – ENSTONE, Bryn – MANOS, Anastasios – PAZAITIS, Dimitrios – PSYCHOYIOS, Dimitrios: Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies. In: SSRN Electronic Journal [online]. 2024, s. 7. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4764911

²² MARKELOS, Raphael N. – ENNIS, Sean F. – ENSTONE, Bryn – MANOS, Anastasios – PAZAITIS, Dimitrios – PSYCHOYIOS, Dimitrios: Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies. In: SSRN Electronic Journal [online]. 2024, s. 7. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4764911

²³ GELŽINYTĖ, Virginija: Digitalisation of Financial Regulators as a Condition for Smarter Regulation and Supervision of the Market. Master's Thesis. Law School International Business Law LLM, Comenius University, 2019. s.29. Dostupné na internete: <https://arno.uvt.nl/show.cgi?fid=149407>

²⁴ SEFERI, Fabio: A working experimentation model for cyber resilience regulatory sandboxes. In: CEUR Workshop Proceedings [online]. 2025, s. 4-6. Dostupné na internete: <https://ceur-ws.org/Vol-3962/paper67.pdf>

vplyvom umožnenia vstupu na trh nebezpečnej inovácie.²⁵ Táto prvá možnosť predstavuje risk, ktorého predchádzanie by malo byť jednou z úloh funkčného sandboxu za účelom ochrany spotrebiteľov a trhu. Druhá alternatíva smeruje priamo k naplneniu tejto úlohy, a ak by sme ju mali pomenovať, išlo by o kreovanie nových spôsobov zabezpečovania kyberbezpečnosti a predchádzanie takýmto hrozbám. Opäť ako sme už uviedli, toto by malo byť integrované do každého jedného sandboxu, aby takéto riziká nevznikali, avšak to je častokrát nemožné, nakoľko technológie napredujú rapídny tempom. Riešením je kreovanie sandboxov na testovanie inovácií v oblasti kyberbezpečnosti.²⁶

Sandbox zameraný na ochranu dát nepredstavuje náš návrh *de lege ferenda*. Pojednávame o konkrétnom sandboxe v podmienkach UK, ktorý vznikol za účelom kreovania spôsobov na ochranu osobných údajov, konkrétne hlasová biometria, technológie na rekogníciu tváre a iné.²⁷ Regulátorom v tomto prípade je The Information Commissioner's Office, ktorý je poverený ochranou osobných údajov v podmienkach UK.²⁸

Záver

V tomto príspevku sme sa snažili potvrdiť hypotézu „Regulačný sandbox predstavuje efektívny nástroj na podporu inovácií v digitálnej ekonomike, ktorý zároveň zabezpečuje primeranú ochranu spotrebiteľov a stabilitu trhu prostredníctvom vyváženej a adaptívnej regulácie na finančnom trhu.“

Na základe dostupných poznatkov a skúseností z implementácie regulačných sandboxov, napríklad vo Veľkej Británii či Singapore, je možné túto hypotézu považovať za potvrdenú. Regulačné sandboxy umožňujú spoločnostiam testovať inovatívne riešenia rýchlo a bezpečne, regulátorom poskytujú cenné poznatky pre formovanie legislatívy a zároveň prispievajú k znižovaniu regulačných bariér bez vážneho ohrozenia ochrany spotrebiteľov či stability trhu. Napriek určitým rizikám, ako sú obavy z „risk washing“ alebo manipulácie dátami, fungovanie a vývoj

²⁵ GUMBO, Lilian – CHUDE-OKONKWO, Uche A. K.: Regulatory sandbox as a frontier for innovation and sustainability: a systematic review. In: Cogent Business & Management [online]. 2025, vol. 12, no. 1, s. 8. Dostupné na internete: <https://www.tandfonline.com/doi/full/10.1080/23311975.2025.25105550>

²⁶ TENG, Huei-Wen et al.: Mitigating digital asset risks. In: SSRN Electronic Journal [online]. 2023, s. 22. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4594467

²⁷ BAGNI, Filippo: The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act. In: SSRN Electronic Journal [online]. 2025, s. 205-206. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5268798

²⁸ ICO: The guide to the sandbox. In: ICO [online]. Dostupné na internete: <https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/the-guide-to-the-sandbox/#:~:text=The%20Regulatory%20Sandbox%20is%20a%20free%20service%20developed,ut ilise%20personal%20data%20in%20innovative%20and%20safe%20ways>

regulačných sandboxov naznačuje, že ide o účinný a perspektívny nástroj modernej regulačnej stratégie v kontexte zrýchlených digitálnych transformácií.

Regulačný sandbox sa ukazuje ako významný a perspektívny nástroj, ktorý umožňuje inovatívnym firmám testovať svoje riešenia v bezpečnom a regulovanom prostredí, ktoré je zároveň dostatočne flexibilné na to, aby reflektovalo dynamiku digitálnej ekonomiky. Tento koncept pomáha prekonávať bariéry vstupu a urýchljuje proces uvádzania nových produktov a služieb na trh bez ohrozenia ochrany spotrebiteľov alebo stability trhu.

Význam regulačných sandboxov presahuje rámec jednotlivých jurisdikcií a sektorov, pretože podporujú nielen technologický rozvoj, ale aj kvalitnejšie a informovanejšie nastavovanie regulačných rámcov prostredníctvom dialógu medzi regulátormi a inovátormi. To vedie k optimalizácii regulačnej praxe a jej lepšiemu prispôsobeniu súčasným potrebám technologického a spoločenského vývoja.

Rovnako dôležitou súčasťou je integrácia digitálnych technológií a kyberbezpečnostných opatrení, ktoré zabezpečujú ochranu dát a minimalizujú riziká spojené s inováciami v digitálnom priestore. Napriek niektorým rizikám, ktoré so sebou toto prostredie prináša, je regulačný sandbox efektívnym inštrumentom na vybalansovanie inovačného potenciálu a právnej istoty.

Ako moderný inštitucionálny koncept vytvára regulačný sandbox paralelu k digitálnej transformácii spoločnosti. Poskytuje nielen priestor pre overovanie nových myšlienok, ale aj základ pre tvorbu regulačných štandardov, ktoré umožňujú udržateľný rozvoj trhov a dôveru ich účastníkov. Preto je jasné, že regulačné sandboxy budú naďalej zohrávať kľúčovú rolu v evolúcii modernej regulácie a v podpore inovácií v digitálnej ekonomike.

Zoznam použitej literatúry

1. ACCLIME: Singapore's Fintech Regulatory Sandbox and Incentives. In: Acclime [online]. Dostupné na internete: <https://singapore.acclime.com/guides/fintech-sandbox-incentives/#part1>
2. ARNER, Douglas W. – BARBERIS, Janos – BUCKLEY, Ross P.: FinTech and RegTech in a nutshell, and the future in a sandbox. [s.l.]: CFA Institute Research Foundation, 2017. S. 16-17. Dostupné na internete: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3088303_code468680.pdf?abstractid=3088303
3. BAGNI, Filippo: The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act. In: SSRN Electronic Journal [online]. 2025, s. 205-206. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5268798

4. BOLDINI, Marco: A New Strategic Approach Towards Financial Regulation: A Comparative Overview of the English and Italian Legal System between Regulatory Needs and Technology Innovations. In: Bratislava Law Review [online]. 2022, roč. 6, č. 2, s. 11. Dostupné na internete: <https://blr.flaw.uniba.sk/index.php/BLR/article/view/276>
5. BROMBERG, Lev – GODWIN, Andrew – RAMSAY, Ian: Fintech Sandboxes: Achieving a Balance between Regulation and Innovation. In: SSRN Electronic Journal [online]. 2017. S.4-6. Dostupné na internete: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3090844_code178811.pdf?abstractid=3090844&mirid=1
6. FCA Regulatory Sandbox Guide. In: Financial Conduct Authority [online]. 2022. Dostupné na internete: [fca-regulatory-sandbox-guide.pdf](https://www.fca.org.uk/firm...ox)
7. Financial Conduct Authority. Regulatory Sandbox. [online]. Dostupné na internete: <https://www.fca.org.uk/firm...ox>
8. Financial Services and Markets Act 2000. Chapter 8. UK Public General Acts. 2000. Dostupné na internete: <https://www.legislation.gov.uk/ukpga/2000/8/part/1A/chapter/1>
9. GELŽINYTĖ, Virginija: Digitalisation of Financial Regulators as a Condition for Smarter Regulation and Supervision of the Market. Master's Thesis. Law School International Business Law LLM, Comenius University, 2019. s.29. Dostupné na internete: <https://arno.uvt.nl/show.cgi?fid=149407>
10. GROMOVA, Elizaveta A. – KONEVA, Natalia S. – TITOVA, Elena V.: Legal barriers to the implementation of digital industry (Industry 4.0) components and ways to overcome them. In: The Journal of World Intellectual Property [online]. S. 198. Dostupné na internete: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/jwip.12215?msocid=2037eb0e892d65173eeff5988e664a7>
11. GUMBO, Lilian – CHUDE-OKONKWO, Uche A. K.: Regulatory sandbox as a frontier for innovation and sustainability: a systematic review. In: Cogent Business & Management [online]. 2025, vol. 12, no. 1, s. 8. Dostupné na internete: <https://www.tandfonline.com/doi/full/10.1080/23311975.2025.2510555o>
12. CHEN, Christopher: Regulatory Sandbox and InsurTech: A Preliminary Survey in Selected Countries. In: SSRN Electronic Journal [online]. 2018, s. 10. Dostupné na internete: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3275929_code1582025.pdf?abstractid=3275929&mirid=1
13. ICO: The guide to the sandbox. In: ICO [online]. Dostupné na internete: <https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/the-guide-to-the->

sandbox/#:~:text=The%20Regulatory%20Sandbox%20is%20a%20free%20service%20developed,utilise%20personal%20data%20in%20innovative%20and%20safe%20ways

14. JOHNSON, Walter G.: Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. In: Regulation & Governance [online]. 2022, vol. 17, no. 3, s. 709. Dostupné na internete: <https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/rego.12487>
15. KAMUANGU, Paulin K.: A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends. In: Journal of Economics, Finance and Accounting Studies [online]. 2024, vol. 6, no. 1, s. 47-53. Dostupné na internete: <https://al-kindipublishers.org/index.php/jefas/article/view/6768>
16. LEDGER: The state of crypto scams in 2025. In: Ledger [online]. Dostupné na internete: <https://www.ledger.com/academy/topics/security/the-state-of-crypto-scams-in-2025>
17. MARKELOS, Raphael N. – ENNIS, Sean F. – ENSTONE, Bryn – MANOS, Anastasios – PAZAITIS, Dimitrios – PSYCHOYIOS, Dimitrios: Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies. In: SSRN Electronic Journal [online]. 2024, s. 7. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4764911
18. Monetary Authority of Singapore Act 1970. Chapter 186. Singapore Statutes Online. Dostupné na internete: <https://sso.agc.gov.sg/Act/MASA1970?Provids=P12-#pr4->
19. Monetary Authority of Singapore. FinTech Regulatory Guidelines. November 2016. Dostupné na internete: https://www.rajahtannasia.com/~media/Files/Asia%20Pacific%20Publications/2016/MAS_Fintech_RegulatorySandbox_Guidelines.pdf
20. NOVELLI, Claudio – HACKER, Philipp – MCDUGALL, Simon – MORLEY, Jessica – ROTOLO, Antonino – FLORIDI, Luciano: Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act. In: SSRN Electronic Journal [online]. 2025, s. 3. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5332161
21. QIU, Yingpeng – YAO, Han – REN, Ping – TIAN, Xueqing – YOU, Mao: Regulatory sandbox expansion: Exploring the leap from fintech to medical artificial intelligence. In: Health Policy and Technology [online]. 2025, s. 121. Dostupné na internete: <https://www.sciencedirect.com/science/article/pii/S2950261625000202>
22. RINGE, Wolf-Georg – RUOF, Christopher: Regulating Fintech in the EU: the Case for a Guided Sandbox. In: European Journal of Risk Regulation [online]. 2020, vol. 11, no. 3, s. 605. Dostupné na internete: <https://www.cambridge.org/core/services/aop-cambridge->

core/content/view/3EE71CEEB3BC22E57A1BF08023073A6F/S1867299X20000082a.pdf/div-class-title-regulating-fintech-in-the-eu-the-case-for-a-guided-sandbox-div.pdf

23. SEFERI, Fabio: A working experimentation model for cyber resilience regulatory sandboxes. In: CEUR Workshop Proceedings [online]. 2025, s. 4-6. Dostupné na internete: <https://ceur-ws.org/Vol-3962/paper67.pdf>
24. TENG, Huei-Wen et al.: Mitigating digital asset risks. In: SSRN Electronic Journal [online]. 2023. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4594467

Kontaktné údaje

Mgr. Dávid Kis

kis20@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

PROČ KRAJSKÁ SAMOSPRÁVA STÁLE POKULHÁVÁ? ZHODNOCENÍ STŘEDOEVROPSKÉ ZKUŠENOSTI SE ZAMĚŘENÍM NA KONKURENCESCHOPNOST

WHY IS REGIONAL SELF-GOVERNANCE STILL LAGGING BEHIND? EVALUATION OF THE CENTRAL EUROPEAN EXPERIENCE, FOCUSING ON COMPETENTIVENESS

Petr Konečný¹

Abstrakt: Čtvrtstoletí regionální samosprávy nevedlo k naplnění dvou základních úkolů, které při svém ustanovení na přelomu tisíciletí dostala do vínku: mocenská decentralizace a vyrovnávání rozdílů mezi regiony. Její fungování je velmi málo efektivní, přičemž rostou náklady na financování svěřených agend. Rozdíly mezi regiony se prohlubují, zejména v porovnání s ústředními regiony, a samosprávné regiony zpravidla zastávají roli nejméně významného aktéra v rámci procesu vládnutí. Tento příspěvek nastiňuje příčiny negativního vývoje a uvádí možný způsob regionální rekonfigurace. Pracuje s komparativním rámcem střední Evropy se zaměřením na Českou republiku, Slovensko a Rakousko. Evaluace je provedena prostřednictvím tří institucionálně-infrastrukturních kritérií konkurenceschopnosti regionu: univerzita mezinárodního významu, fakultní nemocnice a mezinárodní letiště. Vzhledem k většinové absenci těchto prvků mimo ústřední kraj lze konstatovat, že administrativně-politické regiony České republiky a Slovenska převážně postrádají potenciál pro posílení své pozice v rámci víceúrovňového vládnutí. Potenciálně konkurenceschopné jsou pouze některé z nich. Naopak v Rakousku je plně konkurenceschopná naprostá většina spolkových zemí vyjma dvou specifických případů. Na závěr je uvedena inspirace pro možnou rekonfiguraci.

Klíčové slova: autonómia, kraje, regióny, samospráva, územný rozvoj

Abstract: A quarter of a century of regional self-governance has not led to the fulfilment of the two basic tasks it was given when established at the turn of the millennium: decentralization and balancing regional disparities. In post-communist countries, its functioning is ineffective, while the costs of financing

¹ Masarykova univerzita

agendas are rising. The disparities between regions are widening, especially compared to central regions, and self-governing regions generally play the role of the least important actor in the process of governance. This paper outline reasons for the negative development and presents a possible method for regional reconfiguration. It works with a comparative framework of Central Europe, focusing on Czech Republic, Slovakia and Austria. The evaluation is carried out through three institutional-infrastructure criteria of regional competitiveness: university of international importance, teaching hospital and international airport. Due to the predominant absence of these elements outside of the central region (Prague, Bratislava region), it concludes that the Czech and Slovak regions mostly lack a potential for strengthening their position within multilevel governance. In Austria, on the other hand, the vast majority of the Länder are fully competitive, except for two specific cases. The paper concludes with an inspiration for a possible reconfiguration.

Key words: autonomy, regions, self-government, spatial development

Úvod

Regionální samospráva vznikla v postkomunistické části střední Evropy na přelomu tisíciletí. Po uplynutí čtvrtstoletí, které zhruba odpovídá jedné generaci, je načase kriticky zhodnotit její důsledky, poukázat na nedostatky a nastínit možnou budoucnost. Různé indikátory ostatně napovídají, že krajská samospráva v České republice a na Slovensku je v současné podobě neudržitelná a povolna se rozvíjí odborná, společenská i politická diskuze o revizi a komplexní reformě.

Tento příspěvek vychází z dosavadního autorova výzkumu regionální politické autonomie. Nastiňuje komparativní rámec potenciálu autonomního rozvoje na základě institucionálně-infrastrukturních kritérií regionální konkurenceschopnosti. Autor je vědom limitace studie z hlediska hloubky operacionalizace a objemu i charakteru sesbíraných dat. Přesto rád využil této platformy pro prezentaci prefinálních vstupů, které poslouží pro ucelené teoretické zázemí syntetické práce o regionální politické autonomii. Zároveň se jedná o publikační zhodnocení té empirické části jeho disertační práce, která se věnovala regionálním policiím².

² KONEČNÝ, Petr: Za rámec (de)centralizace: regionální autonomie v interdependentním Rakousku a České republice. Disertační práce. Masarykova univerzita, 2025. Přepřacovaná část sekcí teoretické a institucionální byla publikována: KONEČNÝ, Petr: Voluntary Interdependence in Federal Systems: Explaining Deautonomization through Coordinating Conferences in Austria. In: Publius: the Journal of Federalism, online first, 2025.

Prostorová spravedlnost a selhavší kohezní policy

Odborná debata o územním rozvoji prošla v posledních letech zásadním normativním posunem. K dlouhodobě užívanému klíčovému pojmu územní rozvoj (*spatial development*) ve smyslu komplexního posilování infrastrukturních a socioekonomických (či dalších) indikátorů prosperity³, který vycházel primárně z empiricko-analytické větve ekonomie, přibyl nový termín. Prostorová spravedlnost (*spatial justice*) vychází z normativně-institucionálního zázemí a zastřešuje horizontální dimenzi sociální férovosti (rovnosti)⁴.

V této perspektivě nejde už jen o přinášení prosperity do periferních regionů prostřednictvím územně-rozvojových nástrojů, ale o jeden ze zdrojů legitimizace moci. Právě legitimizace veřejné moci je ústředním tématem politologie a tento normativní posun lze vnímat jako významnou příležitost pro vstup politologických teorií do tématu územní samosprávy.

Jde totiž o to, že systém, který není schopen zajistit srovnatelnou dostupnost a kvalitu veřejných služeb od dopravní infrastruktury, přes zdravotní péči až po kulturní vyžití na celém území, takříkajíc i v poslední dědině, ztrácí svou legitimitu. Systémem se v prvé řadě myslí struktura územní (samo)správy, resp. územní dělení státu, ale problém se dotýká celého politického zřízení.

Dosavadní odborná literatura pracuje s principem územní spravedlnosti zejména na komunální úrovni a debatuje např. rozdíly v dostupnosti služeb v jednotlivých částech municipalit, mimo jiné i v souvislosti s amalgamací. Územní spravedlnost se ale logicky týká i regionální úrovně⁵. Ta je v tomto příspěvku chápána primárně ve vztahu k ustanoveným politicko-administrativním regionům.

Vzhledem k empirickému zaměření na Českou republiku a Slovensko se jedná o tamější samosprávné kraje. Závěrečná část příspěvku nabízí srovnání se spolkovými zeměmi v Rakousku, které se sice liší svým státoprávním charakterem, ale podobají se velikostně a do určité míry i funkcionálně tím, že jedinou relevantní částí svěřených autonomních pravomocí je neregulativní, finančně-organizační kompetence zaměřená na územně rozvojové projekty.

Jednou ze základních politik (policies) Evropské unie i jednotlivých členských států je *kohezní politika* neboli politika soudržnosti⁶. Ta vychází z pojetí územního rozvoje, ale lze ji vztáhnout k problematice prostorové spravedlnosti. Pokud se podíváme na

³ Viz např. definice použitá v: PIKE, Andy – RODRÍQUES-POSE, Andrés – TOMANEY, John: Local and Regional Development. London: Routledge, 2016 (2. vydání). 406 s. ISBN 9781315767673.

⁴ Viz např. definice použitá v: WANG, Shaoxu – GU, Wai: Spatial Justice and Planning. Cham: Springer, 2023. 172 s. ISBN 978-3-031-38069-3.

⁵ Výjimku věnující se regionální úrovni představuje např.: JONES, Rhys – MOISIO, Sami: Regions and the search for spatial justice: a question of capacity? In: Regional Studies, Roč. 59, č. 1 (2024).

⁶ Evropská unie. New Cohesion Policy. Dostupné zde: https://ec.europa.eu/regional_policy/2021-2027_en.

mapu evropských regionů dle jednotlivých rozvojových indikátorů, vidíme přetrvávající značné rozdíly, mnohdy i vícenásobné v rámci jednotlivých států. Zejména u postkomunistických států vidíme mírné celkové přiblížení se průměru tzv. starých členských států, ale zároveň i prohlubování vnitrostátních disparit⁷. V prvé řadě se jedná o propastný rozdíl mezi ústředním regionem (zahrnujícím hlavní město) a druhým nejrozvinutějším regionem, ale také mezi regiony mimo hlavní město. Zároveň stav ve stylu dominantní hlavní město vs. zaostávající „venkov“ není evropským standardem, ale pouze standardem takříkajíc východoevropským. Ve vyspělejší části Evropy najdeme státy s poměrně srovnatelnými indikátory napříč všemi regiony. Modelovým příkladem je Rakousko, kde navíc druhý nejrozvinutější region (Salcbursko) v některých indikátorech předstihl hlavní město Vídeň; tento stav platí např. i v Německu (více regionů) a Španělsku (Katalánsko)⁸. Ale i v této části Evropy najdeme státy, kde se nedaří vyrovnávat regionální rozdíly, např. ve Francii. Celkově lze konstatovat, že prakticky ve všech postkomunistických státech selhala kohezní politika. Totéž ale platí pro Evropskou unii jako celek, kdy se dlouhodobě nedaří vyrovnávat regionální rozdíly vnitrostátně ani napříč jednotlivými členskými státy. Představuje to zdroj delegitimizace územně správní struktury a výzvu pro celé politické zřízení. Otevírá se tedy cesta pro revizi této struktury a přípravu reformy vedoucí k relegitimizaci. Jak ukazuje následující sekce, nestačí přitom pouhé kosmetické úpravy; nutná je komplexní reforma, která zasáhne všechny dimenze územní samosprávy.

Čtvrtstoletí neúspěšného krajského experimentu

Velká správní reforma na přelomu tisíciletí v České republice a Slovensku se nesla ve znamení volby těch alternativ, které se s odstupem jeví jako méně vhodné. Namísto relativně velkých krajů (dvě až tři země či osm až devět krajů v ČR a čtyř krajů v SR) byly schváleny tzv. malé kraje (čtrnáct krajů v ČR, osm krajů v SR). Místo oddělené správy, která by reflektovala konkurenční principy autonomie a administrativní efektivity, byla zavedena smíšená správa, na Slovensku posléze na regionální úrovni zrušená (od roku 2007). Na Slovensku byly také zachovány okresní úřady jako profesionální úřady územní správy, které v ČR chybějí. V obou státech navíc byla zachována fragmentovaná obecní struktura.

V ČR tak došlo k vybudování hybridního systému, který směšuje státní správu a samosprávu, aniž by přišel kýžený trade-off. Vzájemně prorostlá státní správa a samospráva vede k dublování agend a praktické nemožnosti aplikovat princip odpovědnosti. Na Slovensku naproti tomu zůstala zachována limitovaná regionální

⁷ Dle dat serveru Eurostat pro regiony NUTS 3, resp. NUTS 2. Dostupné zde: <https://ec.europa.eu/eurostat>.

⁸ Viz předchozí poznámka.

samospráva, což se ukazuje jako příznivější pro budoucí reformu. V ČR je navíc krajská konfigurace chráněna ústavním zákonem. Samosprávné kraje a jejich krajské reprezentace se hájí poukazem na to, že zajišťují celou řadu agend. Pouze některé z nich ale náleží do samosprávné větve.

Právě dělba působnosti krajů ČR na tzv. přenesenou (přenesený výkon státní správy na území kraje) a samostatnou (autonomní) situaci dále znepřehledňuje. Rozložení agend vyžadovalo podrobnou analýzu, ze které navíc vyplynulo, že autonomní kompetence se omezuje pouze na oblast územně rozvojových projektů. I zde jsou kraje limitovány nedostatečnými finančními zdroji, zejména autonomními (tzv. vlastními)⁹. Přibližně dvě třetiny celkových příjmů krajů ČR představují dotace – převážně účelové¹⁰. Literatura indikuje, že obdobná situace panuje na Slovensku¹¹. Zde dotace tvoří přibližně 40 % celkových příjmů krajů¹².

Celkově tedy lze zhodnotit, že krajská samospráva v ČR a SR vykazuje disfunkční institucionální setup ve všech dimenzích: konfigurace (malé kraje; slabá institucionální struktura), kompetence (žádná relevantní autonomní kompetence mimo oblast územně rozvojových projektů), finance (nedostatečné zdroje; významný podíl, resp. převaha účelových dotací). Celkové příjmy krajů přitom tvoří nemalou část státního rozpočtu: oproti příjmům státního rozpočtu pro rok 2025 to bylo na Slovensku 12 % (všechny územní celky dohromady 46 %), v ČR 18 % (všechny územní celky dohromady 44 %).

Kraje postrádají potenciál pro implementaci strategických projektů. Ty jsou přitom klíčové pro zajištění konkurenceschopnosti regionů, která má zásadní vliv na získávání a udržování zdrojů pro rozvoj, což je propojeno s posilováním autonomního postavení. Této kauzalitě se věnuje následující sekce, a to na podkladě debaty o nedostatečné institucionální struktuře krajů, která vede k nenaplňování níže vytyčených kritérií konkurenceschopnosti.

⁹ KONEČNÝ, Petr: Examining Regional Autonomy through Policies: Evidence from the Czech Republic. In: Politologický časopis, Roč. 30, č. 2 (2023), s. 73–94. Upřesněná a doplněná empirická data: KONEČNÝ: disertace, op.cit.

¹⁰ KONEČNÝ, 2023, op.cit.

¹¹ Např. HORVÁTH, Peter – MIHÁLIK, Jaroslav – ŠVIKRUHA, Martin. Give me liberty or give me money: the fiscal decentralization and autonomy of regional governance in Slovakia. In: European Journal of Government and Politics, Roč. 8, č. 1 (2019), s. 96–109.

¹² Ministerstvo financií SROV. Hospodárenie obcí a vyšších územných celkov za rok 2023. Dostupné zde:

https://www.mfsr.sk/files/archiv/85/Vyhodnotenie_vysledkov_rozpocetoveho_hospodarenia_obci_a_vyssich_uzemnych_celkov_za-rok-2023.pdf.

Institucionálně-infrastrukturní kritéria konkurenceschopnosti regionů

Dosavadní literatura nenabízí obecnou teorii regionální politické autonomie. Při jejím teoretickém ukotvování je nezbytné vyjít z teorie víceúrovňového vládnutí a vnímat ji jako součást procesu vládnutí. Jedině tak lze překonat formalismus převážné většiny dosavadních studií, jejichž datová základna se omezuje na ústavní dokumenty (komparativní ústavní právo, resp. komparativní federalismus) a rozpočtové dokumenty (fiskální autonomie).

Především je třeba meziúrovňové vztahy pojímat sofistikovaněji než pouze jako kontinuum mezi centralizací a decentralizací, tedy jako míru delegace rozhodovacích pravomocí z ústředních orgánů na samosprávné celky. Podstatnou roli rovněž sehrává míra sdílení kompetencí – autonomie vs. interdependence. Interdependence, tedy vzájemná závislost jednotlivých úrovní politiky, se projevuje sdílenými kompetencemi, finančními zdroji a vzájemně závislým rozhodováním. Na druhé straně pomyslného kontinua leží autonomie, která se vykazuje výlučnými kompetencemi, vlastními finančními zdroji a samostatným rozhodováním. Interdependence zásadně ovlivňuje proces vládnutí a omezuje autonomní rozhodování, tedy vede k deautonomizaci. Literatura také používá pojmy samovláda a sdílená vláda (self-rule vs. shared rule). Zároveň je třeba kontinuitu autonomie–interdependence pojímat jako samostatnou dimenzi vůči dimenzi decentralizace.

Dosud nejpokročilejší rozlišení dimenzí centralizace–decentralizace a autonomie–interdependence nabízí Bolleyer a Thorlakson (2012)¹³, které na základě široké komparace jedenácti federálních systémů zdůrazňují relevanci této distinkce v rámci komparativního federalismu. Lze ji ale vztáhnout na všechny regionalizované státy včetně unitárních.

Při zkoumání regionální politické autonomie je nutné podchytit dynamiku mezi vstupem, procesováním a výstupem autonomie, tedy mezi institucionálními a procedurálními faktory (autonomizační/interdependizační) a charakterem regionálních policies (originální/adaptivní)¹⁴.

Dosavadní literatura nenabízí širokou komparaci regionálních policies. Z autorova dosavadního empirického výzkumu interdependentních systémů, který zahrnuje Českou republiku, Slovensko, Polsko a Rakousko, vyplývá, že navzdory výčtu nominálních pravomocí jedinou relevantní autonomní kompetencí vedoucí k originálním policies ve strukturách tohoto typu, je neregulativní, finančně-organizační oblast územně rozvojových projektů. Zde lze za uplynulé čtvrtstoletí doložit konkrétní strategické projekty, které jednotlivé regionální reprezentace

¹³ BOLLEYER, Nicole – THORLAKSON, Lori. Beyond Decentralization—The Comparative Study of Interdependence in Federal Systems. In: *Publius: the Journal of Federalism*, Roč. 42, č. 4 (2012), s. 566–591.

¹⁴ Tuto dynamiku, resp. kauzalitu široce rozebírá autorova disertační práce (op.cit).

iniciovaly a implementovaly převážně z vlastních zdrojů. Substanciálně se ovšem liší jejich relevance. Problémem totiž je, že u naprosté většiny projektů se jedná o dílčí, svým rozsahem a dopadem značně omezené projekty.

Strategické územně rozvojové policie, které vedly k trvalému posílení konkurenceschopnosti autor identifikoval pouze u rakouských spolkových zemí. Jako příklad uveďme výstavbu nového areálu ústřední korutanské zemské nemocnice v Klagenfurtu v rámci konsolidace zemské nemocniční struktury, za celkem 328 milionů euro, 2006–2010¹⁵.

Ukazuje se, že právě autonomní finanční zdroje (daňové příjmy, kapitálové příjmy, popř. daně a poplatky) jsou klíčové z hlediska celkového postavení samosprávných regionů v daném systému. Politologická intuice (protože obecná teorie v tomto smyslu stále chybí) ostatně hovoří o tom, že kde je moc, tam jsou zdroje a tam je rozvoj – a naopak. Nabízí se tak možnost komparovat samosprávné regiony z hlediska jejich konkurenceschopnosti.

Při ustanovování kritérií konkurenceschopnosti opět narážíme na absenci obecné teorie. Z obecných poznatků výzkumu v oblasti územního rozvoje¹⁶ a autorova empirického výzkumu vyplývá, že alespoň při porovnávání České republiky, Slovenska a Rakouska se lze zaměřit na tři klíčové institucionální a infrastrukturní prvky, které přímo či nepřímo souvisejí s autonomní regionální pravomocí: *univerzita mezinárodního významu, fakultní nemocnice, mezinárodní letiště*¹⁷.

Univerzitou mezinárodního významu se myslí taková vysoká škola univerzitního typu, kterou lze pojímat jako dostatečně významnou. Jakkoliv bývají komparace univerzit ne zcela přesné, lze využít zavedených žebříčků. Tento příspěvek pracuje s daty z QR World University Ranking dle aktuálních dat pro rok 2026¹⁸. Za dostatečně relevantní se považují univerzity v první tisícovce.

Správa univerzit ani v jednom ze tří států není součástí regionální pravomoci (a to ani přenesené). Přesto na rozvoj univerzit mají samosprávné regiony vliv, a to přinejmenším prostřednictvím partnerství, které zahrnuje i kofinancování vybraných projektů. Jde zejména o rozvoj inovačních center. V Rakousku navíc za poslední čtvrtstoletí došlo ke vzniku několika soukromých univerzit, které mají kvazizemský

¹⁵ Konečný, disertace, op.cit.

¹⁶ GLASS, Michael R. – ADDIE, Jean-Paul – NELLES, Jen: Regional infrastructures, infrastructural regionalism. In: Regional Studies, Roč. 53, č. 12 (2019), s. 1651–1656. RODRÍGUEZ-POSE, Andrés: Do Institutions Matter for Regional Development? In: Regional Studies, Roč. 47, č. 7 (2013), s. 1034–1047. KAZDA, Antonín – HROMÁDKA, Martin – MREKAJ, Boris: Small regional airports operation: unnecessary burdens or key to regional development. In: Transportation Research Procedia, č. 28 (2017), s. 59–68.

¹⁷ Naopak nepatří sem dálnice a železnice včetně vysokorychlostních tratí, které plně náleží pod správu státu.

¹⁸ Dostupné zde: <https://www.topuniversities.com/world-university-rankings>.

charakter. Jednotlivé spolkové země totiž figurovaly, resp. figurují jako významný iniciátor a investor a mají svého zástupce ve správní radě. Jde o Paracelsovu soukromou lékařskou univerzitu v Salcburku, úzce spolupracující se zdravotnickými zařízeními v Salcbursku (Paracelsus Medizinische Privatuniversität, založena 2003, salcburská zemská vláda tehdy poskytla 10 milionů šilinků). Dále o korutanskou soukromou hudební univerzitu pod názvem Gustav Mahler Privatuniversität für Musik (zahájila výuku ve školním roce 2018/19, za významného finančního přispění zemské vlády)¹⁹.

Fakultní nemocnicí se myslí všeobecná nemocnice poskytující praxi vysokoškolským studentům (*teaching hospital*). Zároveň je zde nutné jemnější dělítko z důvodu lišící se terminologie. V České republice se jedná o všechny nominální fakultní nemocnice (celkem dvanáct). Na Slovensku sice existuje jedenáct nominálních fakultních nemocnic, jejich význam se ale podstatně liší. Tento článek pracuje pouze ze třemi tzv. *univerzitními nemocnicami*, které se svým charakterem podobají fakultním nemocnicím v ČR. V Rakousku této kategorii odpovídají tzv. *Landeskliniken*²⁰. Při určování přítomnosti takto definované fakultní nemocnice příspěvek pracuje s údaji zveřejněnými veřejnými nemocnicemi.

Správa fakultních nemocnic nepatří do regionální pravomoci v ČR a na Slovensku; ty spravuje stát. Fakultní nemocnice nicméně zároveň představují ústřední nemocniční zařízení v daném regionu a kraje se podílejí na jejich rozvoji prostřednictvím partnerství. Myslí na ně i krajské strategie rozvoje zdravotní péče. Naproti tomu v Rakousku jsou všechny veřejné nemocnice, s výjimkou úrazových nemocnic, pod zemskou správou.

Mezinárodním letištěm se myslí takové letiště, které stabilně vykazuje pravidelné mezinárodní linky. V rámci tohoto příspěvku pro naplnění kritéria nestačí charterové lety a sezonní linky; hraničním případem jsou letiště s jedním až třemi pravidelnými linkami. Empirická data navíc hovoří o tom, že malá letiště ve středovýchodní Evropě mají problém dlouhodobě udržet lukrativní spojení na významné letecké dopravní uzly. I zde je tedy třeba jemnějšího dělítko. Při určování přítomnosti takto definovaného mezinárodního letiště příspěvek pracuje s daty zveřejněnými ministerstvy dopravy a letištními společnostmi.

Na rozdíl od dvou předcházejících kritérií bývají letiště alespoň v částečné správě regionu (vyjma ústředních státních letišť). Přesněji daný region má své ústřední letiště (částečně) v majetku a alespoň částečně – a často majoritně – zajišťuje jeho provoz prostřednictvím soukromé firmy.

¹⁹ Kvazizemské soukromé univerzity dále představují UMIT Tirol – Soukromá univerzita pro zdravotní vědy a technologie, kterou z 90 % vlastní Tyrolsko. Dolní Rakousy mají čtvrtinový podíl v Soukromé univerzitě pro zdravotní vědy Karla Landsteinerja v Kremži.

²⁰ V některých spolkových zemích nesoucí odlišný název – např. Landeskrankenhäuser ve Vorarlbersku.

Nekonkurenceschopné a potenciálně konkurenceschopné regiony

Ze získaných dat vyplývá, že kritéria konkurenceschopnosti kraje ČR a SR nenaplnují, většina dokonce vůbec. Převážně konkurenceschopný je Jihomoravský kraj, jehož ústřední letiště ale v čase vykazuje značnou proměnlivost počtu pravidelných linek (jedna až čtyři²¹). V potenciálně převážně konkurenceschopném Košickém kraji absentuje významná univerzita a letiště není ve vlastnictví regionu. Podobně Moravskoslezský kraj postrádá významnou univerzitu a letiště vykazuje hraniční hodnoty. Potenciálně konkurenceschopné jsou kraje Plzeňský, Královéhradecký, Olomoucký a Žilinský, které splňují kritérium fakultní nemocnice (Olomoucký kraj má také univerzitu vykazující hraniční hodnoty)²². Plně konkurenceschopné jsou pouze ústřední regiony (Hlavní město Praha, Bratislavský kraj).

Naopak v Rakousku naprostá většina spolkových zemí splňuje všechna tři kritéria. Výjimkou je Burgenlandsko, které historicky vzniklo jako umělý region a které je výrazně závislé z hlediska dojíždky za službami včetně univerzitního vzdělání na Dolních Rakousích, resp. Vídni. Druhou výjimku představuje Vorarlbersko, které je pomezím, takřkajíc přechodovým mikroregionem na pomezí alpského Rakouska, Švýcarska a tzv. Bodamska (Bodenseeraum) a nedostatek institucionálního zázemí vyrovnává silnou turistickou ekonomikou. Rakousko tak představuje příklad dobré praxe, kdy samosprávným regionům je zaručena taková míra autonomie, která zemským reprezentacím umožňuje udržovat a posilovat konkurenceschopnost. Srovnání regionů dle kritérií konkurenceschopnosti shrnuje níže uvedená tabulka a mapy.

Tabulka 1. Institucionálně-infrastrukturní zázemí regionů ČR, Slovenska a Rakouska

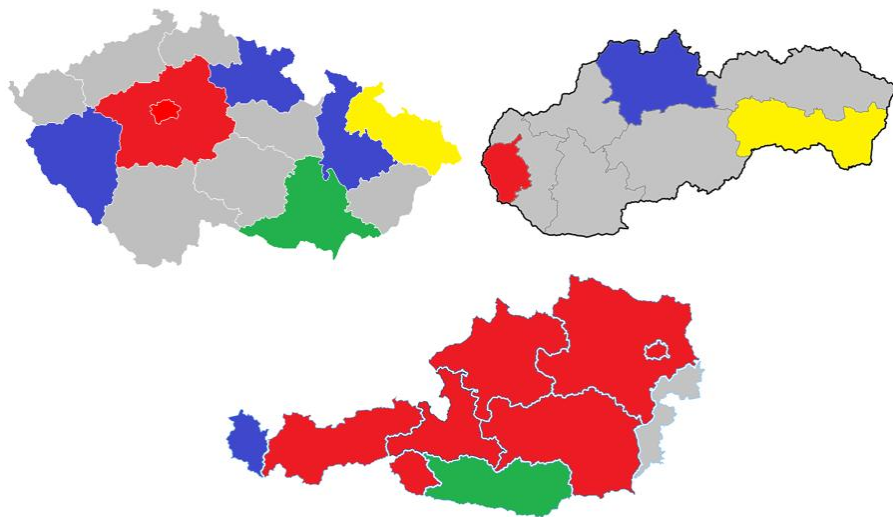
Kritérium konkurenceschopnosti	Region
Univerzita mezinárodního významu	CZ: Praha/SČK, JMK, (OLK) SK: B A: W, NÖ, OÖ, Stmk, Ktn, T, Sbg
Fakultní nemocnice	CZ: Praha/SČK, PLK, HKK, JMK, OLK, MSK SK: B, K, Ž A: W, NÖ, OÖ, Stmk, Ktn, T, Sbg, V
Mezinárodní letiště	CZ: Praha/SČK, (JMK), (MSK) SK: B, K A: W, NÖ, OÖ, Stmk, T, Sbg, (Ktn)

²¹ Přehledně: Ministerstvo dopravy. Dokumenty: Letecká doprava. Dostupné zde: <https://md.gov.cz/Dokumenty/Letecka-doprava>.

²² Letiště Poprad-Tatry je zde hodnoceno jako pod kritickou hranicí, absentuje proto v přehledové tabulce.

Vysvětlivky: SČK = Středočeský kraj, JMK = Jihomoravský kraj, OLK = Olomoucký kraj, MSK = Moravskoslezský kraj, PLK = Plzeňský kraj, HKK = Královéhradecký kraj; B = Bratislavský kraj, K = Košický kraj, Ž = Žilinský kraj; W = Vídeň, NÖ = Dolní Rakousy, OÖ = Horní Rakousy, Stmk = Štýrsko, Ktn = Korutansko, T = Tyrolsko, Sbg = Salcbursko, V = Voralbersko; závorka indikuje hraniční hodnoty kritérií. Zdroj: Ministerstvo školství, mládeže a tělovýchovy ČR, Ministerstvo zdravotnictví ČR, Ministerstvo dopravy ČR, Ministerstvo školstva, výskumu, vývoja a mládeže SR, Ministerstvo zdravotníctva SR, Ministerstvo dopravy SR, oesterreich.gv.at.

Mapa 1. Konkurenceschopnost regionů ČR, Slovenska a Rakouska



Vysvětlivky:

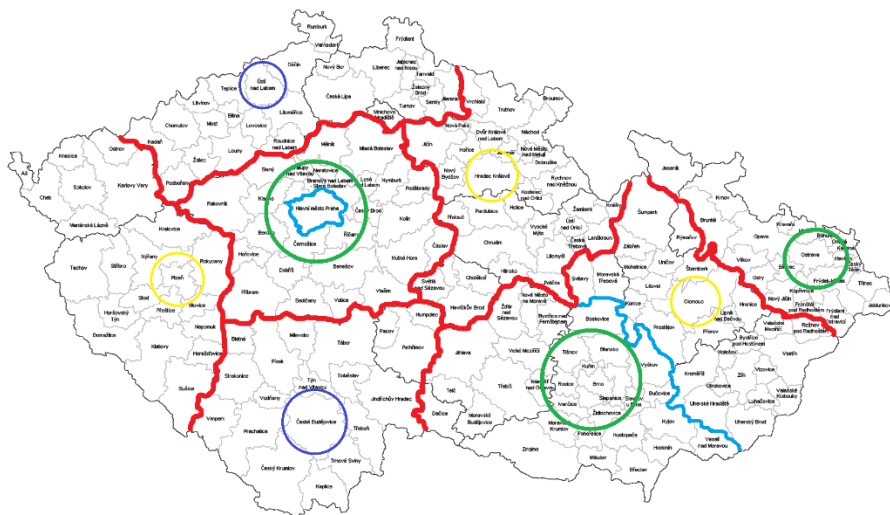
červená barva = plně konkurenceschopný; zelená b. = převážně k.; žlutá b. = potenciálně převážně k.; modrá b. = nek. Zpracoval: autor. Podklad: Ministerstvo pro místní rozvoj ČR, Ministerstvo investícií, regionálneho rozvoja a informatizácie SR, oesterreich.gv.at).

Z výše uvedeného vyplývá, že pokud by při komplexní reformě byla užita metoda těchto kritérií konkurenceschopnosti, dává smysl ustanovit takové regiony, které jsou převážně konkurenceschopné nebo mají alespoň významný potenciál. Naopak nedává smysl udržovat ty regiony, u nichž by naplnění kritérií vyžadovalo nadměrnou investici. Ostatně za uplynulé čtvrtstoletí prakticky nedošlo k strategickému posílení institucionální struktury krajů ČR a Slovenska.

V ČR je tedy k úvaze konfigurace osmi až devíti regionů, která se blíží historicky zvažované variantě tzv. velkých krajů. Tři regiony se navíc opírají o současné metropolitní oblasti, jak je definují unijní a státní strategické dokumenty (ITI). Podobně je tomu na Slovensku, kde by byly ustanoveny čtyři regiony. Střední Čechy a Západní Slovensko jsou zde chápány jako širší zázemí ústředního regionu (hlavního města).

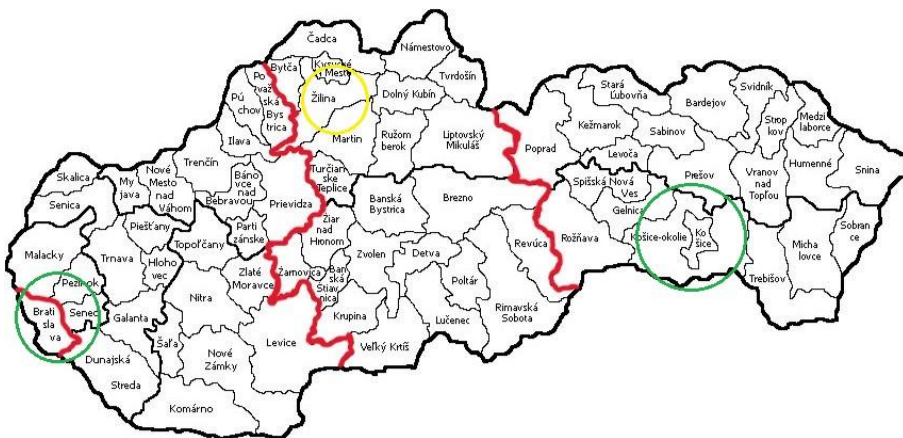
Novou konfiguraci naznačují níže uvedené mapy, přičemž konkrétní hranice dle okresů/ORP je třeba brát jako fakultativní, resp. není zde prostor pro stanovení kritérií mikroregionální příslušnosti.

Mapa 2. Potenciální konfigurace regionální samosprávy ČR



Vysvětlivky: červená linka = nové samosprávné regiony; modrá l. = alternativní nové regiony; zelený kruh = metropolitní oblasti; žlutý k. = nutno vybudovat mez. univerzitu a letiště; modrý k. = nutno vybudovat mez. univerzitu, letiště a fakultní nemocnici; název obce = okres/správní obvod obce s rozšířenou působností. Zpracoval: autor. Podklad: MRR ČR.

Mapa 3. Potenciální konfigurace regionální samosprávy Slovenska



Vysvětlivky: viz výše. Zpracoval: autor. Podklad: MIRRI SR.

Závěr

Závěrečnou sekci využiji pro krátkou úvahou nad možnou budoucností regionální samosprávy v České republice a na Slovensku.

Pokud bude zachován stávající trend, dojde s velkou pravděpodobností k recentralizaci z důvodu snahy o konsolidaci veřejných prostředků, popřípadě k strukturální implozi kvůli nedostatku zdrojů na pokrytí mandatorních výdajů regionů. Jako jediná schůdná alternativa se jeví komplexní reforma, a to ve všech dimenzích – konfigurace, kompetence, finance.

Je třeba stanovit kritéria konkurenceschopnosti a tuto zajistit ve všech regionech. Samosprávným regionům je třeba přiznat takové kompetence a finanční zdroje, aby mohly vybudovat, udržovat a posilovat klíčové institucionálně-infrastrukturní prvky: univerzity mezinárodního významu, fakultní nemocnice a mezinárodní letiště.

Reformu regionální samosprávy je zároveň nutné zasadit do kontextu dalších nevyhnutelných změn v systému veřejné správy. Těm se ostatně věnují další příspěvky v tomto sborníku.

Zoznam použitej literatúry

1. BOLLEYER, Nicole – THORLAKSON, Lori. Beyond Decentralization—The Comparative Study of Interdependence in Federal Systems. In: *Publius: the Journal of Federalism*, Roč. 42, č. 4 (2012), s. 566–591.
2. GLASS, Michael R. – ADDIE, Jean-Paul – NELLES, Jen: Regional infrastructures, infrastructural regionalism. In: *Regional Studies*, Roč. 53, č. 12 (2019), s. 1651–1656.
3. HORVÁTH, Peter – MIHÁLIK, Jaroslav – ŠVIKRUHA, Martin. Give me liberty or give me money: the fiscal decentralization and autonomy of regional governance in Slovakia. In: *European Journal of Government and Politics*, Roč. 8, č. 1 (2019), s. 96–109.
4. JONES, Rhys – MOISIO, Sami: Regions and the search for spatial justice: a question of capacity? In: *Regional Studies*, Roč. 59, č. 1 (2024).
5. KAZDA, Antonín – HROMÁDKA, Martin – MREKAJ, Boris: Small regional airports operation: unnecessary burdens or key to regional development. In: *Transportation Research Procedia*, č. 28 (2017), s. 59–68.
6. KONEČNÝ, Petr: Voluntary Interdependence in Federal Systems: Explaining Deautonomization through Coordinating Conferences in Austria. In: *Publius: the Journal of Federalism*, online first, 2025.
7. KONEČNÝ, Petr: Examining Regional Autonomy through Policies: Evidence from the Czech Republic. In: *Politologický časopis*, Roč. 30, č. 2 (2023)

8. KONEČNÝ, Petr: Za rámec (de)centralizace: regionální autonomie v interdependentním Rakousku a České republice. Disertační práce. Masarykova univerzita, 2025.
9. PIKE, Andy – RODRÍQUES-POSE, Andrés – TOMANEY, John: Local and Regional Development. London: Routledge, 2016 (2. vydání). 406 s. ISBN 9781315767673.
10. RODRÍGUEZ-POSE, Andrés: Do Institutions Matter for Regional Development? In: Regional Studies, Roč. 47, č. 7 (2013), s. 1034–1047.
11. WANG, Shaoxu – GU, Wai: Spatial Justice and Planning. Cham: Springer, 2023. 172 s. ISBN 978-3-031-38069-3.

Kontaktné údaje

Mgr. Petr Konečný, Ph.D.

petr.j.konecny@gmail.com

Masarykova univerzita, Česká republika

VÝZVY V DAŇOVOM PRÁVE V SÚVISLOSTI S DIGITALIZÁCIOU (FOKUS NA VÝMENU INFORMÁCIÍ)

CHALLENGES IN TAX LAW REGARDING DIGITALISATION (FOCUS ON EXCHANGE OF INFORMATION)

Andrea Szakács¹

Abstrakt: Digitalizácia ekonomiky môže predstavovať výzvy pre daňové správy členských štátov EÚ v podobe nedostatočných informácií o príjmoch/výnosoch získaných z aktivít vykonávaných cezhranične v rámci EÚ priestoru aj celosvetovo. Informácie vo všeobecnosti sú v súčasnosti najhodnotnejšou komoditou a to platí dvojnásobne pri daniach. Výmena informácií je zabezpečovaná na globálnej úrovni cez OECD a jej právne nástroje a na úrovni EÚ ju zabezpečuje smernica DAC. V príspevku autor priblíži zavedenie novej kategórie automatickej výmeny informácií v podobe oznámení s informáciami na určenie dorovnávejacej dane. V súvislosti s predmetnou výmenou informácií autor považuje za vhodné priblížiť aj celkový koncept dorovnávejacej dane.

Kľúčové slová: DAC 9, výmena informácií, digitalizácia, dorovnávací daň, Pillar 2

Abstract: The digitalisation of the economy may pose challenges for the tax administrations of the EU Member States in the form of insufficient information on income/revenues obtained from activities carried out cross-border within the EU area and globally. Information in general is currently the most valuable commodity and this is doubly true in the case of taxes. The exchange of information is ensured at the global level through the OECD and its legal instruments and at the EU level by the DAC Directive. In the article, the author will present the introduction of a new category of automatic exchange of information in the form of notifications with information for the determination of the additional tax. In connection with the exchange of information in question, the author considers it appropriate to also explain the overall concept of the equalization tax.

Key words: DAC 9, exchange of information, digitalization, equalization tax (top-up tax), Pillar 2

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra finančného práva

Úvod

Súčasný svet je globalizovaný a čím viac digitalizovaný. V mnohých prípadoch daňové systémy už nie sú vhodné pre globalizovanú a digitalizovanú ekonomiku a je potrebná modernizácia kľúčových prvkov medzinárodného daňového systému. To znamená, že daňové systémy sa musia prispôbovať aktuálnym výzvam a prijať kroky nadväzujúce na globálny vývoj. Organizácia pre hospodársku spoluprácu a rozvoj (ďalej len „OECD“) ako globálna medzinárodná organizácia navrhuje a prijíma rôzne nástroje, ktorými sleduje cieľ boja proti daňovým únikom a proti vyhýbaniu sa daňovým povinnostiam. Prijala napr. Akčný plán proti narúšaniu (znižovaniu) základu dane a presunu ziskov (tzv. BEPS plan), ktorý obsahuje konkrétnych 15 opatrení na zlepšenie spravodlivosti daňových systémov. Opatrenie 1 BEPS plánu rieši daňové výzvy digitalizácie ekonomiky a v rámci predmetného opatrenia bolo prijaté dvoj-pilierové riešenie. Pilier 1 prispôbuje medzinárodné pravidlá zdaňovania najmä príjmov právnických osôb aktuálnemu globalizovanému a digitalizovanému svetu, v ktorom sa mení obchodný model spoločností často smerujúci k podnikaniu bez fyzickej prítomnosti v krajine. Pilier 1 by mal čiastočne prerozdeliť právo zdaňovať príjmy určitých podnikov, ktoré nie sú v danej krajine rezidentmi, ale majú v danej krajine zákazníkov a používateľov, a to s použitím konkrétneho dohodnutého vzorca. Spočiatku sa Pilier 1 mal zamerať hlavne na obchodné spoločnosti, ktoré pôsobia v digitálnom svete. Až následne sa dohodlo, aj za účelom zjednodušenia, že sa Pilier 1 bude zameriavať na nadnárodné skupiny podnikov s obrátom 750 mil. eur ročne a to bez ohľadu na sektor, v ktorom pôsobia. Cieľom Pilieru 2 je zaviesť minimálnu efektívnu hranicu zdanenia príjmov nadnárodných spoločností. Dôvodom zavedenia Pilieru 2 je skutočnosť, že mnohé nadnárodné spoločnosti využívajúc svoje globálne pôsobenie presúvali príjmy/zisky do jurisdikcií s nízkym alebo žiadnym zdanením a tým sa vyhýbali daňovým povinnostiam. Pilier 2 by mal zabezpečiť, že nadnárodné skupiny podnikov zaplatia aspoň minimálnu efektívnu výšku dane v zmysle dohodnutej metodiky a vzorca výpočtu, čím sa sleduje aj obmedzenie, prinajlepšom eliminácia problému vyhýbania sa daňovým povinnostiam.² Európska únia (ďalej len „EÚ“) rovnako, veľakrát aj v spolupráci s OECD, prijíma vlastné právne akty nadväzujúce na tento sledovaný cieľ, avšak výslovne pri daňových výzvach súvisiacich s digitalizáciou ekonomiky uprednostňuje globálne riešenia, ktoré ona preberie.³ Okrem smernice o dorovnávejacej dani EU podnikla mnoho iných legislatívnych iniciatív prispievajúcich

² Oznámenie Komisie Európskemu parlamentu a Rade z 18. mája 2021: Zdaňovanie podnikov v 21. storočí COM(2021) 251 final, str. 8

³ Oznámenie Komisie Európskemu parlamentu a Rade z 18. mája 2021: Zdaňovanie podnikov v 21. storočí COM(2021) 251 final, str. 8

k vzniku digitalizovaného spracovania daní v EÚ (napr. BEFIT⁴, HOT⁵, FASTER⁶, DEBRA⁷).⁸ Slovenská republika (ďalej len „SR“) nasleduje tento trend ako členský štát EÚ a aj ako jeden zo 137 štátov a jurisdikcií, ktorí sa pripojili k Inkluzívnemu rámcu k BEPS.

OECD, EÚ, SR a dorovnávací daň (Pilier 2)

Dňa 14. decembra 2021 boli inkluzívnym rámcem OECD/G20 k BEPS schválené a následne publikované detailné modelové medzinárodné pravidlá proti znižovaniu/narúšaniu základu dane (tzv. Global Anti Base Erosion – GloBE rules),⁹ ktoré sú kľúčovým komponentom plánu modernizácie medzinárodného daňového systému a zabezpečujú, že veľké nadnárodné spoločnosti zaplatia minimálnu daň z príjmov v každej jurisdikcii, v ktorej pôsobia. Pravidlá GloBE vytvárajú systém dvoch vzájomne prepojených pravidiel, pričom jedno pravidlo sa nazýva pravidlo zahrnutia príjmov (IIR – Income Inclusion Rule) a druhé pravidlo je pravidlo nedostatočne zdanených príjmov (UTPR – Undertaxed Profit Rule).¹⁰ Pravidlá GloBE predstavujú koordinovaný systém zdaňovania, ktorý ukladá dodatočnú (dorovnávaciu) daň z príjmov v konkrétnej jurisdikcii, v ktorej je efektívna sadzba dane nižšia ako minimálna sadzba. V zmysle týchto pravidiel príslušní daňovníci vypočítavajú efektívnu sadzbu dane pre každú jurisdikciu, v ktorej pôsobia a platia tzv. dorovnávaciu daň (top-up tax) za rozdiel medzi efektívnou sadzbou dane v danej jurisdikcii a minimálnou sadzbou dane, ktorá je vo výške 15%. Ak vznikne povinnosť zaplatiť dorovnávaciu daň, spravidla sa platí v jurisdikcii konečného materského podniku nadnárodnej skupiny. Pravidlá GloBE sa vzťahujú len na daňovníkov, ktorí majú konsolidované výnosy minimálne 750 mil. eur a nebudú sa uplatňovať v prípadoch, keď v jurisdikcii vznikajú len relatívne nízke príjmy a výnosy.

⁴ Proposal for a Council Directive on Business in Europe: Framework for Income Taxation (BEFIT), COM/2023/532 final,

⁵ Proposal for COUNCIL DIRECTIVE establishing a Head Office Tax (HOT) system for micro, small and medium sized enterprises, and amending Directive 2011/16/EU, COM/2023/528 final

⁶ Smernica Rady (EÚ) 2025/50 z 10. decembra 2024 o rýchlejšej a bezpečnejšej úľave pri nadmerných zrážkových daniach (FASTER)

⁷ Proposal for a COUNCIL DIRECTIVE on laying down rules on a debt-equity bias reduction allowance and on limiting the deductibility of interest for corporate income tax purposes, COM/2022/216 final (DEBRA)

⁸ Ismer, R., Tax Technology for the European Union!, in: EC Tax Review, Volume 32, Issue 6, 2023, p. 234

⁹ OECD (2021), Tax Challenges Arising from the Digitalisation of the Economy – Global Anti-Base Erosion Model Rules (Pillar Two): Inclusive Framework on BEPS, OECD Publishing, Paris, <https://doi.org/10.1787/782bac33-en>.

¹⁰ Pozri OECD Globe

EU prijala smernicu Rady (EÚ) 2022/2523 zo 14. decembra 2022 o zabezpečení globálnej minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín v Únii (ďalej len „smernica o dorovnávej dani“). EU v plnej miere nadväzuje na OECD GloBE pravidlá, čo je vyjadrené v preambule smernice aj tým, že uvádza, že do textu smernice prevzala text dokumentu OECD: Daňové výzvy vyplývajúce z digitalizácie hospodárstva globálne modelové pravidlá proti narúšaniu základu dane (druhý pilier)¹¹ a zároveň aj odkazuje pri jej vykonávaní na sprievodné dokumenty OECD ku predmetným pravidlám, ako napr. príručka, príklady, komentár. Vykonávanie Pilieru 2, a teda aj tejto smernice, bude mať nevyhnutný vplyv na smernicu, ktorej hlavným cieľom je boj proti daňovým únikom, tzv. smernicu ATAD¹² a najmä na pravidlá ohľadne kontrolovaných zahraničných spoločností (CFC). Niektorí autori uvádzajú, že zavedenie smernice o dorovnávej dani môže vzbudiť otázky ohľadne ďalšej relevantnosti smernice ATAD, a to vzhľadom k tomu, že do určitej miery sledujú rovnaký cieľ, a vzhľadom k tomu, že momentálne je EU zameraná na znižovanie administratívnej záťaže v podobe aj znižovania reportovacích povinností¹³, najmä ak sa informácie v rámci reportov prelínajú, napr. aj s DAC 6.^{14,15} EÚ pravidlá týkajúce sa dorovnávej dane sa podľa smernice vzťahujú len na subjekty, ktoré musia splniť minimálne tieto tri podmienky: 1: nachádzajú sa v EÚ, 2: sú členmi veľkých vnútroštátnych skupín podnikov alebo nadnárodných skupín podnikov, 3. ich prah konsolidovaných výnosov za rok dosahuje minimálne 750 mil eur.¹⁶ Zodpovednosť za podanie oznámenia s informáciami relevantnými na stanovenie dorovnávej dane nesie v prvom rade základný subjekt. Avšak podľa čl. 44 ods. 3 smernice základný subjekt sa zbaví tejto povinnosti, ak oznámenie s príslušnými informáciami podal hlavný materský subjekt alebo iný určený podávajúci subjekt.¹⁷ Z dôvodu, aby sa medzi daňovými správami členských štátov EÚ zabezpečila dôsledná vedomosť o týchto oznámeniach, bolo potrebné zaviesť

¹¹ OECD (2021), Tax Challenges Arising from Digitalisation of the Economy – Global Anti-Base Erosion Model Rules (Pillar Two): Inclusive Framework on BEPS, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris, <https://doi.org/10.1787/782bac33-en>.

¹² Smernica Rady (EÚ) 2016/1164 z 12. júla 2016, ktorou sa stanovujú pravidlá proti praktikám vyhýbania sa daňovým povinnostiam, ktoré majú priamy vplyv na fungovanie vnútorného trhu

¹³ Draghi, M., The Future of European Competitiveness, Part A / A Competitiveness Strategy for Europe 65, 2024

¹⁴ Kofler, G., The „Decluttering“ of EU Direct Tax Law, In: EC Tax Review, Volume 34, Issue 1 (2025), p. 4

¹⁵ Hey, J. Editorial: Time for Rethinking: The ATAD experiment and the Conceptual Flaws of Its Hybrid Mismatch Rules, In: Intertax, Volume 52, Issue 11, 2024, p.670

¹⁶ Bod 7 preambuly smernice Rady (EÚ) 2022/2523 zo 14. decembra 2022 o zabezpečení globálnej minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín v Únii

¹⁷ Čl. 3 bod 44, čl. 44 smernice Rady (EÚ) 2022/2523 zo 14. decembra 2022 o zabezpečení globálnej minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín v Únii

automatickú výmenu informácií o týchto oznámeniach, čo je zabezpečené smernicou Rady (EÚ) 2025/872, ktorou sa mení smernica 2011/16/EÚ o administratívnej spolupráci v oblasti daní, tzv. DAC 9.

Slovenská republika reagovala na GloBE pravidlá OECD a v plnej miere transponovala smernicu Rady (EÚ) 2022/2523 zo 14. decembra 2022 o zabezpečení globálnej minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín v Únii do zákona č. 507/2023 Z.z. o dorovnávej dani na zabezpečenie minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín a o doplnení zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o dorovnávej dani“). Modelové pravidlá GloBE, ako aj smernica EU o dorovnávej dani umožňujú členským štátom, aby zaviedli vlastnú vnútroštátnu dorovnávaciu daň. Aj „*Slovenská republika sa vzhľadom na svoje postavenie tzv. zdrojového štátu/dovozcu kapitálu s nízkym počtom materských subjektov a vyšším počtom dcérskych subjektov a zároveň v záujme zamedzenia zdanenia príjmov dotknutých subjektov v zahraničí, rozhodla zabezpečiť minimálne zdanenie vo forme vnútroštátnej dorovnávej dane.*“¹⁸ Zodpovednosť za podanie oznámenia s informáciami relevantnými a potrebnými na stanovenie dorovnávej dane bola daná daňovníkovi, ktorý je stanovený v §37 zákona o dorovnávej dani, ktorým je: a) základný subjekt, ktorý nie je stálou prevádzkarňou; hlavný subjekt stálej prevádzkarne, ktorá je základným subjektom; a spoločný podnik a subjekt pridružený k spoločnému podniku. Zákon umožňuje daňovníkovi určiť iný subjekt – miestne určený subjekt, ktorý za neho podá správcovi dane predmetné oznámenie s informáciami potrebnými na určenie dorovnávej dane.¹⁹ Rovnako daňovník nie je povinný podať správcovi dane oznámenie s informáciami, ak za neho tieto informácie oznámil hlavný materský subjekt alebo určený podávajúci subjekt, ktorý sa nachádza v štáte, s ktorým má SR účinnú kvalifikovanú dohodu príslušných orgánov. V tomto prípade je daňovník alebo miestne určený subjekt povinný oznámiť správcovi dane identifikačné údaje hlavného materského subjektu alebo určeného podávajúceho subjektu a štát, v ktorom sa nachádzajú.²⁰ Daňovník oznamuje správcovi dane za príslušné zdaňovacie obdobie informácie potrebné na určenie dorovnávej dane, ktoré sú taxatívne vymenované v § 39 ods. 1 zákona o dorovnávej dani (napr. názov, adresa sídla, IČO, DIČ, typ daňovníka a jeho postavenie v rámci nadnárodnej skupiny podnikov alebo veľkej vnútroštátnej skupiny; informácie o podnikovej štruktúre nadnárodnej skupiny podnikov alebo veľkej vnútroštátnej skupiny a pod.). Predmetné informácie, ktoré sú súčasťou

¹⁸ Dôvodová správa – všeobecná časť k zákonu o dorovnávej dani

¹⁹ § 39 ods. 4 a ods. 5 zákona o dorovnávej dani

²⁰ §39 ods. 6 zákon o dorovnávej dani

oznámenia, je daňovník povinný oznámiť elektronickými prostriedkami FR SR, ako príslušnému správcovi dane v SR, a to najneskôr do 15 mesiacov po uplynutí oznamovaného účtovného obdobia. Alebo do 18 mesiacov, ak je oznamované účtovné obdobie prestupným rokom. Lehotu nie je možné predĺžiť ani jej zmeškanie odpustiť.²¹ Oznamované účtovné obdobie je zdaňovacie obdobie. Zdaňovacím obdobím v prípade dorovnávej dane je účtovné obdobie, za ktoré zostavuje konsolidovanú účtovnú závierku hlavný materský subjekt nadnárodnej skupiny podnikov alebo veľkej vnútroštátnej skupiny alebo kalendárny rok, ak ide o konsolidovanú účtovnú závierku podľa § 2 písm. i) štvrtého bodu zákona o dorovnávej dani.

DAC 9

Smernica Rady (EÚ) 2025/872 o 14. apríla 2025, ktorou sa mení smernica 2011/16/EÚ o administratívnej spolupráci v oblasti daní je úzko prepojená so smernicou EU o dorovnávej dani, ktorá v plnej miere nadväzuje na globálne modelové pravidlá proti narúšaniu základu dane (druhý pilier) – GloBE vytvorených OECD. Smernica EU o dorovnávej dani už obsahuje pravidlá týkajúce sa podávania oznámení s informáciami potrebnými na určenie dorovnávej dane a všeobecne aj uvádza kategórie oznamovaných informácií. Tieto oznámenia sú pre daňové správy podstatné na posúdenie rizika, zhodnotenie správnosti výpočtu daňovej povinnosti a na monitorovanie správnosti uplatňovania pravidiel ustanovených v smernici EU o dorovnávej dani.²² Smernica DAC 9 zavádza pravidlá na automatickú výmenu informácií v podobe oznámení s informáciami na určenie dorovnávej dane. Ak oznámenie s informáciami na určenie dorovnávej dane dostal príslušný orgán členského štátu nie od základného subjektu, ale od hlavného materského subjektu alebo určeného podávajúceho subjektu, v tom prípade tento príslušný orgán členského štátu by mal oznámiť ostatným príslušným orgánom členských štátov relevantné špecifické časti tohto oznámenia.²³

SR a DAC 9

Členské štáty majú implementovať smernicu DAC 9 do vnútroštátnych právnych poriadkov do 31. decembra 2025. Smernica DAC 9 sa začne uplatňovať od 1. januára 2026. Ministerstvo financií SR predložilo v priebehu júna 2025 do medzirezortného pripomienkového konania (MPK) návrh zákona, ktorým sa mení a dopĺňa zákon o dorovnávej dani (č. 507/2023 Z.z.), zákon č. 563/2009 Z.z. o správe daní, ako aj zákon č. 442/2012 Z.z. o medzinárodnej pomoci a spolupráci pri správe daní. Návrh

²¹ §39 ods. 1 a 2 zákona o dorovnávej dani

²² Preambula bod 2 smernice DAC 9

²³ Čl. 8ae smernice DAC 9

zákona bol schválený 21. októbra 2025 na 40. schôdzi Národnej rady SR a nadobudne účinnosť 1. januára 2026. 79 poslancov hlasovalo za tento návrh, 68 poslancov sa zdržalo a 5 poslancov nebolo prítomných. Zákon č. 291/2025 Z.z. z 21. októbra 2025, ktorým sa mení a dopĺňa zákon č. 507/2023 Z. z. o dorovnávej dani na zabezpečenie minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín a o doplnení zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v znení zákona č. 355/2024 Z. z. a ktorým sa mení a dopĺňa zákon č. 442/2012 Z. z. o medzinárodnej pomoci a spolupráci pri správe daní v znení neskorších predpisov (ďalej len „zákon k DAC 9“) predstavuje právny základ pre automatickú výmenu oznámení s informáciami na určenie dorovnávej dane na úrovni EÚ, tým že implementuje smernicu DAC 9 a právny základ aj pre automatickú výmenu oznámení na globálnej úrovni, ktorá sa bude uskutočňovať na základe Multilaterálnej medzinárodnej dohody príslušných orgánov štátov o výmene GloBE informácií,²⁴ tým že plne reaguje na celosvetové modelové pravidlá GloBE prijaté OECD v rokoch 2024 a 2025.

Automatická výmena informácií sa vykoná medzi kompetentným orgánom SR, ktorým je FR SR, a príslušnými orgánmi členských štátov EÚ (DAC 9) a príslušnými orgánmi zmluvných štátov Multilaterálnej medzinárodnej dohody príslušných orgánov štátov (OECD GloBE pravidlá).

Povinnosť predkladať príslušnému orgánu SR oznámenia o informáciách na určenie dorovnávej dane; zoznam informácií, ktoré obsahuje oznámenie; ako aj určenie daňovníkov, ktorí majú povinnosť predkladať príslušnému orgánu SR oznámenia o informáciách pre určenie dorovnávej dane vyplývajú zo zákona o dorovnávej dani.²⁵ Oznámenie s informáciami sa podáva prostredníctvom formulára určeného FR SR, ktorý bude kopírovať štandardný vzor oznámenia obsiahnutý v prílohe VII oddiele IV smernice DAC9. Predmetom automatickej výmeny budú oznámenia o informáciách pre určenie dorovnávej dane, ktoré podali daňovníci SR, „pričom v prvých obdobiach sa zohľadní postavenie Slovenskej republiky ako „štátu, ktorý uplatňuje len kvalifikovanú vnútroštátnu dorovnávaciu daň“.²⁶

FR SR, ako príslušný orgán, je povinný do 3 mesiacov po uplynutí lehoty na podanie oznámenia s informáciami potrebnými na určenie dorovnávej dane, zaslať informácie kompetentným orgánom príslušným štátom. Ak by bolo oznámenie

²⁴ OECD (2025), Tax Challenges Arising from the Digitalisation of the Economy – Multilateral Competent Authority Agreement on the Exchange of GloBE Information (January 2025), OECD/G20 Inclusive Framework on BEPS, OECD, Paris, <https://www.oecd.org/content/dam/oecd/en/topics/policy-subissues/global-minimum-tax/multilateral-competent-authority-agreement-exchange-of-globeinformation.pdf..>

²⁵ § 37 a § 39 ods. 1, ods. 2 zákona o dorovnávej dani

²⁶ Osobitná časť dôvodovej správy k § 22r k zákonu k DAC 9

podané po lehote, tak FR SR sa ponecháva 3 mesačná lehota od prijatia oznámenia na zaslanie týchto informácií kompetentným orgánom príslušných štátov.²⁷ Ako sme už uviedli v predchádzajúcej kapitole, daňovníci podávajú oznámenie s informáciami potrebnými na určenie dorovnávacjej dane podľa § 39 ods. 2 zákona o dorovnávacjej dani do 15 alebo 18 mesiacov po uplynutí oznamovaného obdobia.

Záver

Celý koncept výmeny informácií v oblasti daní a najmä automatickej výmeny smeruje k dosiahnutiu cieľa spravodlivejšieho daňového systému, v ktorom by existovala väčšia transparentnosť daní platených zo strany veľkých hospodárskych subjektov a najmä väčšia efektívnosť pri platení primeraného a hlavne spravodlivého podielu daní do príslušných štátov a jurisdikcií. Zároveň koncept výmeny informácií účinne napomáha k obmedzeniu, resp., eliminácii daňových únikov a vyhýbaniu sa daňovým povinnostiam, ku ktorým sa uchylujú najmä právnické osoby – veľké obchodné spoločnosti pôsobiace nadnárodne naprieč viacerými štátmi, jurisdikciami. Práve tieto veľké nadnárodné skupiny podnikov sa uchylujú k presúvaniu príjmov/ich ziskov do štátov s minimálnym alebo žiadnym daňovým zaťažením a tak platia minimálne alebo žiadne dane aj v štátoch, v ktorých vykonávajú svoju činnosť alebo v ktorých majú svojich používateľov/zákazníkov. Z uvedeného dôvodu sa na úrovni OECD, a následne aj na úrovni EÚ zaviedli nástroje, ktoré by mali zabezpečiť, že tieto skupiny podnikov zaplatia aspoň minimálnu efektívnu výšku dane v zmysle dohodnutej metodiky a vzorca výpočtu podľa Pilieru 2, ktorý predstavuje dorovnávaciu daň a ktorá bola stanovená vo výške 15%. Informácie potrebné na určenie dorovnávacjej dane sú súčasťou oznámenia predkladaného príslušnými daňovníkmi príslušným orgánom štátov. Aby sa tieto oznámenia s podstatnými informáciami dostali k príslušným orgánom príslušných štátov, tak je potrebná ich automatická výmena, ktorá sa má zabezpečiť smernicou DAC 9.

Zoznam použitej literatúry

Odborné články:

1. Ismer, R., Tax Technology for the European Union!, in: EC Tax Review, Volume 32, Issue 6, 2023, p. 234
2. Kofler, G., The „Decluttering“ of EU Direct Tax Law, In: EC Tax Review, Volume 34, Issue 1 (2025), p. 4

²⁷ § 22 ods. 4 a 5 zákona k DAC 9

3. Hey, J. Editorial: Time for Rethinking: The ATAD experiment and the Conceptional Flaws of Its Hybrid Mismatch Rules, In: Intertax, Volume 52, Issue 11, 2024, p.670
4. Draghi, M., The Future of European Competitiveness, Part A / A Competitiveness Strategy for Europe 65, 2024

Dokumenty OECD a Európskej komisie

1. Oznámenie Komisie Európskemu parlamentu a Rade z 18. mája 2021: Zdaňovanie podnikov v 21. storočí COM(2021) 251 final
2. OECD (2021), Tax Challenges Arising from the Digitalisation of the Economy – Global Anti-Base Erosion Model Rules (Pillar Two): Inclusive Framework on BEPS, OECD Publishing, Paris, <https://doi.org/10.1787/782bac33-en>.
3. OECD (2025), Tax Challenges Arising from the Digitalisation of the Economy – Multilateral Competent Authority Agreement on the Exchange of GloBE Information (January 2025), OECD/G20 Inclusive Framework on BEPS, OECD, Paris, <https://www.oecd.org/content/dam/oecd/en/topics/policy-subissues/global-minimum-tax/multilateral-competent-authority-agreement-exchange-of-globeinformation.pdf>.

Právne akty EÚ

1. Smernica Rady (EÚ) 2016/1164 z 12. júla 2016, ktorou sa stanovujú pravidlá proti praktikám vyhýbania sa daňovým povinnostiam, ktoré majú priamy vplyv na fungovanie vnútorného trhu
2. smernice Rady (EÚ) 2022/2523 zo 14. decembra 2022 o zabezpečení globálnej minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín v Únii
3. Smernica Rady (EÚ) 2025/872 o 14. apríla 2025, ktorou sa mení smernica 2011/16/EÚ o administratívnej spolupráci v oblasti daní
4. Smernica Rady (EÚ) 2025/50 z 10. decembra 2024 o rýchlejšej a bezpečnejšej úľave pri nadmerných zrážkových daniach (FASTER)
5. Proposal for a Council Directive on Business in Europe: Framework for Income Taxation (BEFIT), COM/2023/532 final,
6. Proposal for COUNCIL DIRECTIVE establishing a Head Office Tax (HOT) system for micro, small and medium sized enterprises, and amending Directive 2011/16/EU, COM/2023/528 final
7. Proposal for a COUNCIL DEIRECTIVE on laying down rules on a debt.equity biac reduction allowance and on limiting the deductability of interest for corporate income tax purposes, COM/2022/216 final (DEBRA)

Právne akty SR

1. zákon č. 507/2023 Z.z. o dorovnávej dani na zabezpečenie minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín a o doplnení zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
2. Zákon č. 291/2025 Z.z. z 21. októbra 2025, ktorým sa mení a dopĺňa zákon č. 507/2023 Z. z. o dorovnávej dani na zabezpečenie minimálnej úrovne zdanenia nadnárodných skupín podnikov a veľkých vnútroštátnych skupín a o doplnení zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v znení zákona č. 355/2024 Z. z. a ktorým sa mení a dopĺňa zákon č. 442/2012 Z. z. o medzinárodnej pomoci a spolupráci pri správe daní v znení neskorších predpisov
3. Všeobecná a osobitná časť dôvodovej správy k zákonu č. 291/2025 Z.z.
4. Všeobecná a osobitná časť dôvodovej správy k zákonu č. 507/2023 Z.z.

Kontaktné údaje

Mgr. Andrea Szakács, PhD.
andrea.szakacs@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta
Katedra finančného práva

Sekcia obchodného a hospodárskeho práva
Digitalizácia podnikateľského prostredia a umelá
inteligencia v obchodnom práve

MANIPULATÍVNE PRAKTIKY OBCHODNÍKOV V DIGITÁLNOH PROSTREDÍ – PRÁVNA KVALIFIKÁCIA TZV. *DARK PATTERNS*

MANIPULATIVE PRACTISES OF TRADERS IN THE DIGITAL ENVIRONMENT - LEGAL QUALIFICATION OF THE SO - CALLED *DARK PATTERNS*

Regina Šťastová¹

Abstrakt: Príspevok sa zameriava na problematiku manipulatívnych praktík, bežne označovaných ako „*dark patterns*“, ktoré obchodníci čoraz častejšie využívajú v digitálnom prostredí, najmä v digitálnom marketingu. Tieto praktiky sú často zamerané na zneužívanie postavenia spotrebiteľa a na ovplyvňovanie jeho správania v spotrebiteľskej zmluve. V mnohých prípadoch uvedené praktiky totiž naplňajú znaky nekalých obchodných praktík v dôsledku čoho je spotrebiteľ v spotrebiteľskom vzťahu vystavený značnému riziku. Hlavným cieľom je preto analyzovať postavenie uvedených praktík v právnom poriadku Slovenskej republiky, ako aj v práve Európskej únie. Okrem uvedeného je cieľom príspevku vymedziť hranicu medzi prípustnými marketingovými technikami obchodníka a už neprípustnými praktikami, ktoré naplňajú znaky nekalých obchodných praktík pre spotrebiteľa. Využívanie manipulatívnych praktík označovaných ako *dark patterns* obchodníkom vo vzájomných vzťahoch so spotrebiteľom je vo viacerých prípadoch možné subsumovať pod znaky nekalej obchodnej praktiky podľa zákona o ochrane spotrebiteľa. Nemožno však dospieť k záveru, že každá kategória či forma *dark patterns* naplňa znaky nekalej obchodnej praktiky v spotrebiteľskom vzťahu, keďže slovenský právny poriadok ponecháva hranicu medzi spomínanými praktikami a prípustným marketingom obchodníka relatívne neurčitú. Určenie danej hranice je nejasné aj z dôvodu absencie explicitnej právnej úpravy takéhoto konania zo strany obchodníka.

Kľúčové slová: B2C, digitálne prostredie, digitálny marketing, „*dark patterns*“, ochrana spotrebiteľa, nekalé obchodné praktiky.

¹ Ústav štátu a práva, Slovenská akadémia, v. v. i.

Abstract: The article focuses on manipulative practises, commonly referred to as "*dark patterns*", that traders are increasingly using in the digital environment, especially in digital marketing. These practises are often aimed at exploiting the consumer's position and influencing their behaviour in consumer contracts. In many cases, these practises constitute unfair commercial practices, as a result of which consumers are exposed to considerable risk in consumer relations. The main objective is therefore to analyse the status of these practises in the legal system of the Slovak Republic and in European Union law. In addition, the aim of this paper is to define the boundary between permissible marketing practises used by traders and impermissible practises that constitute unfair commercial practices for consumers. The use of manipulative practises known as dark patterns by traders in their relations with consumers can in many cases be subsumed under the characteristics of unfair commercial practices under the Civil Code or the Consumer Protection Act. However, it cannot be concluded that every category or form of dark pattern constitutes an unfair commercial practice in a consumer relationship, as Slovak law leaves the boundary between these practises and permissible marketing by traders relatively vague. The determination of this line is also unclear due to the absence of explicit legal regulation of such conduct on the part of the trader.

Key words: B2C, digital environment, "dark patterns", consumer protection, unfair commercial practices.

Úvod

Digitalizácia a rastúci vplyv informačných technológií na všetky aspekty záväzkových vzťahov prinášajú nielen nové príležitosti, ale zároveň vyvolávajú doteraz neriešené etické a právne výzvy. V oblasti digitálneho obchodu, najmä pri uzatváraní spotrebiteľských zmlúv, sa čoraz častejšie stretávame s obchodnou praxou, ktorej podstatou je psychologické ovplyvňovanie rozhodovania spotrebiteľa v prospech samotného obchodníka. Táto prax v odbornej literatúre a aplikačnej praxi označovaná ako „*dark patterns*“ (v slov. prekl. „*temné vzory*“), predstavuje komplexný súbor manipulatívnych praktík,² ktoré zámerne zneužívajú ľudskú psychiku a vyvolávajú kognitívne skreslenie u spotrebiteľa. Práve online priestor vystavuje

² Pozn. autorky: V praxi nejde o jediné konanie obchodníka s negatívnym dopadom na spotrebiteľa. Okrem týchto praktík sa môže obchodník dopustiť aj iných nekalých obchodných praktík voči spotrebiteľovi. Za nekalé obchodné praktiky sa považujú aj tie, ktoré sú uvedené označené v prílohe č. 1 zákona č. 108/2024 Z. z. o ochrane spotrebiteľa. Za nekalú obchodnú praktiku možno považovať nepravdivé tvrdenia obchodníka, pyramidové schémy, nátlakové alebo inak agresívne konanie voči spotrebiteľovi, a ďalšie skutkové podstaty. Tento príspevok sa zameriava výlučne na právne posúdenie manipulatívnych praktík označovaných ako dark patterns.

spotrebiteľov najväčšiemu riziku a stávajú sa tak pre obchodníkov ľahkým cieľom. Cieľom príspevku je preto nielen analyzovať postavenie uvedených praktík v právnom poriadku Slovenskej republiky³ a v práve Európskej únie, ale aj identifikovať zákonne prípustnú mieru využívania marketingových praktík v digitálnom prostredí zo strany obchodníka. Na tomto základe príspevok vychádza z dvoch základných hypotéz:

1. *Používanie manipulatívnych praktík označovaných ako dark patterns v digitálnom prostredí napĺňa znaky nekalej obchodnej praktiky podľa zákona č. 108/2024 Z. z. o ochrane spotrebiteľa; pričom ich právna kvalifikácia môže viesť k vzniku zodpovednosti u obchodníka.*
2. *Nie všetky doteraz známe formy manipulatívnych praktík dark patterns možno právne kvalifikovať ako nekalé obchodné praktiky v zmysle horeuvedených zákonov, keďže hranica medzi prípustnou marketingovou činnosťou obchodníka a už neprípustnou manipuláciou spotrebiteľa zostáva v slovenskom právnom poriadku vágnou.*

Metodologicky príspevok vychádza z vedeckého výskumu založeného na systematickej analýze postavenia manipulatívnych praktík v právnom poriadku Slovenskej republiky ako aj v práve Európskej únie, a to prostredníctvom skúmania relevantných prameňov práva. Závety príspevku sú formulované na základe syntézy získaných poznatkov, pričom deduktívna metóda slúži na potvrdenie alebo vyvrátenie stanovených hypotéz.

Úvod do problematiky – vymedzenie manipulatívnych praktík obchodníka

Ako už bolo spomenuté v úvode, manipulatívne praktiky obchodníkov tzv. *dark patterns* negatívne vplyvajú na osobu spotrebiteľa. Empirický výskum realizovaný na vzorke 11 000 internetových obchodov identifikoval 1 818 prípadov výskytu takýchto foriem manipulatívnych praktík, pričom boli prítomné až na 1 254 webových stránkach, čo predstavuje výskyt u 11,1 % skúmaných obchodníkov.⁴ Uskutočnený výskum zároveň potvrdil, že čím populárnejší bol daný internetový obchod, tým vyššia bola pravdepodobnosť výskytu manipulatívnych praktík.⁵ Ďalší empirický

³ Pozn. autorky: Tento príspevok sa nezameriava na uvedenú problematiku z pohľadu práva na ochranu proti nekalej súťaži. Otázky nekalosúťažného konania podľa zákona č. 513/1991 Zb. Obchodný zákonník sú preto zámerne ponechané mimo rámca skúmania a budú predmetom samostatného výstupu. Všeobecne k ochrane spotrebiteľa proti nekalej súťaži bližšie pozri: ZLOCHA, Ľubomír - STRÉMY, Jana: Nekalá súťaž. Generálna klauzula, menej tradičné prípady a zahraničné právne úpravy. Bratislava: C. H. Beck, (2023), s. 41 – 170.

⁴ MATHUR, Arunesh. et al. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. In: Proceedings of the ACM on Human-Computer Interaction. New York: Association for Computing Machinery, Volume 3, Article 81, (2019), p. 2.

⁵ Tamtiež.

výskum poukázal na výskyt až 2 320 prípadov použitia manipulatívnych praktík *dark patterns* u 105 poskytovateľov služieb v rôznych prostrediach, vrátane ich výskytu v aplikáciách, mobilnom webe alebo v klasickom desktopovom webe, pričom sa manipulatívne praktiky najčastejšie vyskytovali v mobilných aplikáciách.⁶ Potvrdilo sa, že každý poskytovateľ služieb (celkovo 105 subjektov) mal vo svojom prostredí aspoň jednu manipulatívnu praktiku a zároveň „najtemnejší“ poskytovatelia používali až 18 rôznych typov manipulatívnych praktík *dark patterns* na službu.⁷ Rovnako tak v 240 aplikáciách, bežne používaných spotrebiteľmi sa manipulatívne praktiky *dark patterns* vyskytli až v 95 % prípadov, pričom obľúbené aplikácie spotrebiteľov ich v priemere obsahovali minimálne sedem.⁸ Ide o manipulatívne praktiky *dark patterns*, ako je manipulácia s vizuálnym usporiadaním prvkov, prednastavenie možností bez vedomosti spotrebiteľa, ponúkajúce dočasne výhodných ponúk či skrytie dôležitých informácií, ktoré by vo výraznej miere mohli ovplyvniť rozhodnutie spotrebiteľa. Okrem toho sú najrozšírenejšími *dark patterns* praktikami aj otravovanie spotrebiteľa, zložitá možnosť na zrušenie, nútená registrácia, ktoré využívajú aj najpopulárnejšie webové stránky a aplikácie spotrebiteľov v rámci Európskej únie.⁹

Najzásadnejším zistením je časť výskumu, ktorá poukázala na skutočnosť, že väčšina oslovených používateľov (z celkového počtu 589 účastníkov výskumu) nedokázala rozpoznať manipulatívnu praktiku typu *dark pattern* alebo si jej rozpoznaním nebola istá.¹⁰ Za dôvod neistoty označili účastníci to, že *dark patterns* sú v súčasnosti tak rozšírené a bežné, že sa stávajú súčasťou interakčného toku pri používaní aplikácií.¹¹ Uvedené výskumy jednoznačne poukazujú na dva významné dopady na osobu spotrebiteľa. Prvým z nich je skutočnosť, že manipulatívne praktiky *dark patterns* sú

⁶ GUNAWAN, Johanna. et al.: A Comparative Study of Dark Patterns Across Mobile and Web Modalities In: Proceedings of the 22nd ACM Internet Measurement Conference. New York: Association for Computing Machinery, Article 377, (2021), p. 13.

⁷ Tamtiež, p. 13.

⁸ DI GERONIMO, Linda - BRAZ, Larissa - FREGNAN, Enrico - PALOMBA, Fabio - BACCHELLI, Alberto: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In: Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems. New York: Association for Computing Machinery, (2020), p. 1.

⁹ LUPIÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-05]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>, p. 120.

¹⁰ DI GERONIMO, Linda - BRAZ, Larissa - FREGNAN, Enrico - PALOMBA, Fabio - BACCHELLI, Alberto: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In: Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems. New York: Association for Computing Machinery, (2020), p. 9.

¹¹ Tamtiež, p. 9.

v súčasnosti bežnou súčasťou činnosti obchodníkov bez ohľadu na prostredie, v ktorom sa vyskytujú, či už ide o tradičný spotrebiteľský styk alebo o digitálne prostredie. Z vykonaných výskumov však možno vidieť ich zvýšenú prítomnosť v digitálnom prostredí, ako sú aplikácie alebo webové rozhrania. Druhým zistením je, že integrácia *dark patterns* do každodennej obchodnej praxe vo výraznej miere ohrozuje úsudok spotrebiteľov. Čoraz častejšie sa stáva, že priemerný spotrebiteľ nedokáže správne a včas identifikovať ich prítomnosť v spotrebiteľskom styku ani nástrahy, ktoré tieto praktiky prinášajú. Manipulatívne praktiky *dark patterns* tak narúšajú ochranu spotrebiteľa a vo výraznej miere zvyšujú jeho zraniteľnosť aj v digitálnom prostredí.

Negatívny dopad *dark patterns* sa prejavuje najmä v povahe samotných manipulatívnych praktík. Používané *dark patterns* a ich povaha zahŕňajú rôzne skryté, klamlivé informácie alebo svojou povahou smerujú k utajeniu relevantných informácií.¹² Tieto manipulatívne praktiky využívajú postupy a vzorce, ktoré svojim charakterom alebo formou uvádzajú spotrebiteľov do omylu a / alebo zároveň zámerne zatajújú pravdivé informácie, ktoré by pre spotrebiteľa mohli byť rozhodujúce pri vstupe do spotrebiteľského vzťahu s obchodníkom. Zásadne tak obmedzujú slobodnú voľbu spotrebiteľa a jeho práva na prístup k informáciám.¹³

Zároveň mnohé *dark patterns* praktiky používajú dva efekty so zásadným dopadom na spotrebiteľa. Premyslené a sofistikované využívanie psychologických mechanizmov spotrebiteľského správania a zneužívanie kognitívneho skreslenia spotrebiteľov je postavené na predvolenom efekte (z. angl. *default effect*) a efekte rámcovania rozhodnutia (z. angl. *framing effect*).¹⁴ Podstatou nastavenia predvoleného efektu pri rozhodovaní spotrebiteľa je odstrániť kognitívnu záťaž a eliminovať potrebu aktívne sa rozhodnúť v danom momente.¹⁵ Spotrebiteľ sa tak v danom momente cíti zbavený potreby neustále prijímať rozhodnutia, ktoré sú súčasťou každodenného života a bežných aktivít počas dňa. Efekt rámcovania ovplyvňuje podvedomú úroveň jednotlivca, pričom jeho podstatou je vplyv

¹² MATHUR, Arunesh. Et al. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. In: Proceedings of the ACM on Human-Computer Interaction. New York: Association for Computing Machinery, Volume 3, Article 81, (2019), s. 2.

¹³ K náčrtu práv spotrebiteľa pozri: EURÓPSKA SPOTREBITEĽSKÁ ORGANIZÁCIA. Všeobecné spotrebiteľské právo – Teoretický východiskový dokument. 1. verzia. [online]. Luxemburg: BEUC, 2021. Dostupné na:

https://www.beuc.eu/sites/default/files/publications/consumerpro_consumer_rights_tbd_sk.pdf.

¹⁴ MATHUR, Arunesh. Et al. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. In: Proceedings of the ACM on Human-Computer Interaction. New York: Association for Computing Machinery, Volume 3, Article 81, (2019), p. 2.

¹⁵ MONEYTHOR. The Default Effect: Behavioural Science in Banking. [online]. 2022. [cit. 2025-09-15]. Dostupné na: <https://www.moneythor.com/analysis-opinions/behavioural-science/the-default-effect-behavioural-science-in-banking/>.

subjektívnej interpretácie informácií, ktorá je priamo závislá na spôsobe, akým tieto informácie sú v praxi podávané a nie ich objektívneho uchopenia.¹⁶ Samotný efekt však nemusí byť v praktickej rovine vždy vnímaný negatívne. Efekt rámcovania môže byť využívaný aj k pozitívnym dopadom na jednotlivca, pričom jeho využitie môže pôsobiť v prospech, napríklad na zlepšenie komunikácie.¹⁷ Pri využití efektu rámcovania rozhodnutia spotrebiteľa je vždy kľúčový úmysel obchodníka.

Okrem uvedených efektov môžu na rozhodovanie spotrebiteľa vplývať aj ďalšie mechanizmy kognitívneho skreslenia. Medzi najznámejšie patria:

- efekt ukotvenia (z ang. *anchoring effect*), ktorého podstatou je vytvoriť počiatočnú informáciu, tzv. kotvu pre budúce rozhodnutia jednotlivca;
- stádový efekt (z ang. *bandwagon effect*), ktorého podstatou je vytvoriť pozitívny dojem jednotlivca na základe dojmov od iných ľudí;
- efekt skreslenia nedostatku (z ang. *scarcity bias*), ktorého podstatou je sklon jednotlivcov pripisovať vyššiu hodnotu veciam, ktoré sú vzácne a ktoré sa ťažšie získavajú;
- a ďalšie efekty.¹⁸

Mnohé manipulatívne praktiky teda nezahŕňajú iba jeden spôsob ovplyvňovania psychiky a kognitívneho skreslenia spotrebiteľa, ale predstavujú súhrn efektov a spôsobov, akými obchodník na nich pôsobí. Nemusí ísť len o pôsobenie na spotrebiteľa, ktoré vedie k uzatvoreniu spotrebiteľskej zmluvy, ale môže na spotrebiteľa pôsobiť počas jej trvania, prípadne môže spotrebiteľovi sťažiť alebo dokonca znemožniť ukončiť spotrebiteľský vzťah. Na základe uvedených štatistík možno hovoriť už o systémovom výskyte manipulatívnych praktík *dark patterns* v digitálnom obchode a nie len o ojedinelých prípadoch používania rôznych marketingových stratégií obchodníkom s negatívnym dopadom na spotrebiteľa. Dôležité je preto ich pojmové vymedzenie.

Pojem „dark patterns“

Terminologicky možno pojem „dark patterns“ vymedziť ako „*pojem, ktorý sa všeobecne používa na označenie praktík v digitálnych rozhraniach, ktoré vedú, klamú, nútia alebo manipulujú spotrebiteľov, aby robili rozhodnutia, ktoré často nie sú v ich*“

¹⁶ PSYCHOINFO.SK. Framing efekt (efekt rámcovania). [online]. 2025. [cit. 2025-09-15]. Dostupné na: <https://psychoinfo.sk/psychologicky-slovník/framing-efekt-efekt-ramcovania/>.

¹⁷ Tamtiež.

¹⁸ MATHUR, Arunesh. Et al. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. In: Proceedings of the ACM on Human-Computer Interaction. New York: Association for Computing Machinery, Volume 3, Article 81, (2019), p. 6.

najlepšom záujme".¹⁹ Spoločným cieľom praktík je tak prinútiť spotrebiteľov, aby si kúpili, resp. kúpili viac alebo pokračovali v nákupe tovaru alebo služby, ktorú by inak nekúpili alebo by ju v konečnom dôsledku iba kúpili v menšom množstve.²⁰ Cieľom je tak zabezpečiť, aby spotrebiteľia naplnili obchodný model obchodníka v čo najvyššej možnej miere. Zároveň možno manipulatívne praktiky *dark patterns* v teórii zadefinovať ako „*obchodné praktiky využívajúce prvky digitálnej architektúry voľby, najmä v online používateľských rozhraniach, ktoré narúšajú alebo zhoršujú autonómiu, rozhodovanie alebo voľbu spotrebiteľov*"; a to tak, že „*často klamú, nútia alebo manipulujú so spotrebiteľmi a pravdepodobne spôsobia priamu alebo nepriamu ujmu spotrebiteľom rôznymi spôsobmi, hoci v mnohých prípadoch môže byť ťažké alebo nemožné takúto ujmu merať*." Na úrovni práva Európskej únie možno nachádzať definíciu v Nariadení Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES. Toto nariadenie definuje *dark patterns* ako praktiky „*ktoré zámerne alebo fakticky narúšajú alebo oslabujú schopnosť príjemcov služby prijímať samostatné a informované rozhodnutia*"; a zároveň „*môžu byť využívané na presvedčovanie príjemcov služby na nechcené správanie alebo na nežiaduce rozhodnutia, ktoré majú pre nich negatívne dôsledky*".²¹ Nariadenie zároveň v článku 25 obsahuje explicitný zákaz poskytovateľov online platforiem akýmkoľvek spôsobom zavádzať alebo manipulovať s príjemcami ich služieb a to tak, aby sa nenarušila schopnosť príjemcov prijímať slobodné a informované rozhodnutia.²²

Právny poriadok Slovenskej republiky popri práve Európskej únie vo svojom znení neobsahuje pojem ani legálnu definíciu „*dark patterns*". V primeranom rozsahu sa na poskytovateľov bude priamo vzťahovať uvedené nariadenie.

¹⁹ LUPÍÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-10]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>, p. 20.

²⁰ OECD. Dark commercial patterns. OECD Digital Economy Papers, number 336. Paríž: OECD. [Online]. 2022. [cit. 2025-09-08]. Dostupné na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf, p. 8.

²¹ 67 bod. Preambuly.

²² Pozn. autorky: Uvedený zákaz sa nevzťahuje na postupy uvedené v Smernici Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 (ďalej len „smernica o nekalých obchodných praktikách"); a zároveň na postupy zakotvené vo všeobecnom nariadení o ochrane osobných údajov.

V súčasnosti možno badať značnú terminologickú nekonzistentnosť pojmu a jednotlivých kategórií *dark patterns* v literatúre.²³ Citované definície sa v celku svojím obsahom nestotožňujú, ale možno identifikovať spoločné znaky týchto manipulatívnych praktík. Za základné spoločné znaky manipulatívnych praktík možno označiť:

- manipulatívny charakter konania obchodníka voči spotrebiteľovi – t. j. *praktiky určitým spôsobom vedú, klamú, zavádzajú, nútia alebo inak zasahujú do správania spotrebiteľa*;
- zásah do autonómie spotrebiteľa – t. j. *zásah narúša schopnosť spotrebiteľa samostatne a informovane sa rozhodnúť na základe slobodnej vôle*;
- ekonomický cieľ obchodníka – t. j. *obchodník využíva manipulatívne praktiky s cieľom obohatiť sa na úkor spotrebiteľa*;
- vznik ujmy na strane spotrebiteľa – t. j. *dochádza k určitému ohrozeniu alebo poškodeniu práv spotrebiteľa*.

Manipulatívne praktiky *dark patterns* sú charakterizované určitou špecifickou formou konania obchodníka voči spotrebiteľovi. Obchodník priamo alebo nepriamo určitým negatívnym spôsobom ovplyvňuje spotrebiteľovo rozhodnutie. Konanie obchodníka môže mať klamlivý, zavádzajúci, donucujúci alebo až nátlakový charakter. Môže pôsobiť priamo na osobu spotrebiteľa a jeho rozhodnutie alebo nepriamo. Za *dark patterns* sa najmä považujú tie, ktoré sú klamlivé a neodrážajú najlepší záujem spotrebiteľov, teda nie každá marketingová praktika bude hneď označovaná aj ako *dark patterns* praktika, no v súčasnosti je hranica medzi prípustnosťou a už neprípustnou praktikou čoraz viac rozmazaná.²⁴ Manipulatívne praktiky *dark patterns* však vždy zasahujú do autonómie spotrebiteľa. Spotrebiteľ tak v dôsledku ich využitia nedokáže urobiť slobodné a informované rozhodnutie pred a počas trvania spotrebiteľského vzťahu. Dôsledkom je rozhodnutie, ktoré by v opačnom prípade spotrebiteľ nikdy neurobil. Čo znamená, že ak by obchodník nevyužil voči spotrebiteľovi vybranú manipulatívnu praktiku spotrebiteľ by urobil iné rozhodnutie, ktorého výsledkom nemusí byť uzatvorenie spotrebiteľskej zmluvy, resp. vstup do spotrebiteľského vzťahu s obchodníkom. Manipulatívne praktiky *dark patterns* sledujú spoločný cieľ, a to zabezpečiť obchodníkovi prospech, ktorý by bez ich

²³ K tomu pozri: ISOLA, Cecilia - ESPOSITO, Fabrizio: A systematic literature review on dark patterns for the legal community: definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. In: Computer Law & Security Review. United Kingdom: Elsevier, volume 58, number 106169, (2025). [online]. 2025. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S2212473X25000422?via%3Dihub>, p. 10.

²⁴ SIN, Ray - HARRIS, Ted - NILSSON, Simon - BECK, Talia: Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying? In: Behavioural Public Policy, Cambridge: Cambridge University Press, volume 9, (2025), p. 81.

využitia nebol pre obchodníka garantovaný. Obchodník tak využíva manipulatívne praktiky vo svoj prospech na úkor osoby spotrebiteľa.

Manipulatívne praktiky *dark patterns* a ich následok vedie k ohrozeniu alebo vzniku ujmy na strane spotrebiteľa. V uvedenom prípade nemusí dochádzať iba k vzniku majetkovej ujmy, niektoré *dark patterns* praktiky totiž môžu viesť aj k vzniku nemajetkovej ujmy. Výrazne tak manipulatívne praktiky vedú k ohrozeniu alebo porušeniu práv spotrebiteľa, ktoré mu priznáva právny poriadok, alebo právo Európskej únie. Spoločným kľúčovým znakom každej manipulatívnej praktiky *dark patterns* je nielen ich manipulatívna alebo klamlivá povaha, ale aj následok ich využitia. Následok využitia bude mať v každom prípade negatívny alebo škodlivý výsledok. Jednotlivé formy *dark patterns*, ako napríklad dotieravé obťažovanie spôsobuje aj nepriame následky, vrátane zvyšovania zraniteľnosti spotrebiteľov voči porušeniam ich súkromia a výrazne uľahčujú protisúťažné konanie obchodníkov.²⁵

Osobitnú kategóriu manipulatívnych praktík *dark patterns* tvoria tzv. *hyper-pútavé dark patterns* (z angl. *hyper-engaging dark patterns*), ktoré predstavujú sofistikovanejšiu a intenzívnejšiu formu *dark patterns* praktiky. Ide o praktiky, ktoré využívajú obchodníci v digitálnom prostredí. Využitie týchto praktík smeruje k manipulácii používateľov, vrátane spotrebiteľov prostredníctvom rozhrania, a to tak, aby si daný používateľ vytvoril zvyk používať poskytovanú službu.²⁶ Uvedený návyk si tak používateľ vytvorí pomocou adaptívnych algoritmov a dátovo riadeného dizajnu rozhrania.²⁷ Cieľene sa zameriavajú na pozornosť spotrebiteľa v digitálnom prostredí. Nastavenie algoritmov a dizajnu smeruje k zabezpečeniu udržania spotrebiteľa pomocou nekončiaceho skrolovania, automatického prehrávania obsahu, rôznymi vyskakovacími oknami, vizualizáciami a pod. Svojou podstatou po celý čas pútajú pozornosť používateľov prostredníctvom rôznych dizajnových stratégií, pričom ohrozia ich schopnosť robiť racionálne rozhodnutia a nútia ich konať automaticky.²⁸ Často pritom poskytovatelia upravujú algoritmy a ich zobrazený obsah na základe predchádzajúcich interakcií s používateľom, čím zvyšujú u používateľa pocit odmeny a posilňujú pozitívne správanie k smerom používateľovi.²⁹ Ide teda o ľahkú rovnicu založenú na odmene pre používateľa, ktorá uňho vyvolá pozitívne pocity, čím si poskytovateľ zabezpečí, že

²⁵ [HUNG, Alison: Keeping Consumers in the Dark: Addressing “Nagging” Concerns and Injury. In: Columbia Law Review. New York: Columbia Law Review Association, volume 121, number 8, \(2021\), p. 2488.](#)

²⁶ ESPOSITO, Fabrizio - FERREIRA, Cathoud Maciel Thaís: Addictive Design as an Unfair Commercial Practice: The Case of Hyper -Engaging Dark Patterns. In: European Journal of Risk Regulation. Cambridge: Cambridge University Press, volume 15, special issue 4, (2024), p. 1000.

²⁷ Tamtiež, pp. 999 – 1000.

²⁸ Tamtiež, p. 1000.

²⁹ Tamtiež, pp. 1000 – 1001.

daný používateľ zopakuje svoje konanie aj do budúcnosti. V praxi tak pocit odmeny zvyšuje pravdepodobnosť budúcej interakcie používateľa s poskytovateľom.

V závere časti definície pojmu „*dark patterns*“ je na mieste vymedziť si dva úzko súvisiace pojmy, a to pojem „*technika*“ a pojem „*praktika*“. Technika označuje určitý spôsob alebo postup, prípadne vykonávanie činnosti, ako aj odbornú schopnosť.³⁰ Praktiku možno vymedziť ako osvedčený spôsob realizácie niečoho, pričom má aj iný význam. Zároveň možno praktiku vymedziť ako neprimeraný, až zlý postup a podvod.³¹ Vzhľadom na povahu a charakter konania obchodníka pri využití *dark patterns* je vhodnejšie používať v uvedenom kontexte pojem „*praktika*“, teda *praktika dark patterns*. Negatívne ponímanie praktiky tak odráža naplnenie vyššie uvedených definičných znakov manipulatívnych praktík *dark patterns*.

Kategórie a formy *dark patterns*

Existuje niekoľko foriem praktík *dark patterns* v spotrebiteľských vzťahoch v digitálnom priestore. Podľa jednotlivých kategórií možno rozlišovať niekoľko foriem, a to:

1. Založené na sociálnom aspekte:
 - *Správy o aktivite (nepravdivé, zavádzajúce informácie o nákupoch iných)*
 - *Recenzie (nepravdivé, zavádzajúce pozitívne recenzie od zákazníkov),*
2. Založené na časovom naliehaní:
 - *Odpočítavanie času (časomer s vizuálnym signálom obmedzenej ponuky),*
 - *Časovo obmedzená správa (správa obsahuje informáciu o obmedzenej príležitosti);*
3. Založené na určitej prekážke:
 - *Roach motel (asymetria medzi založením a zrušením napríklad účtu jednotlivca),*
 - *Zabránenie možnosti porovnať ceny (zabraňuje alebo znemožňuje porovnať ceny),*
 - *Virtuálna mena (donucuje jednotlivca používať virtuálnu menu namiesto zobrazovania cien v reálnej mene),*
 - *„Nesmrtelné účty“ (účet a údaje jednotlivca nie sú možné trvalo vymazať),*
4. Založené na donútení:
 - *Spam od priateľov/ sociálna pyramída/ vykrádanie adresára (je založená na manipulatívnom získavaní informácií o iných používateľoch),*
 - *Zneužívanie súkromia (nedobrovoľné zdieľanie údajov jednotlivca),*

³⁰ Jazykovedný ústav Ľ. Štúra SAV. Technika. Slovník cudzích slov [online]. 2005. [cit. 2025-09-25]. Dostupné na: https://www.juls.savba.sk/slovník_cudzích_slov_2005.html.

³¹ Jazykovedný ústav Ľ. Štúra SAV. Praktika. Historický slovník slovenského jazyka. [online]. 2008. [cit. 2025-09-25]. Dostupné na: <https://www.juls.savba.sk/hssj.html>.

- *Gamifikácia (funkcie sa získavajú opakovaným používaním),*
- *Nútená registrácia (uviedenie do omylu jednotlivca o tom, že registrácia je potrebná);*
- a ďalšie iné kategórie a formy dark patterns.³²

Právna literatúra rozlišuje viacero kategorizácií a členení manipulatívnych praktík *dark patterns*. Tieto možno rozlišovať podľa toho, či zasahujú do súkromie, zameriavajú sa na jeho správanie, vychádzajú z konkrétnej manipulatívnej praktiky obchodníka, a ďalšie delenia.³³

V súčasnosti nemožno hovoriť o uzatvorenom výpočte manipulatívnych praktík *dark patterns*. Globalizácia a rýchlo meniace sa digitálne prostredie prináša stále nové a nové praktiky, ktoré využívajú obchodníci vo svoj prospech. Už na základe horeuvedených kategórií je možné vidieť, že ide pomerne rozsiahle kategórie rozličných foriem, ktoré obchodníci využívajú vo svoj prospech.

Dark patterns ako nekalé obchodné praktiky?

V tejto súvislosti vzniká otázka do akej miery slovenský právny poriadok pripúšťa manipulatívne praktiky označované ako *dark patterns* v rámci konania obchodníka v spotrebiteľských vzťahoch. Základom ochrany samotného spotrebiteľa je zákon č. 108/2024 Z. z. o ochrane spotrebiteľa (*ďalej len „zákon o ochrane spotrebiteľa“*). Ten dopĺňa ako *lex specialis* zákon č. 40/1964 Zb. Občiansky zákonník ako *lex generalis* (*ďalej len Občiansky zákonník*). Zákon o ochrane spotrebiteľa okrem práv strán spotrebiteľského vzťahu explicitne zakotvuje povinnosti obchodníka voči spotrebiteľovi. Obchodník nielen že voči spotrebiteľovi nemôže používať nekalé obchodné praktiky. Tento zákaz explicitne upravuje § 4 ods. 2 písm. a) až písm. b) daného zákona. Nedodržanie uvedeného ustanovenia zákona následne vedie k vzniku zodpovednosti na strane obchodníka.

Zákon označuje za nekalú obchodnú praktiku podľa § 9 ods. 1 takú praktiku, ktorá je v rozpore s požiadavkami odbornej starostlivosti obchodníka a o vzťahu k produktu podstatne narušuje alebo môže podstatne narušiť ekonomické správanie priemerného spotrebiteľa, ku ktorému sa obchodná praktika dostane, alebo ktorému je adresovaná, alebo priemerného člena skupiny spotrebiteľov, ak je obchodná

³² LUGURI, Jamie - STRAHILEVITZ, Jacob Lior: Shining a Light on Dark Patterns. In: Journal of Legal Analysis. Oxford: Oxford University Press, Volume 13, Issue 1, (2021), s.53. Pozn. autorky: *Uvedený zdroj obsahujúci prehľad kategórií a foriem dark patterns je vytvorený autormi zdroja a zosumarizovaný na základe vedeckých výskumov ďalších autorov.*

³³ K prehľadu existencie rôznych kategorizácií a delení bližšie pozri: LUPIÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-25]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>, pp. 29 – 41.

praktika orientovaná na určitú skupinu spotrebiteľov.³⁴ Ide o dve kumulatívne podmienky, ktoré musia byť naplnené na to, aby bolo možné uskutočnenú praktiku zadefinovať v zmysle zákona za nekalú. Podstatným narušením ekonomického správania³⁵ je správanie, ktoré využíva obchodnú praktiku na značné obmedzenie schopnosti spotrebiteľa urobiť informované rozhodnutie v dôsledku ktorého spotrebiteľ učiní také rozhodnutie o obchodnej transakcii, ktoré by inak bez jej použitia neurobil. V praxi tak môže ísť praktiku namierenú voči jednotlivcovi alebo skupine spotrebiteľov. Vo všeobecnosti je spotrebiteľom fyzická osoba, ktorá nekoná v rámci svojej podnikateľskej činnosti alebo povolania v súvislosti so spotrebiteľskou zmluvou alebo z nej vyplývajúcim záväzkom.³⁶ Priemerným spotrebiteľom sa rozumie fyzická osoba, ktorá je priemerne informovaná, pozorná a obozretná.³⁷ Ochrana je v danom prípade poskytovaná spotrebiteľom, ktorí vyvinuli náležitú opatrnosť a dostatočnú starostlivosť na predchádzanie ujme na svojich subjektívnych právach.³⁸ Ide tak o spotrebiteľa, ktorý predstavuje podmnožinu skupiny s určitými špecifickými vlastnosťami. Medzník v ochrane tak predstavuje rozumná miera starostlivosti, pozornosti a opatrnosti, kde uvedené vlastnosti daný subjekt cieľovej skupiny od zraniteľnejších, dôverčivých či impulzívnych spotrebiteľov, ktorí sú menej pozorní, neorientujú sa podľa všeobecných odporúčaní a nechávajú sa ľahko ovplyvniť reklamnými tvrdeniami bez potrebnej kritickej miery posúdenia.³⁹ Dané podmienky generálnej klauzuly uvedenej v § 9 zákona sú jednoznačne naplnené pri manipulatívnej praktike *dark patterns* nazývanej vizuálna interferencia so spotrebiteľom. Túto praktiku možno chápať ako synonymum pojmu „*nekalá obchodná praktika*“.⁴⁰ Jej podstatou je používanie takých vizuálnych prvkov, jazyka alebo emócií, ktoré nasmerujú spotrebiteľa k alebo od konkrétnej voľby.⁴¹ Už len samotné jej využitie smeruje k naplneniu základnej definície manipulatívnych praktík *dark patterns*. Ako bolo už v predošlej kapitole uvedené ich podstatou je zabezpečiť, aby spotrebiteľ vykonal taký úkon, ktorý smeruje k prospechu na strane obchodníka

³⁴ Článok 5 Smernice o nekalých obchodných praktikách.

³⁵ § 9 ods. 3 Zákona o ochrane spotrebiteľa.

³⁶ § 52 ods. 4 Občianskeho zákonníka.

³⁷ Rozsudok Súdneho dvora zo dňa 16. júla 1998 vo veci Gut Springenheide GmbH a Rudolf Tusky proti Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung, sp. zn. C 210/96.

³⁸ DUFKOVÁ, Anna: Ochrana slabší strany ve světle nekalé soutěže a nekalých obchodních praktik. In: Obchodněprávní revue. Praha: C. H. Beck, číslo, 1, (2021), s. 32.

³⁹ Tamtiež.

⁴⁰ ISOLA, Cecilia - ESPOSITO, Fabrizio: A systematic literature review on dark patterns for the legal community: definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. In: Computer Law & Security Review. United Kingdom: Elsevier, volume 58, number 106169, (2025). [online]. 2025. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S2212473X25000422?via%3Dihub>, p. 13.

⁴¹ Tamtiež, p. 11.

a priamo alebo nepriamo podstatne ovplyvnil hospodárske správanie spotrebiteľa, ktoré by bez uvedenej manipulatívnej praktiky neurobil. Vizuálna interferencia nielen, že bráni spotrebiteľovi k informovanému rozhodnutiu, ale vedie k rozhodnutiam, ktoré by spotrebiteľ za bežných okolností a bez prítomnosti *dark patterns* nevykonával. Naplňa tak znaky porušenia odbornej starostlivosti na strane obchodníka. Za odbornú starostlivosť je potrebné považovať špeciálnu schopnosť a starostlivosť obchodníka, ktorú je možno rozumne od neho očakávať pri jeho konaní voči spotrebiteľom, zodpovedajúcu čestnej obchodnej praxi a / alebo všeobecnej zásade dobrej viery uplatňujúcej sa v oblasti obchodníckej činnosti.⁴² Pri využití takýchto praktík nie je možné naplniť požiadavku odbornej starostlivosti obchodníka. Predpokladá čestnú obchodnú prax, ktorú obchodník poruší svojim úmyslom manipulovať osobu spotrebiteľa.

Zákon o ochrane spotrebiteľa v § 9 ods. 5 ustanovuje za nekalú obchodnú praktiku také konanie, ktoré sa považuje za klamlivé.⁴³ Okrem klamlivého konania považuje za nekalú obchodnú praktiku aj klamlivé opomenutie konania⁴⁴ a agresívne obchodné praktiky.⁴⁵ Za klamlivé konanie pri využití praktík možno označiť praktiky *dark patterns*, ako sú: falošné zľavy, falošná hierarchia, falošné recenzie, správy o vysokom dopyte, zneužitie súkromia, virtuálne meny, správy o nízkom stave zásob alebo nedostatku tovaru, sociálne pyramídy, zavádzajúce otázky, a podobne.⁴⁶ Klamlivým konaním podľa § 10 ods. 1 zákona o ochrane spotrebiteľa je obchodná praktika, ktorá zapríčiňuje alebo môže zapríčiniť, že priemerný spotrebiteľ urobí rozhodnutie o obchodnej transakcii, ktoré by inak neurobil, pretože obsahuje nesprávne informácie a je preto nepravdivá, alebo akýmkoľvek spôsobom uvádza do omylu alebo môže viesť do omylu priemerného spotrebiteľa, a to aj ak je táto informácia vecne správna vo vzťahu k určitej skutočnosti. Táto skutočnosť sa podľa uvedeného ustanovenia môže týkať:

- a) *existencie produktu alebo povahy produktu;*
- b) *hlavných vlastností produktu, ako sú jeho dostupnosť, výhody, riziká, vyhotovenie, zloženie, príslušenstvo, pomoc a služby po predaji produktu, zodpovednosť za vady, výrobný postup, dátum výroby alebo dodania, spôsob*

⁴² Článok 2 písm. h) Smernice o nekalých obchodných praktikách.

⁴³ Článok 6 Smernice o nekalých obchodných praktikách.

⁴⁴ Tamtiež, článok 7.

⁴⁵ Tamtiež, článok 8.

⁴⁶ ISOLA, Cecilia - ESPOSITO, Fabrizio: A systematic literature review on dark patterns for the legal community: definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. In: Computer Law & Security Review. United Kingdom: Elsevier, volume 58, number 106169, (2025). [online]. 2025. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S2212473X25000422?via%3Dihub>, p. 12.

- dodania, účel použitia, možnosti využitia, množstvo, špecifikácia, zemepisný pôvod alebo obchodný pôvod, výsledky použitia, či výsledky skúšok alebo kontrol;*
- c) rozsahu záväzkov obchodníka, motívov obchodnej praktiky, charakteru procesu predaja, akémukoľvek vyhláseníu alebo symbolu týkajúcemu sa priameho alebo nepriameho sponzorstva alebo schválenia obchodníka alebo produktu;*
 - d) ceny, spôsobu výpočtu ceny alebo k existencii osobitnej cenovej výhody;*
 - e) potreby údržby, náhradného dielu, výmeny alebo opravy;*
 - f) osoby, vlastností a práv obchodníka alebo jeho splnomocnenca vrátane totožnosti, majetku, kvalifikácie, postavenia, uznania, členstva v organizáciách, právnych vzťahov, vlastníctva práv vyplývajúcich z obchodného alebo duševného vlastníctva, ocenení alebo vyznamenaní;*
 - g) práv spotrebiteľa vrátane práv zo zodpovednosti za vady produktu;*
 - h) rizík, ktorým môže byť spotrebiteľ vystavený.*

Za klamlivé konanie sa tak považuje každé konanie obchodníka, ktorým obchodník uvádza spotrebiteľovi nepravdivé alebo nesprávne informácie týkajúce sa vyššie uvedených skutočností.

Klamlivým konaním je podľa odseku 2 uvedeného ustanovenia aj obchodná praktika, ktorá s prihliadnutím na všetky jej znaky a okolnosti zapríčiňuje alebo môže zapríčiniť, že priemerný spotrebiteľ urobí rozhodnutie o obchodnej transakcii, ktoré by inak neurobil, pričom podmienkou je, aby zahŕňala aj:

- a) marketing produktu vrátane porovnávacej reklamy, ktorý spôsobuje nebezpečenstvo zámeny s iným produktom, ochrannou známkou, obchodným menom alebo iným rozlišujúcim znakom účastníka hospodárskej súťaže;*
- b) neplnenie záväzkov obsiahnutých v kódexe správania, k dodržiavaniu ktorých sa obchodník zaviazal, ak nejde len o snahu zaviazat' sa, ale o jednoznačný záväzok, ktorý môže byť preverený, a obchodník v obchodnej praktike uvedie, že je viazaný kódexom správania;*
- c) marketing tovaru spôsobom, ktorý prezentuje tovar ako identický s tovarom uvádzaným na trh v iných členských štátoch Európskej únie alebo v štátoch, ktoré sú zmluvnou stranou Dohody o Európskom hospodárskom priestore (ďalej len „členský štát“), hoci tovar má podstatne odlišné zloženie alebo vlastnosti; obchodná praktika sa nepovažuje za klamlivú, ak odlišné zloženie a vlastnosti tovaru sú odôvodnené legitímnymi alebo objektívnymi faktormi.*

Skutková podstata klamlivého konania obchodníka voči spotrebiteľovi zahŕňa aj akékoľvek marketingové praktiky, ktoré nielen narúšajú jeho rozhodovaciu schopnosť, ale aj zásadným spôsobom narúšajú jeho kognitívne vnímanie. Klamlivé konanie je preto koncipované široko s účelom zabezpečiť, aby obchodník, ktorý môže byť postihovaný vzniknutou zodpovednosťou, prispôbil interakciu so spotrebiteľom, vrátane marketingových stratégií, požiadavkám zákona o ochrane spotrebiteľa. Obchodníci tak pri svojich praktikách, ako sú reklama, stratégie či

marketing, musia dbať na zákonne prípustnú hranicu a neohrozovať tak slabšiu pozíciu spotrebiteľa. Dôsledkom je práve vznik zodpovednosti a sankcie pre obchodníka.

Klamlivým opomenutím konania je zo strany obchodníka využitie dark patterns praktík, a to konkrétne praktiky skrytých informácií a praktiky nazývanej prechodná mena.⁴⁷ Podstatou konania je podľa § 11 zákona o ochrane spotrebiteľa je opomenutie podstatnej informácie, ktorú priemerný spotrebiteľ potrebuje k tomu, aby urobil zásadné rozhodnutie o obchodnej transakcii. Súčasťou naplnenia skutkovej podstaty je aj skrývanie informácie alebo nejasné, nezrozumiteľné poskytnutie informácie obchodníkom. Absentuje tak informovanosť spotrebiteľa o informáciách, ktoré sú kľúčové k vykonaniu obchodnej transakcie.

Za agresívnu obchodnú praktiku možno považovať otravovanie alebo spam zo strany obchodníkov.⁴⁸ Agresívnou je *„obchodná praktika je obchodná praktika, ktorá obťažovaním, nátlakom vrátane použitia fyzickej sily alebo neprimeraným vplyvom s prihliadnutím na všetky jej znaky a okolnosti podstatne zhoršuje alebo je spôsobilá významne zhoršiť slobodu voľby alebo správanie priemerného spotrebiteľa vo vzťahu k produktu, a tým zapríčiňuje alebo môže zapríčiniť, že spotrebiteľ urobí rozhodnutie o obchodnej transakcii, ktoré by inak neurobil.“*⁴⁹

Právna kvalifikácia dark patterns si vyžaduje nielen teoretické, ale aj praktické posúdenie na základe konkrétnych prípadov. V súčasnosti však neexistuje judikatúra slovenských súdov, ktorá by teoretické chápanie *dark patterns* posudzovala.

Marketingové stratégie obchodníkov a ich úskalia v kontexte nekalých obchodných praktík pre spotrebiteľa

Praktiky obchodníkov, vrátane používania manipulatívnych *dark patterns* často v praxi fungujú v nejasnej oblasti medzi legitímnymi pokusmi o presvedčanie a nelegitímnymi manipulatívnymi technikami obchodníka.⁵⁰ Zákon o ochrane spotrebiteľa síce obsahuje skutkové podstaty nekalých obchodných praktík, no

⁴⁷ Bližšie pozri: ISOLA, Cecilia - ESPOSITO, Fabrizio: A systematic literature review on dark patterns for the legal community: definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. In: Computer Law & Security Review. United Kingdom: Elsevier, volume 58, number 106169, (2025). [online]. 2025. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S2212473X25000422?via%3Dihub>, p. 12.

⁴⁸ Bližšie pozri: Tamtiež.

⁴⁹ § 12 ods. 1 Zákona o ochrane spotrebiteľa.

⁵⁰ LUPÍÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-10]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>, p. 6.

priamo *dark patterns* vo svojom znení nedefinuje. Je pritom preukázané, že používatelia vystavení *dark patterns* boli viac ako dvakrát náchylnejší zaregistrovať sa na pochybné služby, pričom agresívne *dark patterns* zvýšili túto pravdepodobnosť takmer štvornásobne.⁵¹ Vo všeobecnosti majú ale spotrebitelia tendenciu robiť nekonzistentné rozhodnutia aj v priestore, vrátane digitálneho, kde sa samotné manipulatívne praktiky *dark patterns* nevyskytujú, avšak ak toto prostredie obsahuje v určitej forme tieto praktiky sa pravdepodobnosť ich nekonzistentného správania zvýšila, a to výrazne.⁵² Je preto preukázané, že digitálne prostredie, ktoré obsahuje manipulatívne praktiky *dark patterns* ohrozuje spotrebiteľov a ich rozhodovanie. Zadefinovať konkrétnu manipulatívnu praktiku *dark patterns* možno až v prípade, ak táto praktika je zaužívaná a spĺňa definičné znaky uvedené vyššie. Katalóg manipulatívnych praktík je však aktuálne vzhľadom na vyvíjajúce sa digitálne prostredie neuzatvorený. V súčasnosti zároveň spotrebiteľom chýba zvýšené povedomie o používaní nekalých praktík obchodníkmi a až akonáhle tieto praktiky identifikujú spotrebitelia ich vnímajú negatívne.⁵³ Bežné ukazovatele zraniteľnosti spotrebiteľov, ako sú príjem, vzdelanie alebo vek neboli preukázateľným dôkazom o náchylnosti týchto osôb podľahnúť manipulatívnym technikám *dark patterns*.⁵⁴ Náchylnosť osôb podľahnúť manipulatívnym technikám preto nemožno v súčasnosti pripisovať sociálnym aspektom spotrebiteľa. V prípade prevzatia právnej definície *dark patterns* vo vyššie uvedenom nariadení do právneho poriadku je potrebné vzťahovať definíciu na všetkých priemerných spotrebiteľov.

Záver

Manipulatívne praktiky označované ako *dark patterns* predstavujú len jednu z kategórií nekalého konania obchodníka voči spotrebiteľovi. Ich využívanie vo vzťahoch so spotrebiteľom je možné v mnohých prípadoch subsumovať pod znaky nekalej obchodnej praktiky podľa zákona o ochrane spotrebiteľa. Vzhľadom na absentujúcu definíciu pojmu „*dark patterns*“ je však najprv potrebné vymedziť spoločné znaky takéhoto konania obchodníka. Len na základe týchto znakov je

⁵¹ LUGURI, Jamie - STRAHILEVITZ, Jacob Lior: Shining a Light on Dark Patterns. In: Journal of Legal Analysis. Oxford: Oxford University Press, Volume 13, Issue 1, (2021), p. 43.

⁵² LUPIÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-10]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>, p. 119.

⁵³ Tamtiež, p. 120.

⁵⁴ Bližšie pozri: ZAC, Amit – HUANG, Yu Chun – VON MOLTKE, Amédée – DECKER, Christoph – EZRACHI, Ariel: Dark patterns and consumer vulnerability. In: Behavioural Public Policy. Cambridge: Cambridge University Press, (2025), pp. 1 – 25.

možné následne identifikovať konanie obchodníka a subsumovať ho pod skutkové podstaty nekalých obchodných praktík podľa § 9 až § 12 daného zákona. Nemožno pritom predpokladať, že každá kategória alebo forma *dark patterns* automaticky napĺňa znaky nekalej obchodnej praktiky, pretože slovenský právny poriadok ponecháva hranicu medzi spomínanými praktikami a prípustným marketingom obchodníka relatívne neurčitú. Tento priestor umožňuje priestor ďalší výklad zo strany súdnej praxe alebo prípadnú legislatívnu úpravu novelou zákona o ochrane spotrebiteľa. Demonštratívny výpočet súčasne ponecháva priestor na širšie chápanie manipulatívneho konania obchodníka, no zároveň poskytuje priestor na rozdielne ponímanie konkrétnej manipulatívnej praktiky, čím sa výrazne narúša ochrana spotrebiteľa. Spresneniu právnej úpravy by napomohlo doplnenie definície *dark patterns*, prípadne vymedzenie znakov takéhoto konania zo strany obchodníka v právnom poriadku. Definícia v Nariadení Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES, ktoré definuje *dark patterns* ako praktiky „ktoré zámerne alebo fakticky narúšajú alebo oslabujú schopnosť príjemcov služby prijímať samostatné a informované rozhodnutia“... a ... „môžu byť využívané na presvedčovanie príjemcov služby na nechcené správanie alebo na nežiaduce rozhodnutia, ktoré majú pre nich negatívne dôsledky“; by napomohla k vytvoreniu pevného právneho základu aj v otázke spotrebiteľských vzťahov. Legislatívne opatrenia tohto typu by mohli spotrebiteľom priniesť vyššiu ochranu.

Zoznam použitej literatúry

1. DI GERONIMO, Linda - BRAZ, Larissa - FREGNAN, Enrico - PALOMBA, Fabio - BACCHELLI, Alberto: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In: Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems. New York: Association for Computing Machinery, (2020), pp. 1 – 14. ISBN 978-1-4503-6819-3. <https://doi.org/10.1145/3313831.3376600>.
2. DUFKOVÁ, Anna: Ochrana slabší strany ve světle nekalé soutěže a nekalých obchodních praktik. In: Obchodněprávní revue. Praha: C. H. Beck, číslo, 1, (2021), s. 32. ISSN : 1803-6554.
3. EUROPEAN PARLIAMENT. Regulating dark patterns in the EU: Towards digital fairness. [online]. 2025. [cit. 2025-09-28]. Dostupné na: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_AT_A%282025%29767191_EN.pdf.
4. EURÓPSKA SPOTREBITEĽSKÁ ORGANIZÁCIA. Všeobecné spotrebiteľské právo – Teoretický východiskový dokument. 1. verzia. [online]. Luxemburg: BEUC. [online]. 2021. 23 s. Dostupné na:

https://www.beuc.eu/sites/default/files/publications/consumerpro_consumer_rights_tbd_sk.pdf.

5. ESPOSITO, Fabrizio - FERREIRA, Cathoud Maciel Thaís: Addictive Design as an Unfair Commercial Practice: The Case of Hyper -Engaging Dark Patterns. In: European Journal of Risk Regulation. Cambridge: Cambridge University Press, volume 15, special issue 4, (2024), pp. 999 – 1016. ISSN 2190-8249. <https://doi.org/10.1017/err.2024.8>.
6. GUNAWAN, Johanna. et al.: A Comparative Study of Dark Patterns Across Mobile and Web Modalities In: Proceedings of the 22nd ACM Internet Measurement Conference. New York: Association for Computing Machinery, Article 377, (2021), pp. 336 – 351. ISBN 978-1-4503-9129-0. <https://doi.org/10.1145/3479521>
7. HUNG, Alison: Keeping Consumers in the Dark: Addressing “Nagging” Concerns and Injury. In: Columbia Law Review. New York: Columbia Law Review Association, volume 121, number 8, (2021), pp. 2483 – 2520. ISSN 0010-1958. <https://doi.org/10.1145/3479521>
8. ISOLA, Cecilia - ESPOSITO, Fabrizio: A systematic literature review on dark patterns for the legal community: definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. In: Computer Law & Security Review. United Kingdom: Elsevier, volume 58, number 106169, (2025). [online]. 2025. [cit. 2025-09-20]. pp. 1 – 16. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S2212473X25000422?via%3Dihub>. ISSN 2212-4748. <https://doi.org/10.1016/j.clsr.2025.106169>.
9. Jazykovedný ústav Ľ. Štúra SAV. Praktika. Historický slovník slovenského jazyka. [online]. 2008. [cit. 2025-09-25]. Dostupné na: <https://www.juls.savba.sk/hssj.html>.
10. Jazykovedný ústav Ľ. Štúra SAV. Technika. Slovník cudzích slov [online]. 2005. [cit. 2025-09-25]. Dostupné na: https://www.juls.savba.sk/slovník_cudzich_slov_2005.html.
11. LUGURI, Jamie - STRAHILEVITZ, Jacob Lior: *Shining a Light on Dark Patterns*. In: Journal of Legal Analysis. Oxford: Oxford University Press, Volume 13, Issue 1, (2021), pp. 43 - 109. ISSN 2161-721X. <https://doi.org/10.1093/jla/laaa006>.
12. LUPIÁÑEZ-VILLANUEVA, Francisco et al.: Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation: final report. Luxembourg: Publications Office of the European Union. [online]. 2022. [cit. 2025-09-10]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en#>. 302 p. ISBN 978-92-76-52316-1. <https://data.europa.eu/doi/10.2838/859030>.
13. MATHUR, Arunesh. et al.: Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. In: Proceedings of the ACM on Human-Computer

Interaction. New York: Association for Computing Machinery, Volume 3, Article 81, (2019), pp. 1 – 32. ISSN: 2573-0142.

14. MONEYTHOR. The Default Effect: Behavioural Science in Banking. [online]. 2022. [cit. 2025-09-15]. Dostupné na: <https://www.moneythor.com/analysis-opinions/behavioural-science/the-default-effect-behavioural-science-in-banking/>.
15. OECD. Dark commercial patterns. OECD Digital Economy Papers, number 336. Paríž: OECD. [Online]. 2022. [cit. 2025-09-08]. 96 s. Dostupné na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf.
16. PSYCHOINFO.SK. Framing efekt (efekt rámcovania). [online]. 2025. [cit. 2025-09-15]. Dostupné na: <https://psychoinfo.sk/psychologicky-slovník/framing-efekt-efekt-ramcovania/>.
17. Rozsudok Súdneho dvora zo dňa 16. júla 1998 vo veci Gut Springenheide GmbH a Rudolf Tusky proti Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung, sp. zn. C 210/96.
18. SIN, Ray - HARRIS, Ted - NILSSON, Simon - BECK, Talia: Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying? In: Behavioural Public Policy, Cambridge: Cambridge University Press, volume 9, (2025), pp. s. 61 – 87. ISSN 2398-0648. <https://doi.org/10.1017/bpp.2022.11>.
19. ZAC, Amit – HUANG, Yu Chun – VON MOLTKE, Amédée – DECKER, Christoph – EZRACHI, Ariel: Dark patterns and consumer vulnerability. In: Behavioural Public Policy. Cambridge: Cambridge University Press, (2025), pp. 1 – 25. ISSN 2398-0648. <https://doi.org/10.1017/bpp.2024.49->.
20. ZLOCHA, Ľubomír - STRÉMY, Jana: Nekalá súťaž. Generálna klauzula, menej tradičné prípady a zahraničné právne úpravy. Bratislava: C. H. Beck, (2023), 357 s. ISBN: 978-80-8232-043-8.

Kontaktné údaje

Mgr. Regina Šťastová, PhD.

regina.stastova@savba.sk

ORCID: 0009-0005-9569-8759

Ústav štátu a práva, Slovenská akadémia vied, v. v. i.

ZAKLADANIE SPOLOČNOSTÍ V EURÓPSKEJ ÚNII: AKTUÁLNY STAV, LIMITY HARMONIZÁCIE A PERSPEKTÍVA 28. REŽIMU¹

COMPANY FORMATION IN THE EUROPEAN UNION: CURRENT FRAMEWORK, LIMITS OF HARMONISATION AND THE PERSPECTIVE OF THE 28TH REGIME

Barbora Grambličková²

Abstrakt: Jednoduché, rýchle a cezhranične dostupné zakladanie obchodných spoločností predstavuje kľúčový predpoklad fungovania vnútorného trhu a konkurencieschopnosti Európskej únie. Tento príspevok analyzuje aktuálny stav harmonizácie v oblasti zakladania spoločností, a to najmä v kontexte opatrení zavedených smernicou (EÚ) 2019/1151 a následne rozšírených smernicou (EÚ) 2025/25. Príspevok zároveň reflektuje výstupy verejnej konzultácie k iniciatíve „28. režim – právny rámec EÚ pre podniky“, ktoré odhaľujú zásadné problémy respondentov prekážajúce efektívnemu zakladaniu spoločností v Európskej únii. Na tomto základe príspevok hodnotí potenciál 28. režimu ako nového nadnárodného modelu, ktorý by mohol prekonať súčasné harmonizačné limity a ponúknuť jednotný proces (nielen) zakladania spoločností naprieč členskými štátmi.

Kľúčové slová: cezhraničné zakladanie spoločností a pobočiek, digitalizácia, smernica (EÚ) 2019/1151, smernica (EÚ) 2025/25, 28. režim

Abstract: Simple, fast, and cross-border accessible company formation constitutes a key prerequisite for the functioning of the internal market and the competitiveness of the European Union. This article examines the current state of harmonisation in the area of company formation, particularly in the context of the measures introduced by Directive (EU) 2019/1151 and subsequently expanded by Directive (EU) 2025/25. It also reflects the findings of the public consultation on the initiative “28th regime – EU corporate legal framework”, which reveal significant obstacles hindering effective company formation

¹ Tento príspevok je výstupom riešenia projektu VEGA: 1/0732/25 „Výzvy a riziká správy, riadenia a kontroly obchodných spoločností s majetkovou účasťou mesta (MOE/mestský podnik) v kontexte cieľov a naplňania mestských politík“.

² Právnická fakulta Univerzity Komenského v Bratislave.

within the European Union. Building on these insights, the article assesses the potential of the 28th regime as a new supranational model capable of overcoming the current limits of harmonisation and offering a unified process for (not only) company formation across the Member States.

Key words: Cross-border formation of companies and branches, Digitalization, Directive (EU) 2019/1151, Directive (EU) 2025/25, 28th regime

Úvod – aktuálne výzvy Európskej únie v zakladaní spoločností v časoch inovačnej krízy

Dňa 8. júla 2025 vyhlásila Európska komisia verejnú konzultáciu k iniciatíve: 28. režim – právny rámec EÚ pre podniky (ďalej len „28. režim“) s cieľom zozbierania podnetov k tejto iniciatíve.³ 28. režim reaguje na správu o konkurencieschopnosti Európskej únie (Kompas konkurencieschopnosti⁴), v ktorej je konštatované, že Európska únia čelí dlhodobým bariéram a štrukturálnym nedostatkom, ktoré brzdia jej rast, keďže za posledné dve desaťročia nedokázala držať krok s hlavnými ekonomikami sveta (USA, Čína) a zaostala najmä v oblasti produktivity a inovácií. Situáciu európskych spoločností zhoršuje aj vysoká regulačná záťaž.⁵ Zakladanie a rozširovanie spoločností v Európe je v súčasnosti brzdené fragmentáciou právnych poriadkov, obmedzeným prístupom k rizikovému kapitálu a nedostatočnou podporou inovácií.⁶ Zvýšenie konkurencieschopnosti vo všetkých sektoroch je podľa tohto dokumentu možné najmä prostredníctvom zjednodušenia regulačného prostredia, znižovania administratívnej záťaže, uprednostňovania rýchlosti a flexibility zakladania ako aj fungovania spoločností.⁷

³ 28. režim – právny rámec EÚ pre podniky, dostupné na: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU_sk (cit. 27.09.2025), s. 3.

⁴ Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A Competitiveness Compass for the EU, Brussels, 29.1.2025 COM(2025) 30 final (ďalej len „**Kompas konkurencieschopnosti**“). Kompas konkurencieschopnosti nadviazal a vychádza z Letta Reportu (LETTA, Enrico: Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens, April 2024, s. 1-146) a Draghi Reportu (The future of European competitiveness, Luxembourg: Publications Office of the European Union, 2025, s. 1-70, ISBN 978-92-68-22715-2 doi:10.2872/9356120 ES-01-24-000-EN-N).

⁵ Kompas konkurencieschopnosti, s. 1.

⁶ Kompas konkurencieschopnosti, s. 4.

⁷ Kompas konkurencieschopnosti, s. 3.

Následne sa sprievodný dokument k verejnej konzultácii 28. režimu odvoláva aj na dokument: Stratégia pre startupy a scaleupy⁸, v ktorom Európska únia upozorňuje na potrebu naštartovania inovácií a zakladania startupov ako aj podpory scaleupov, keďže až 30% európskych „jednorožcov“⁹ sa premiestňuje do USA a len 8% globálnych scaleupov je alokovaných v Európskej únii.¹⁰ Predmetné je spôsobené nedostatkom rizikového kapitálu v období, keď startupy ešte nemajú komerčný produkt a neskôr v čase škálovania spoločnosti (scaling).¹¹ Európska únia v dokumente uvádza, že je potrebné prijať opatrenia, ktoré by mali odstrániť bariéry pri zakladaní a raste inovatívnych spoločností, a predstavuje 28. režim ako možnosť voliteľného európskeho právneho rámca, paralelného s národnou právnou úpravou. Tento rámec by mal poskytnúť štandardizované a zjednodušené pravidlá, nižšie náklady pre rýchlejšie založenie spoločností a menšiu fragmentáciu národných poriadkov.¹²

28. režim má zároveň reagovať na potreby podnikateľov a poskytnúť spoločnostiam, najmä inovatívnym, jednotný súbor pravidiel, ktorý im uľahčí fungovanie, investovanie a pôsobenie na jednotnom trhu, pričom jeho hlavným pilierom by mal byť nový právny rámec pokrývajúci široké spektrum kľúčových otázok, založený na online postupoch a digitálnych nástrojoch v rámci práva obchodných spoločností Európskej únie. Tento právny rámec by mal byť podporený aj opatreniami v iných oblastiach (daňová, insolvenčná a pracovnoprávna regulácia), ktoré pomôžu inovatívnym spoločnostiam rozvíjať sa a rásť v Európskej únii.¹³

Cieľom tohto príspevku je analyzovať spätnú väzbu respondentov získanú v rámci verejnej konzultácie k 28. režimu, pričom mapovanie odpovedí bolo zámerne filtrované na otázky súvisiace so zakladaním obchodných spoločností. Tento prístup bol zvolený vzhľadom na to, že empirická skúsenosť respondentov so zakladaním

⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The EU Startup and Scaleup Strategy, Choose Europe to start and scale, Brussels, 28.5.2025 COM(2025) 270 final (ďalej len „**Stratégia pre startupy a scaleupy**“).

⁹ Valuácia spoločnosti nad 1 miliardu EUR.

¹⁰ Stratégia pre startupy a scaleupy, s. 2.

¹¹ Stratégia pre startupy a scaleupy, s. 2.

¹² Stratégia pre startupy a scaleupy, s. 2 a 5. Potrebu zavedenia 28. režimu a zníženia administratívnych, a regulačných prekážok zakladania spoločností obsahuje aj dokument: Stratégia jednotného trhu. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The Single Market: our European home market in an uncertain world, A Strategy for making the Single Market simple, seamless and strong, Brussels, 21.5.2025, COM(2025) 500 final (ďalej len „**Stratégia jednotného trhu**“), s. 8.

¹³ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU_sk (cit. 27.09.2025).

spoločností predstavuje dôležitý indikátor efektívnosti legislatívno-regulačného rámca a zároveň je jedným z kľúčových predpokladov pre podporu a rozvoj inovačného potenciálu Európskej únie.

Príspevok zároveň rámcovo hodnotí proces zakladania spoločností v kontexte doteraz prijatých harmonizačných opatrení EÚ, najmä prostredníctvom príslušných smerníc (Smernica 2019/1151¹⁴ a Smernica 2025/25¹⁶), a následne predstavuje koncepciu tzv. 28. režimu, vrátane plánovaných iniciatív Európskej únie smerujúcich k jeho novej implementácii.

Súbežne sa príspevok zameriava aj na analyticko-syntetické spracovanie dokumentu „Simplification of Registration of Companies in the 28th Regime“ od Prof. Dr. Floriana Möseleina, LL.M., ktorý bol vypracovaný na základe požiadavky Výboru pre právne veci (JURI) Európskeho parlamentu, a ktorý predstavuje významné odborné východisko pre diskusiu o zjednodušení zakladania spoločností v Európskej únii.

Ďalším cieľom príspevku je vyhodnotiť, do akej miery môžu byť problematické aspekty identifikované respondentmi vo verejnej konzultácii eliminované prijatím Smernice 2025/25 a jej transponovaním do právnych poriadkov členských štátov, prípadne prostredníctvom návrhov súvisiacich s 28. režimom ako aj ďalších odborných materiálov prezentovaných Európskou uniou v tejto oblasti.

¹⁴ Smernica Európskeho parlamentu a Rady (EÚ) 2019/1151 z 20. júna 2019, ktorou sa mení smernica (EÚ) 2017/1132, pokiaľ ide o používanie digitálnych nástrojov a postupov v rámci práva obchodných spoločností (ďalej len „**Smernica 2019/1151**“).

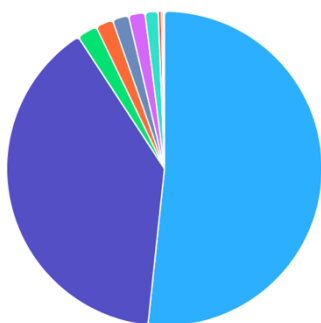
¹⁵ Autorka zároveň uvádza, že článok sa nevenuje transpozičnému procesu Smernice 2019/1151 do slovenského právneho poriadku, ani spracovávanú tému neanalyzuje s ohľadom na prebiehajúce legislatívne zmeny právnej úpravy obchodného registra v Slovenskej republike. Pre aspekty transpozície Smernice 2019/1151 ako aj jej dopadov na slovenský právny poriadok, ako aj iných aspektov digitalizácie slovenského korporačného práva pozri bližšie: MRÁZOVÁ, Žofia – CUKEROVÁ, Dominika: How the Digitalisation Has Changed the Slovak Company Law: Implementation of the Directive 2019/1151 (Digitalisation Directive) and What Next? In: EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC), č. 7 (2023), s. 334-360; SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. Bratislava: Nakladateľství C.H.Beck-SK, 1. vydanie, 2024. S. 1-144. ISBN: 978-80-8232-050-6; ŠULEKOVÁ, Žofia: Elektronizácia v korporačnom práve. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.): Právo, obchod, ekonomika VI. Košice: Univerzita P. J. Šafárika v Košiciach, 2016, s. 551-559; CSACH, Kristián: Digital corporate governance in Slovakia. In: Právny obzor, special issue 105 (2022), s. 3-13.

¹⁶ Smernica Európskeho parlamentu a Rady (EÚ) 2025/25 z 19. decembra 2024, ktorou sa menia smernice 2009/102/ES a (EÚ) 2017/1132, pokiaľ ide o ďalšie rozšírenie a zdokonalenie využívania digitálnych nástrojov a postupov v oblasti práva obchodných spoločností (ďalej len „**Smernica 2025/25**“).

28. režim – spätná väzba a návrhy subjektov k zakladaniu spoločností vo verejnej konzultácii

V rámci verejnej konzultácie k 28. režimu sa vyjadrilo približne 700 subjektov z Európskej únie¹⁷, z toho najväčší počet odpovedí bolo z Nemecka (cca 261 odpovedí), nasledovalo Holandsko (cca 107 odpovedí) a Taliansko (cca 90 odpovedí).¹⁸ S ohľadom na kategorizáciu subjektov, ktoré sa zapojili do konzultácie je možné konštatovať, že sa v najväčšej miere zapojili občania Európskej únie¹⁹ (cca 51,67% respondentov) a následne spoločnosti (cca 39,12% respondentov).

Podľa kategórie respondenta



Zdroj: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/public-consultation_skv

Po vyfiltrovaní slov ako „creation of a company“, „establishment of a company“ alebo „formation of a company“, sa približne 80 odpovedí venovalo aspoň čiastočne aspektu zakladania spoločností, pričom je dôležité podotknúť, že väčšina týchto odpovedí bola z Nemecka. Z týchto príspevkov bola zrejmá veľká miera kritiky k procesu zakladania spoločností a respondenti boli v mnohých prípadoch aj pomerne expresívny, a popisovali tento proces aj nasledovne: „... proces zakladania

¹⁷ V čase, keď autorka odovzdávala príspevok ostávali do konca verejnej konzultácie približne 3 dni. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/public-consultation_sk (cit. 27.09.2025).

¹⁸ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/public-consultation_sk (cit. 27.09.2025).

¹⁹ V mnohých prípadoch išlo o zakladateľov spoločností.

*spoločnosti je pre motivovaného jednotlivca frustrujúci a ponížujúci... skutočnosť, že sme najprv museli notárovi zaplatiť a ten potom nahlas čítal zakladateľskú zmluvu, pôsobil ako scéna z groteskného filmu... zakladanie spoločnosti je veľmi nepríjemná skúsenosť, často chaotická a frustrujúca, pričom celý proces trpí nedostatkom jasnosti a koordinácie medzi rôznymi jurisdikciami...*²⁰

Spätnú väzbu respondentov v rámci verejnej konzultácie k 28. režimu s ohľadom na proces zakladania spoločností v rámci Európskej únie je možné zhrnúť po obsahovej stránke do nasledujúcich oblastí. Prvým aspektom je **byrokracia a neefektívnosť** – respondenti opisovali procesy zakladania spoločnosti ako zastarané a pomalé, v mnohých prípadoch namietali dĺžku založenia spoločnosti ako aj nízku digitalizáciu, a potrebu osobnej prítomnosti pred notárom v tomto procese. Po druhé, respondenti poukazovali na **vysoké náklady a ako negatívne namietali postavenie notárov v procese zakladania spoločností**. Kritizovaným aspektom bola najmä povinnosť účasti notárov v procese zakladania spoločností, ako uvádzame vyššie, táto kritika bola viazaná hlavne na Nemecko. V tejto súvislosti respondenti zdôrazňovali aj vysoké náklady na založenie spoločnosti, zbytočné úkony z pohľadu zakladateľov ako je čítanie zakladateľských dokumentov nahlas nezohľadňujúc jazykové limity zakladateľov v prípade cezhraničného zakladania spoločnosti. Respondenti poukazovali, že potreba prítomnosti notára pri zakladaní spoločnosti spôsobuje, že náklady na notára sú vyššie než administratívne náklady na samotné založenie spoločnosti. V drvivej väčšine bolo postavenie notára v tomto procese vnímané zakladateľmi ako zastarané a nepotrebné. Tretím aspektom, ktorý sa objavoval v odpovediach vo verejnej konzultácii bola **fragmentácia trhu a právnej úpravy v Európskej únii**, keďže respondenti poukazovali na veľké rozdiely medzi členskými štátmi pri zakladaní spoločností. Ďalším aspektom, spojeným s vyššie uvedenými bodmi, bola **konkurenčná nevýhoda Európskej únie**, keďže startupy radšej zakladajú spoločnosti v USA (Delaware) alebo sa vo fáze škálovateľnosti (scaleing) presúvajú do USA (flips) kvôli získaniu ďalšieho rizikového kapitálu pre rast. Zaujímavým aspektom adresovaným v rámci tejto verejnej konzultácie v spojitosti so zakladaním spoločností v Európskej únii bolo postavenie **bánk**, ktoré mnohokrát **vyžadujú osobnú prítomnosť pri zakladaní podnikateľského účtu** z dôvodu opatrení proti praniu špinavých peňazí a tým sa stávajú novými bariérami zakladania spoločností.²¹

²⁰ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/feedback_sk?p_id=19997 (cit. 27.09.2025).

²¹ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/feedback_sk?p_id=19997 (cit. 27.09.2025).

V rámci verejnej konzultácie respondenti neuvádzali len problematické aspekty v otázke zakladania spoločností, ale aj možné návrhy na zlepšenie tohto procesu v Európskej únii. Respondenti by uvítali **jednotnú európsku právnu formu spoločnosti**, ktorá by bola uznávaná vo všetkých štátoch Európskej únie. Zároveň by mal byť **proces zakladania spoločností plne digitálny a dostupný v angličtine**, a jeho trvanie by malo byť maximálne 2–5 dní. Ďalšie aspekty, ktoré by mohli podporiť zakladanie spoločností v Európskej únii, a tým podporiť inovačný rast, by malo byť **zníženie nákladov na založenie spoločností**, automatické uznávanie spoločností v rámci európskeho priestoru a zníženie administratívnej záťaže. Respondenti zároveň uvádzali, že kľúčovým aspektom 28. režimu by malo byť aj prijatie **moderného rámca spoločností, ktorý by bol vytvorený od nuly** a nebol by „patchwork-om“ existujúcich národných právnych regulácií.²²

Je nutné zopakovať, že predstavená spätná väzba sa dominantne týkala Nemecka, ktoré je ale najväčšou ekonomikou Európskej únie (24% HDP Európskej únie²³).

Smernica 2019/1151 – prvý veľký krok v digitalizácii zakladania spoločností

Zjednodušenie procesu zakladania spoločností v Európskej únii je už aj v súčasnosti hlboko zakotvené v legislatívnej činnosti Európskej únie. Dňa 20. júna 2019 bola prijatá Smernica 2019/1151 a dňa 19. decembra 2024 bola prijatá Smernica 2025/25. Prijatie Smernice **2019/1151** vychádzalo z analýzy skupiny Informal Company Law Expert Group (ICLEG)²⁴ – „Report on digitalisation in company law“, ktorá bola vypracovaná v marci 2016. V niektorých ustanoveniach Smernica 2019/1151 nadväzuje dokonca na návrh Smernice SUP²⁵, v rámci ktorého bola predstavená koncepcia online registrácie spoločností²⁶ vrátane poskytnutia vzorových stanov²⁷ pre spoločnosti s jedným spoločníkom.

²² https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU/feedback_sk?p_id=19997 (cit. 27.09.2025).

²³ https://european-union.europa.eu/principles-countries-history/eu-countries/germany_en?utm_source=chatgpt.com (cit. 27.09.2025).

²⁴ ICLEG predstavuje neformálnu pracovnú skupinu odborníkov na obchodné právo, zriadenú Európskou komisiou na poskytovanie odborných odporúčaní v oblasti digitalizácie práva obchodných spoločností.

²⁵ Návrh smernice Európskeho parlamentu a Rady o spoločnostiach s ručením obmedzeným s jedným spoločníkom /* com/2014/0212 final - 2014/0120 (cod) */ (ďalej len „**Smernica SUP**“).

²⁶ BITĚ, Virginijus – ROMASHCHENKO, Ivan: Online Formation of Companies in Lithuania in a Comparative Context: Implementation of the Digitalisation Directive and Beyond. In: European Business Organization Law Review, Roč. 24, č. 4 (2023) 24, s. 650.

²⁷ ŠULEKOVÁ, Žofia: Elektronizácia v korporačnom práve. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.): Právo, obchod, ekonomika VI. Košice: Univerzita P. J. Šafárika v Košiciach, 2016, s. 554.

Smernica 2019/1151²⁸ predstavovala prvý veľký krok v digitalizácii zakladania spoločností (a pobočiek) v Európskej únii, keďže medzi členskými štátmi bol veľký rozdiel v dostupnosti digitálnych nástrojov (nielen) v procese zakladania obchodných spoločností.²⁹ Smernica 2019/1151 priniesla s ohľadom na proces zakladania spoločností najmä online zakladanie spoločností bez potreby fyzickej prítomnosti zakladateľov³⁰ aspoň pre určité právne formy spoločností³¹ vrátane zakladania pobočiek, ako aj elektronické podávanie dokumentov a informácií do registrov.³² Ďalším cieľom smernice zameraným na zjednodušenie procesu zakladania spoločností bolo poskytnutie vzorov zakladateľských dokumentov dostupných prostredníctvom jednotnej digitálnej brány.³³ Zakladatelia by mať možnosť zvoliť si založenie spoločnosti pomocou online dostupných vzorov namiesto klasického zakladacieho aktu.³⁴ V zmysle smernice by členské štáty mali vzory sprístupniť vo svojom úradnom jazyku ako aj ďalšom úradnom jazyku EÚ, ktorému rozumie čo najviac cezhraničných používateľov.³⁵ Proces zakladania spoločností ale nie je len o zakladateľskom dokumente, jednotlivé jurisdikcie požadujú pri zakladaní rôzne iné dokumenty, ktorých poskytnutie nie je v rámci smernice riešené a štandardizované, čo podľa nášho názoru limituje dosiahnutie cieľa smernice o (plnohodnotnom) online procese zakladania obchodných spoločností.³⁶

²⁸ Smernica 2019/1151 sa venuje aj iným otázkam ako je zjednodušenie procesu zakladania spoločností, ktoré ale nie sú predmetom analýzy v rámci tohto príspevku.

²⁹ MAKSIMOVIĆ SEKULIĆ, Nina: The significance of Directive 2019/1151 in the digitalization of European Union company law. In: Pravo - teorija i praksa, Roč. 40, č. 3 (2023), s. 68.

³⁰ Fyzická prítomnosť navrhovateľa by sa mala vyžadovať len výnimočne, napríklad, ak existuje podozrenie na falšovanie totožnosti alebo nejasnosti týkajúce sa oprávnenia zastupovať spoločnosť. Smernica 2019/1151, preambula, bod 21.

³¹ Smernica 2019/1151 bola zameraná na spoločnosti typu spoločnosti s ručením obmedzeným. Smernica 2019/1151, Príloha IIA.

³² Smernica 2019/1151, preambula, bod 14.

³³ Smernica 2019/1151, preambula, bod 18.

³⁴ V kontexte otázky miery možnosti modifikácie vzorových dokumentov súhlasíme s Mrázovou a Cukerovou, ktoré uvádzajú, že keďže Smernica 2019/1151 nešpecifikuje rozsah, v akom môžu zakladatelia modifikovať vzorový zakladateľský dokument, úplné priznanie zmluvnej voľnosti by pravdepodobne odporovalo samotnému účelu vzorových zakladateľských zmlúv. MRÁZOVÁ, Žofia – CUKEROVÁ, Dominika: How the Digitalisation Has Changed the Slovak Company Law: Implementation of the Directive 2019/1151 (Digitalisation Directive) and What Next? In: EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC), č. 7 (2023), s. 340.

³⁵ Smernica 2019/1151, článok 13h ods. 3.

³⁶ Zhodne Mrázová a Cukerová, ktoré v tomto kontexte uvádzajú: „On the other hand, the standardisation is assumed only in relation to the articles of association, therefore the simplification and acceleration of the process by using the online tools could be slightly relativised. Other documents and data will have to be prepared and provided by the founders in electronic form in accordance with the national law of the Member State in which the company is to have its registered office.“ MRÁZOVÁ, Žofia

Smernica 2019/1151 bola zároveň zameraná na i) podporu transparentnosti a dôveryhodnosti prostredníctvom prepojenia obchodných registrov v Európskej únii (BRIS)³⁷, ii) používania prostriedkov elektronickej identifikácie v zmysle Nariadenia eIDAS³⁸ ako aj iii) prevencie proti podvodom a ochranu pred zneužitím, ako je napríklad tzv. „company hijacking“. ³⁹ Smernica 2019/1151 zavádza aj kľúčový princíp „jedenkrát a dost“ v procese zakladania spoločností a pobočiek, ktorého cieľom bolo zabezpečiť, aby spoločnosti nemuseli predkladať orgánom verejnej správy dokumenty viac ako raz a zároveň, aby spoločnosť založená v jednom členskom štáte mala mať možnosť využívať predtým predložené dokumenty pri zápise pobočky v inom štáte a predkladať zmeny údajov len jednému registru. Registre by si mali tieto údaje automaticky vymieňať elektronicke cez systém prepojenia registrov.⁴⁰ Cieľom smernice bolo aj zabezpečenie rovnováhy medzi digitalizáciou a právnou istotou, čo umožnilo členským štátom, aby si mohli zachovať niektoré garancie v procese zakladania spoločností (napr. využitie notárov alebo právnych expertov), pokiaľ to nebolo v rozpore s požiadavkou, že proces zakladania spoločnosti musí byť možný aj online.⁴¹ Transpozičné obdobie Smernice 2019/1151 uplynulo 1. augusta 2022 a vo vzťahu k niektorým článkom smernice 1. augusta 2023.

Je nepochybné, že Smernica 2019/1151 predstavovala dôležitý posun smerom k digitalizácii obchodného práva, ale z jej rozsahu je zrejmé, že jej účinky sú limitované

– CUKEROVÁ, Dominika: How the Digitalisation Has Changed the Slovak Company Law: Implementation of the Directive 2019/1151 (Digitalisation Directive) and What Next? In: EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC), č. 7 (2023), s. 340.

³⁷ Pravidlá pre prepojenie obchodných registrov v rámci Európskej únie boli zavedené Smernicou Európskeho parlamentu a Rady 2012/17/EÚ z 13. júna 2012, ktorou sa mení a dopĺňa smernica Rady 89/666/EHS a smernice Európskeho parlamentu a Rady 2005/56/ES a 2009/101/ES, pokiaľ ide o prepojenie centrálnych registrov, obchodných registrov a registrov spoločností, ako aj Vykonávacím nariadením Európskej komisie (EÚ) 2015/884 z 8. júna 2015 2012/17/EÚ. Momentálne sú tieto pravidlá obsiahnuté v Smernici Európskeho parlamentu a Rady (EÚ) 2017/1132 zo 14. júna 2017 týkajúcej sa niektorých aspektov práva obchodných spoločností a vo Vykonávacom nariadení Komisie (EÚ) 2021/1042 z 18. júna 2021, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2017/1132, pokiaľ ide o technické špecifikácie a postupy pre systém prepojenia registrov, a ktorým sa zrušuje vykonávacie nariadenie Komisie (EÚ) 2020/2244 (ďalej len „BRIS“). BRIS umožňuje elektronický prístup k informáciám a dokumentom o spoločnostiach uloženým v obchodných registroch členských štátov prostredníctvom Európskeho portálu elektronickej justície a zároveň zabezpečuje výmenu údajov medzi jednotlivými registrami o cezhraničných operáciách, spoločnostiach a ich pobočkách. https://commission.europa.eu/business-economy-euro/doing-business-eu/company-law-and-corporate-governance_en (cit. 27.09.2025).

³⁸ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronicke transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“).

³⁹ Smernica 2019/1151, preambula, bod 20.

⁴⁰ Smernica 2019/1151, preambula, bod 28.

⁴¹ Smernica 2019/1151, preambula, bod 20.

a nepokrývajú všetky fázy existencie spoločnosti, keďže smernica sa zameriava práve na aspekty zakladania spoločností⁴² a nie na širší aspekt ich fungovania. Ako uvádza aj Sokol, aplikácia digitálnych technológií v celom životnom cykle obchodnej spoločnosti bola zdôrazňovaná už v Oznámení Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom „Zlepšovanie jednotného trhu: viac príležitostí pre ľudí a podniky“ z roku 2015.⁴³ Limit smernice spočíva aj v izolovanom zameraní na poskytnutie vzoru zakladateľského dokumentu, bez poskytnutia vzorov iných dokumentov, ktoré členské štáty požadujú v procese zakladania spoločností.

Smernica 2025/25 – ďalší krok v digitalizácii zakladania spoločností

S ohľadom na pretrvávajúce otvorené otázky digitalizácie zakladania spoločností, hlavne s ohľadom na cezhraničné situácie⁴⁴, Európska únia nadviazala na Smernicu 2019/1151 prijatím Smernice 2025/25 dňa 19. decembra 2024. **Smernica 2025/25** predstavuje reakciu na iniciatívu: „Upgrading digital company law“⁴⁵, verejnú konzultáciu, reporty ICLEG⁴⁶ ako aj nasledujúce strategické dokumenty Európskej únie: Digitalizácia justície v Európskej únii: súbor príležitostí⁴⁷, Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob⁴⁸, Stratégia pre MSP pre

⁴² MRÁZOVÁ, Žofia – CUKEROVÁ, Dominika: How the Digitalisation Has Changed the Slovak Company Law: Implementation of the Directive 2019/1151 (Digitalisation Directive) and What Next? In: EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC), č. 7 (2023), s. 337.

⁴³ SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. Bratislava: Nakladateľství C.H.Beck-SK, 1. vydanie, 2024. S. 5-9, marg. č. 23. ISBN: 978-80-8232-050-6 (cit. 29.11.2025).

⁴⁴ SCHMIDT, Jessica: The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers. In: European Company and Financial Law Review, Roč. 21, č. 5-6 (2024), s. 564.

⁴⁵ SCHMIDT, Jessica: The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers. In: European Company and Financial Law Review, Roč. 21, č. 5-6 (2024), s. 564.

⁴⁶ ICLEG, Report on Transparency of Company Data, 2023; ICLEG, Report on crossborder use of company information, 2023 (oba reporty sú dostupné na: https://commission.europa.eu/business-economy-euro/doing-business-eu/company-law-and-corporate-governance_en). SCHMIDT, Jessica: The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers. In: European Company and Financial Law Review, Roč. 21, č. 5-6 (2024), s. 564.

⁴⁷ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Digitalizácia justície v Európskej únii – súbor príležitostí, COM/2020/710 final.

⁴⁸ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob, COM(2021) 118 final.

udržateľnú a digitálnu Európu⁴⁹ a Aktualizácia novej priemyselnej stratégie na rok 2020: budovanie silnejšieho jednotného trhu pre obnovu Európy⁵⁰.

S ohľadom na zjednodušenie zakladania spoločností v Európskej únii⁵¹ je cieľom Smernice 2025/25 zabezpečiť správnu a bezpečnú identifikáciu zakladateľov a riaditeľov spoločností s cieľom podporiť zákonnosť transakcií, spoľahlivosť verejných registrov a prevenciu nezákonných činností.⁵² Smernica umožňuje členským štátom zaviesť doplnkové elektronické kontroly totožnosti a právnej spôsobilosti vrátane zlepšenia, spoľahlivosti a aktuálnosti údajov v registroch, ako aj zvýšenia prepojenia registrov.⁵³ Preambula Smernice 2025/25 uvádza, že prístup k spoľahlivým údajom o spoločnostiach z registrov a ich využitie v cezhraničných situáciách je stále obmedzený. Údaje o spoločnostiach nie sú dostatočne dostupné ani vo vnútroštátnych registroch, ani cez systém prepojenia obchodných registrov (BRIS) na európskej úrovni a zakladanie spoločností je brzdené aj časovo a finančne náročnými postupmi, ako sú administratívne formality pred orgánmi, súdne konania či potreba apostilovania a úradných prekladov dokumentov. Cieľom Smernice 2025/25 je v kontexte zakladania spoločností aj odstránenie týchto bariér prostredníctvom nasledujúcich nástrojov⁵⁴: (i) digitálna plná moc EÚ, (ii) osvedčenie spoločnosti EÚ a (iii) prehlbovanie princípu „jedenkrát a dost“.

Digitálna plná moc EÚ by mala byť založená na viacjazyčnom spoločnom európskom vzore, ktorý sa spoločnosti môžu rozhodnúť používať s cieľom opraviť osobu, aby zastupovala spoločnosť v konkrétnych postupoch s cezhraničným rozmerom v rozsahu pôsobnosti smernice. Tento vzor by mal obsahovať aspoň dátové polia týkajúce sa rozsahu zastúpenia, osoby oprávnenej zastupovať spoločnosť a druhu zastúpenia. Digitálna plná moc EÚ by sa vyhotovovala v súlade s vnútroštátnymi právnymi požiadavkami. Zároveň, by digitálna plná moc EÚ mala spĺňať požiadavky na elektronické osvedčenie atribútov stanovené v nariadení

⁴⁹ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Stratégia pre MSP pre udržateľnú a digitálnu Európu, COM/2020/103 final.

⁵⁰ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Aktualizácia novej priemyselnej stratégie na rok 2020: budovanie silnejšieho jednotného trhu pre obnovu Európy, COM/2021/350 final.

⁵¹ Smernica 2025/25 sa venuje aj iným otázkam ako je zjednodušenie procesu zakladania spoločností, ktoré ale nie sú predmetom analýzy v rámci tohto príspevku.

⁵² Smernica 2025/25, preambula, bod 10.

⁵³ Predmetné by malo byť zabezpečené prepojením nielen obchodných registrov (BRIS), ale aj registrov konečných užívateľov výhod (BORIS) a systému vzájomného prepojenia insolvenčných registrov (IRI) na úrovni Európskej únie. Smernica 2025/25, preambula, bod 10.

⁵⁴ Smernica 2025/25 obsahuje aj iné nástroje (napríklad preventívnu kontrolu), ktoré ale nie sú predmetom analýzy v rámci tohto príspevku.

Európskeho parlamentu a Rady (EÚ) 2024/1183 (12)⁵⁵ a technické špecifikácie európskej peňaženky digitálnej identity⁵⁶, aby sa zabezpečilo spoločné riešenie so zvýšenou používateľskou ústretovosťou. Digitálna plná moc EÚ by mala existovať výlučne v digitálnej podobe a jej autentifikácia by mala prebiehať prostredníctvom dôveryhodných služieb v súlade s Nariadením eIDAS.⁵⁷

Osvedčenie spoločnosti EÚ by malo predstavovať nový štandardizovaný dokument, ktorý by mal byť vydávaný národnými registrami a mal by potvrdzovať existenciu ako aj základné údaje o spoločnosti. Tento dokument by mal byť dostupný vo všetkých úradných jazykoch EÚ. Vydávať by sa mal v digitálnej podobe a mal by byť automaticky uznávaný vo všetkých členských štátoch bez potreby ďalších overovaní či apostíl. Osvedčenie spoločnosti EÚ by malo uľahčiť najmä cezhraničné zakladanie spoločností a pobočiek ako aj dokazovanie právnej existencie spoločnosti, a jej základných dát pri bankách, investoroch, úradoch a orgánoch. Elektronické osvedčenie spoločnosti EÚ by sa malo autentifikovať prostredníctvom dôveryhodných služieb v súlade s Nariadením eIDAS. Aj tretie strany, vrátane orgánov, ktoré potrebujú spoľahlivé základné údaje o spoločnostiach, by mali mať možnosť požiadať o elektronické osvedčenie spoločnosti EÚ pre konkrétnu spoločnosť.⁵⁸

Smernica 2025/25 prehlbuje aplikáciu zásady „**jedenkrát a dost**“ hlavne pri zakladaní dcérskych spoločností a pobočiek cezhranične. Spoločnosti nebudú musieť opakovane predkladať tie isté údaje viacerým orgánom alebo v rôznych členských štátoch. Údaje zadané raz (napr. pri zápise do obchodného registra) sa budú zdieľať a sprístupňovať cez systém prepojenia obchodných registrov (BRIS) v celej Európskej únii. Predmetné výrazne zníži duplicitu administratívnych úkonov ako aj náklady na preklad, overovanie alebo apostilovanie.⁵⁹ Orgány, ktoré potrebujú overiť konkrétne údaje o spoločnosti z iného členského štátu, by mali najprv použiť elektronické osvedčenie spoločnosti EÚ alebo údaje zo systému prepojenia registrov, namiesto žiadosti o preklad celého dokumentu. Právo členských štátov požadovať neúradný preklad do jedného zo svojich úradných jazykov zostáva zachované, ak je potrebný celý dokument pre konkrétny postup. V prípade úradných prekladov by sa právne požiadavky mali obmedziť na nevyhnutné minimum a tieto preklady by sa mali vyžadovať len v osobitných prípadoch.⁶⁰

⁵⁵ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>) (cit. 27.09.2025).

⁵⁶ European Digital Identity Wallet.

⁵⁷ Smernica 2025/25, preambula, body 27-28.

⁵⁸ Smernica 2025/25, preambula, bod 24.

⁵⁹ Smernica 2025/25, preambula, body 12-13.

⁶⁰ Smernica 2025/25, preambula, body 32.

Transpozícia Smernice 2025/25 je stanovená na 31. júla 2027 s účinnosťou zákonov a právnych predpisov od 31. júla 2028, pričom niektoré články Smernice majú posunutú transpozíciu do 1. augusta 2028 s účinnosťou zákonov a právnych predpisov od 1. augusta 2029.⁶¹

28. režim – právny rámec EÚ pre podniky – ďalšie kroky Európskej únie v zjednodušovaní zakladania spoločností v Európskej únii

Ako sme v úvode uviedli, Európska komisia v júli 2025 vyhlásila verejnú konzultáciu k 28. režimu za účelom zozbierania spätnej väzby, ako aj problémov a návrhov riešení zakladania ako aj fungovania spoločností v Európskej únii.⁶² Sprievodný materiál k tejto iniciatíve uvádza, že základným problémom Európskej únie v otázke zakladania spoločností je fragmentácia právnych poriadkov v jednotlivých členských štátoch, čo obmedzuje podnikateľskú činnosť a bráni spoločnostiam využívať príležitosti jednotného trhu pri zakladaní, tvorbe štruktúry ako aj prevádzkovaní spoločností.⁶³ Podnikatelia požadujú zníženie administratívnej záťaže, zvýšenie digitalizácie a prehlbovanie aplikácie zásady „jedenkrát a dost“ v procese zakladania spoločností. Startupy zároveň upozorňujú, že zakladanie spoločností a investovanie sú stále príliš zložité, pomalé a rozdielne v jednotlivých členských štátoch, čo im bráni škálovať v rámci Európskej únie. Zároveň chýba jednotná a rozpoznateľná značka spoločnosti Európskej únie, ktorá by posilnila dôveru investorov a partnerov.⁶⁴

Európska komisia v sprievodnom dokumente k 28. režimu uvádza, že právnym základom iniciatívy by mohlo byť buď nariadenie alebo smernica a zároveň uvádza rôzne scenáre, ktoré môžu byť výsledkom vyhlásenej iniciatívy. Po prvé, ak nenastane zmena politiky, tak spoločnosti vrátane startupov a scaleupov, budú aj naďalej čeliť rôznym vnútroštátnym pravidlám, ich fragmentácii a nedostatočnej digitalizácii postupov pri zakladaní spoločností, čo by naďalej obmedzovalo ich rast a prilákanie investícií naprieč Európskou úniou.⁶⁵

Druhou cestou je, že politiky pre právny rámec Európskej únie v tejto oblasti by spájali už existujúce aj pripravované prvky s cieľom znížiť administratívnu záťaž a podporiť zakladanie inovačných spoločností (startupy) ako aj rast scaleupov. Základom by mali byť online postupy pre zakladanie spoločností a zapisovanie údajov do registra, využívanie systému BRIS a digitálnych nástrojov, ako je EUID⁶⁶, osvedčenie spoločnosti EÚ a európska podniková peňaženka⁶⁷. Súčasťou právneho

⁶¹ Smernica 2025/25, článok 4.

⁶² 28. režim – právny rámec EÚ pre podniky, s. 3.

⁶³ 28. režim – právny rámec EÚ pre podniky, s.1.

⁶⁴ 28. režim – právny rámec EÚ pre podniky, s.2.

⁶⁵ 28. režim – právny rámec EÚ pre podniky, s. 2.

⁶⁶ Európsky jedinečný identifikátor (EUID).

⁶⁷ European Business Wallet.

rámca by bolo aj stanovenie štruktúry a základných prvkov spoločností podľa 28. režimu a zabezpečenie jednoduchých, flexibilných a rýchlych procesov vrátane možnosti založiť spoločnosť do 48 hodín. Dôležitým prvkom by bola aj podpora investícií prostredníctvom digitálnych riešení, rôznych tried akcií či dohôd v oblasti súkromného kapitálu.⁶⁸

Po ukončení 12-týždňovej verejnej konzultácie by malo nasledovať jej vyhodnotenie, následne diskusie s členskými štátmi a zainteresovanými stranami, odborné debaty v rámci skupiny ICLEG ako aj ďalšie ciele konzultácie s podnikateľmi a spoločnosťami v roku 2025. Konečná správa z verejnej konzultácie je momentálne plánovaná na hlasovanie v pléne Európskeho parlamentu na december 2025, ambicióznosť časového harmonogramu zodpovedá politickým a ekonomickým prioritám tejto iniciatívy v Európskej únii.⁶⁹

Bližší vhľad do 28. režimu v kontexte zakladania spoločností prináša dokument vypracovaný na základe požiadavky Výboru pre právne veci (JURI) Európskeho parlamentu: *Simplification of registration of companies in the 28th Regime, Towards a single digital company register*⁷⁰, ktorého autorom je Prof. Dr. Florian MÖSLEIN, LL.M.⁷¹

Tento dokument uvádza, že kľúčovým pilierom 28. režimu je zjednodušenie a digitalizácia procesov registrácie spoločností, ktoré sú v súčasnosti fragmentované v jednotlivých členských štátoch. Iniciatíva má za cieľ vytvoriť **jednotný register spoločností na úrovni Európskej únie (európsky obchodný register) a inovatívnu európsku spoločnosť (Innovative European Company, IEC).**

Európsky obchodný register by mal mať viacjazyčný prístup s možnosťou spracovania údajov v reálnom čase prostredníctvom bezpečných digitálnych identifikačných systémov podľa Nariadenia eIDAS a mal by zabezpečovať zakladanie v spoločnosti v lehote 48 hodín. V otázke zjednodušenia zakladania spoločností by 28. režim mal stavať na základoch nedávnej legislatívy Európskej únie, vrátane Smerníc 2019/1151 a 2025/25, a zároveň ísť výrazne ďalej tým, že by mal prechádzať od koordinácie národných systémov členských štátov k vytvoreniu jednotného právneho rámca na úrovni Európskej únie. Jeho konečným cieľom nie je byť len právnou alternatívou, ale slúžiť ako základný nástroj na podporu zakladania

⁶⁸ 28. režim – právny rámec EÚ pre podniky, s. 3.

⁶⁹ *Simplification of registration of companies in the 28th Regime, Towards a single digital company register*, Policy Department for Justice, Civil Liberties and Institutional Affairs Directorate-General for Citizens' Rights, Justice and Institutional Affairs PE 776.000 - July 2025, s. 12.

⁷⁰ *Simplification of registration of companies in the 28th Regime, Towards a single digital company register*, Policy Department for Justice, Civil Liberties and Institutional Affairs Directorate-General for Citizens' Rights, Justice and Institutional Affairs PE 776.000 - July 2025 (ďalej len „**Simplification of registration of companies in the 28th Regime, Towards a single digital company register**“).

⁷¹ Institute for Law and Regulation of Digitalisation (IRDi), Marburg University, School of Law.

a fungovania spoločností v rámci jednotného trhu aj prostredníctvom európskeho obchodného registra.⁷²

Navrhovaný 28. režim by preto nadväzoval na existujúce *acquis communautaire*, no jeho cieľom je výrazne posunúť hranice tým, že umožní zakladanie spoločností cez jednotný, centrálné spravovaný registračný systém európskeho obchodného registra. Tým by sa eliminovala potreba odlišných vnútroštátnych postupov a súčasne by sa zabezpečila vyššia právna istota, jednoduchšia cezhraničná operabilita a efektívnejšia administratíva.⁷³ V prípade európskeho obchodného registra by malo ísť o platformu prevádzkovanú na úrovni Európskej únie (napr. prostredníctvom agentúry alebo nového orgánu), na ktorej by sa realizovali všetky zakladania a zápisy pre novú právnu formu spoločnosti Európskej únie. Takýto register by dopĺňal alebo rozširoval BRIS, a namiesto prepojenia národných databáz by vytváral priamy vstupný bod pre spoločnosti registrované podľa právneho rámca Európskej únie. Všetky udalosti počas životného cyklu spoločnosti (založenie, zápisy, aktualizácie) by sa spravovali iba raz a údaje by boli prístupné vo všetkých členských štátoch, čo by zaručovalo jednotnú používateľskú skúsenosť a rovnaký prístup pre zakladateľov bez ohľadu na ich polohu.⁷⁴

Jednotný systém elektronickej identifikácie a autentifikácie je pre zakladanie spoločností kľúčový, a preto sa navrhuje využitie rámca eIDAS vrátane pripravovaných európskych digitálnych peňaženiek⁷⁵ na bezpečné overenie totožnosti podnikateľov. Zakladatelia by mali mať možnosť spoločnosť založiť online z ktoréhokolvek miesta v Európskej únii bez fyzických dokumentov či notárskeho overenia. Používanie eIDAS-kompatibilných podpisov a dokumentov by eliminovalo potrebu legalizácií, ako sú apostily alebo overené preklady, čím sa výrazne znížila administratívna záťaž.⁷⁶ Sprievodný dokument k 28. režimu spomína pre zjednodušenie procesu zakladania spoločností aj inkorporáciu moderných technológií, ako blockchain a inteligentné kontrakty (smart contracts), aby sa zabezpečili nezmeniteľné záznamy, reálne aktualizácie registra a vyššia dôvera v údaje, pričom tieto technológie by umožnili efektívnu a bezpečnú prevádzku európskeho obchodného registra. Návrh zahŕňa prísne dodržiavanie opatrení proti

⁷² Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 9.

⁷³ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 13.

⁷⁴ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 25.

⁷⁵ European Digital Identity Wallet.

⁷⁶ Predmetná bariéra zakladania spoločností v podobe potreby overovania, apostilovania a prekladov dokumentov by mala byť výrazne eliminovaná už aj transpozíciou Smernice 25/2025 do právnych poriadkov členských štátov.

praniu špinavých peňazí (AML), prepojenie s registrom konečných užívateľov výhod a prípadný dohľad na úrovni Európskej únie, aby sa zabezpečila dôvera v spoločný systém. Kombinácia vhodnej technológie, právnych predpisov a správy systému by umožnila, aby bol európsky obchodný register efektívny, rýchly, používateľsky prívetivý a zároveň právne spoľahlivý.⁷⁷

28.režim by mal zároveň priniesť nový európsky právny nástroj v podobe **inovatívnej európskej spoločnosti (Innovative European Company, IEC)**⁷⁸, ktorá bola podporená aj v Letta Reporte.⁷⁹ IEC by disponovala jednotnou digitálnou identitou platnou v celej Európskej únii uznávanou všetkými členskými štátmi, pričom registrácia by prebiehala centralizovane na úrovni Európskej únie.⁸⁰ Dokument uvádza, že ideálne by bolo zavedenie IEC ako nadnárodnej právnej formy upravenej nariadením, keďže takýto model by umožnil úplné osamostatnenie od národných postupov zakladania spoločností a zabezpečilo by sa jednotné zaobchádzanie. IEC by mohlo byť prijaté ale aj prostredníctvom smernice, ak by sa členské štáty dohodli na plnej harmonizácii registračných pravidiel a centralizovanom prenesení niektorých administratívnych funkcií na úroveň Európskej únie. Takto upravený systém by musel presiahnuť súčasný rámec BRIS-u, aby umožnil priamy zápis, overovanie a aktualizácie dát o spoločnostiach počas celého životného cyklu prostredníctvom registra spravovaného Európskou úniou.⁸¹

V závere dokument (Simplification of registration of companies in the 28th Regime, Towards a single digital company register) zhŕňa základné odporúčania pre európsky obchodný register:

- **Zaviest' jednotnú digitálnu identitu a identifikátor spoločnosti (Adopt a Unified Digital Identity and Company Identifier):** Vytvoriť jednotnú digitálnu identitu a identifikátor spoločnosti prepojené s pripravovanou európskou digitálnou peňaženkou (European Digital Identity Wallet), ktorá umožní bezpečne uchovávať a zdieľať overiteľné dokumenty, ako sú

⁷⁷ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 25.

⁷⁸ Ako uvádzajú Meyer-Erdmann a Hoffman, aj keď mnohé podrobnosti návrhu zostávajú nejasné, z celkových diskusií vyplýva, že predložená iniciatíva „EU-Inc.org“ (2025), podporovaná startupmi a investormi rizikového kapitálu, sa stala východiskom pre návrh 28. režimu. MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 4.

⁷⁹ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 11.

⁸⁰ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 12.

⁸¹ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 26.

zakladateľské listiny, rozhodnutia predstavenstva alebo daňové doklady s orgánmi v celej Európskej únii.

- **Využiť blockchain pre dôveru a transparentnosť (Leverage Blockchain for Trust and Transparency):** Aplikovať technológiu blockchain, inšpirovanú systémami EBSI⁸² a estónskym KSI, na nezmeniteľné časové pečiatky dôležitých udalostí spoločností (napr. zakladanie, prevod akcií, rozhodnutia predstavenstva) a poskytovať šablóny inteligentných kontraktov (smart contracts) na automatizáciu rutinných kontrol, ako sú pravidlá zachovania kapitálu alebo ročné ukladania podkladov do registra.
- **Zaviest' princíp „jedenkrát a dost“ a cezhraničnú výmenu údajov (Implement the Once-Only Principle and Cross-Border Data Exchange):** Všetky procesy „start a business“ musia byť do roku 2026 plne digitalizované a interoperabilné podľa cieľov Single Digital Gateway⁸³, pričom štandardizované rozhrania na programovanie aplikácií (Application Programming Interfaces, APIs) umožnia prepojenie národných registrov a rozšírenie systému BRIS na automatické zdieľanie údajov.
- **Automatizovať overovanie pomocou AI a digitálnej verifikácie (Automate Validation with AI and Digital Verification):** Integrovať nástroje umelej inteligencie na automatické overovanie zakladateľských dokumentov, identít a notárskych overení v reálnom čase, vrátane kontroly národných a európskych registrov a zoznamov (konečný užívateľ výhod, sankčné zoznamy) a napojenia na databázy e-Justice a obchodných registrov.
- **Zaviest' overiteľné poverenia a elektronické podpisy (Embed Verifiable Credentials and e-Signatures):** Zabezpečiť, aby všetky nové dokumenty (zakladateľské listiny, rozhodnutia, plné moci) boli prijímané výlučne v digitálnej forme s použitím kvalifikovaných elektronických podpisov alebo certifikátov (Nariadenie eIDAS); európska digitálna peňaženka umožní uchovávať právne záväzné certifikáty a predkladať ich na požiadanie v ktoromkoľvek členskom štáte.
- **Architektúra platformy s modulárnym prístupom (Architect the 28th-regime platform with plug-in modules):** Platforma by mala byť modulárna, aby umožňovala pridávanie funkcií, ako sú ESG reportovanie, zjednodušené formuláre pre malé a stredné podniky alebo štandardné doložky pre rizikový kapitál (venture capital), bez zásahu do jadra systému; súkromný sektor a akademická obec by mohli navrhovať nové moduly prostredníctvom transparentného trhu založeného na APIs.

⁸² European Blockchain Services Infrastructure.

⁸³ https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway_en (cit. 27.09.2025).

- **Vytvoriť orgán správy a dohľadu (Create a governance body):** Zriadiť správnu radu zloženú z národných registrov, Európskej komisie, Európskeho dozorného úradníka pre ochranu údajov (European Data Protection Supervisor) a zástupcov priemyslu a občianskej spoločnosti, ktorá bude dohliadať na integritu systému, schvaľovať nové moduly, monitorovať výkonnosť (napr. čas potrebný na založenie spoločnosti) a koordinovať technické štandardy.⁸⁴

Záver – dokážu harmonizačné opatrenia Európskej únie a 28. režim riešiť problémy praxe pri zakladaní spoločností?

Spätná väzba respondentov v rámci verejnej konzultácie jasne ukazuje, že medzi praktickou realitou zakladania spoločností a ambíciami európskej legislatívy stále existuje značná priepasť. Hoci Smernica 2019/1151 zaviedla povinnosť členských štátov umožniť online zakladanie spoločností, elektronické podávanie listín do registrov, poskytnutie vzorov zakladateľských dokumentov a prepojenie registrov prostredníctvom systému BRIS, respondenti opakovane poukazujú, že postupy zakladania spoločností zostávajú pomalé, administratívne náročné a výrazne odlišné naprieč členskými štátmi.⁸⁵ Digitalizácia sa tak podľa respondentov prejavuje skôr formálne než obsahovo, pričom v praxi pokračuje klasické „papierové“ zakladanie spoločností, pretrvávajú prietahy v procese zakladania spoločností, duplicita predkladania dokumentov ako aj potreba fyzickej prítomnosti zakladateľov.

Smernica 2025/25 reaguje na viaceré z týchto výhrad, najmä zavedením osvedčenia spoločnosti EÚ a digitálnej plnej moci EÚ, ktoré eliminujú potrebu apostilovania a opakovaných overení existencie spoločnosti. Smernica zároveň prehlbuje princíp „jedenkrát a dost“. Z pohľadu spätnej väzby od respondentov ide o zásadný krok, pretože odstránenie nadbytočných overovaní, úradných prekladov a fragmentovaných postupov patrilo medzi najčastejšie uvádzané komplikácie. Smernica 2025/25 síce neeliminuje úplne potrebu prekladov dokumentov, ale výrazne ju koriguje, pričom bude závisieť od členských štátov, ako v procese transpozície naplnia ciele smernice a minimalizujú byrokratizáciu a vysoké transakčné náklady zakladania spoločností.

Zásadným problémom, ktorý v spätných väzbách rezonoval, je aj pretrvávajúca rola notárov a finančná nákladnosť procesu zakladania spoločností. Smernica 2019/1151 výslovne ponecháva členským štátom možnosť zachovať účasť notárov v procese

⁸⁴ Simplification of registration of companies in the 28th Regime, Towards a single digital company register, s. 38-39.

⁸⁵ Samozrejme zohľadňujeme, že tieto nedostatky boli identifikované predovšetkým v odpovediach nemeckých respondentov, považujeme ich ale za relevantné s ohľadom na skutočnosť, že Nemecko predstavuje najväčšiu ekonomiku EÚ.

zakladania spoločností, a hoci Smernica 2025/25 znižuje administratívne náklady nepriamo, najmä odstránením apostíl a úradných prekladov, samotnú povinnosť využívať notára neprelamuje. Respondenti vo viacerých prípadoch uvádzajú, že práve nevyhnutná notárska participácia, často spojená s potrebou osobnej účasti zakladateľov, predstavuje najväčšie úskalie celého procesu, pričom digitálne nástroje sú v praxi degradované na doplnkové prostriedky.⁸⁶ Je citelné, že v tejto otázke Európska únia váži digitalizáciu a potrebu *ex ante* kontroly v procese zakladania spoločností, ktorú sa snaží tiež zjednocovať.

Podstatnou výhradou respondentov je tiež pretrvávajúca fragmentácia korporáčného práva, keďže ani Smernica 2019/1151, ani Smernica 2025/25 neriešia materiálne rozdiely medzi právnymi poriadkami, ale upravujú len procesné a technické otázky zakladania spoločností a pobočiek. Respondenti často uvádzajú, že vnútorný trh je síce deklarovaný, no v oblasti zakladania spoločností pôsobí skôr ako 27 samostatných trhov, pričom každý vyžaduje iné formality a predpoklady. Táto fragmentácia zároveň znižuje atraktivitu európskych právnych foriem pre investorov. Tieto nedostatky sú zreteľne reflektované v návrhoch 28. režimu, ktorý predstavuje najambicióznejší pokus prekonať fragmentáciu právnych poriadkov prostredníctvom zavedenia jednotného európskeho registra ako aj novej európskej právnej formy (IEC). 28. režim rieši možnosti využitia automatizovaných kontrol zákonnosti a rozšírenia digitalizácie na úroveň, ktorá presahuje rámec technickej modernizácie smerníc. Dokument Prof. Möseleina, vypracovaný na požiadavku výboru JURI, ponúka ďalšie odborné odporúčania, napríklad nahradenie tradičných overovacích mechanizmov tzv. smart validáciou alebo centralizované preverovanie údajov v rámci EÚ. Mnohé z odporúčaní reagujú priamo na problémy, ktoré uvádzali respondenti – napríklad nemožnosť plynule zakladať spoločnosti cez hranice, rôzne požiadavky na notárske úkony či opakujúce sa AML a KYC procesy. Odborný dokument je vysoko ambiciózny, pričom je zrejmé, že ochranné mechanizmy sú v ňom menej zdôraznené v porovnaní so smernicami 2019/1151 a 2025/25. Iniciatívy v dokumente výrazne presahujú rámec týchto smerníc a zostáva otvorené, do akej miery a v akej forme sa podarí nájsť politickú vôľu a konsenzus na ich realizáciu.

Pri predstavení IEC ako riešenia situácie inovačnej krízy Európskej únie, ale nie je možné zabudnúť na predchádzajúce dve (neúspešné) iniciatívy európskeho zákonodarcu s ohľadom na úpravu jednotnej právnej formy európskej súkromnej

⁸⁶ Zaujímavé je, že v akademickej spisbe sa stretáme skôr s negatívnym názorom na potlačenie prítomnosti notára v procese zakladania spoločností. Rovnako je kritizovaný aj aspekt rýchlosti zakladania spoločnosti. Pre kritiku potlačania prítomnosti notára v procese zakladania spoločností pozri bližšie: JAKUPAK, Tina – BREGEŠ, Željka: Digitalization: balance and protection – state-of-the-art. In: Intereulaweast, Roč. VII, č. 2 (2020), s. 223, pre kritiku krátenia času zakladania spoločností pozri bližšie: MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 5.

spoločnosti v podobe Nariadenia o európskej súkromnej spoločnosti (Societas Privata Europae, SPE)⁸⁷ a Smernice SUP⁸⁸⁸⁹. Tieto iniciatívy však boli pozastavené v dôsledku významného odporu členských štátov a zainteresovaných spoločenských aktérov.⁹⁰

Je dôležité poznamenať, že cieľom 28. režimu nie je obmedziť sa len na korporáčne právo, ale zahrnúť do zjednocovacieho procesu aj oblasť pracovného, daňového a insolvenčného práva, ktoré budú ale Achillovou pätou takéhoto konceptu regulácie.⁹¹ 28. režim predstavuje mimoriadne ambiciózny zámer, ktorý, s ohľadom na desaťročia prebiehajúcej harmonizácie vo vyššie uvedených oblastiach, bude úspešný predovšetkým v závislosti od politickej vôle, ktorá však môže byť stimulovaná akútnosťou situácie – kríza konkurencieschopnosti Európskej únie v globálnom meradle. Zároveň bude nevyhnutné nájsť rovnováhu medzi inovatívnymi krokmi, flexibilitou 28. režimu a stále sa prehľbujúcou reguláciou AML, transparentnosti a správy skupín spoločností.⁹²

⁸⁷ Návrh Nariadenia o európskej súkromnej spoločnosti (SPE) mal zjednodušiť zakladanie a fungovanie malých a stredných spoločností a podporiť jednotný trh, avšak projekt bol v roku 2014 stiahnutý pre výrazný nesúhlas členských štátov a obavy kritikov, že absencia stropu na veľkosť alebo obrat by umožnila veľkým korporáciám obchádzať národné pracovnoprávne predpisy a ochranu veriteľov. MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 3.

⁸⁸ Návrh smernice Európskeho parlamentu a Rady o spoločnostiach s ručením obmedzeným s jediným spoločníkom /* com/2014/0212 final - 2014/0120 (cod) */.

⁸⁹ Po návrhu Nariadenia o európskej súkromnej spoločnosti bola predložená iniciatíva v podobe Smernice SUP, ktorej cieľom bola harmonizácia existujúcich vnútroštátnych pravidiel bez vytvárania novej európskej právnej formy. Táto forma by umožnila elektronickú registráciu s minimálnym základným kapitálom 1 €. Smernica SUP mala podporiť podnikateľské aktivity, spoluprácu medzi spoločnosťami, rast a zamestnanosť. V roku 2015 Výbor Európskeho parlamentu pre zamestnanosť a sociálne veci odporučil zamietnutie návrhu. Vo svojom stanovisku, prijatom dvoj tretinovou väčšinou, upozornil na riziko, že Smernica SUP by mohla oslabiť pracovnoprávne štandard, znížiť ochranu veriteľov a podporiť tzv. forum-shopping do krajín s priaznivejšími pravidlami. Napokon návrh čelil v Európskom parlamente ďalším kontroverziám a obavám o subsidiaritu, Európska komisia ho oficiálne stiahla v roku 2018. DE GRANDES PASCUAL, Luis: Single-member private limited liability companies (Societas Unius Personae), In "Connected digital single market". Dostupné na: <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-single-member-companies> (cit. 27.09.2025) a MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 4.

⁹⁰ MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 2.

⁹¹ MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 1.

⁹² Požiadavku na transparentnosť skupín spoločností obsahuje aj Smernica 2025/25 (napríklad body 19 a 21 preambuly smernice).

Je zrejmé, že podnikatelia potrebujú flexibilnejšie a rýchlejšie režimy na efektívnu cezhraničnú expanziu. Budúci vývoj, najmä implementácia digitálnych riešení, centralizovaných registrov a jednotnej digitálnej identity, bude preto kľúčová pre úspech iniciatívy 28. režimu a pre celkovú konkurencieschopnosť Európy. Sledovanie a hodnotenie týchto krokov bude nevyhnutné na zabezpečenie rovnováhy medzi inováciou, bezpečnosťou a právnou istotou.⁹³

Zoznam použitej literatúry

1. BITĚ, Virginijus – ROMASHCHENKO, Ivan: Online Formation of Companies in Lithuania in a Comparative Context: Implementation of the Digitalisation Directive and Beyond. In: European Business Organization Law Review, Roč. 24, č. 4 (2023) 24, s. 645–676.
2. CSACH, Kristián: Digital corporate governance in Slovakia. In: Právny obzor, special issue 105 (2022), s. 3-13.
3. DE GRANDES PASCUAL, Luis: Single-member private limited liability companies (Societas Unius Personae), In "Connected digital single market", dostupné na: <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-single-member-companies>.
4. JAKUPAK, Tina – BREGEŠ, Željka: Digitalization: balance and protection – state-of-the-art. In: Intereulaweast, Roč. VII, č. 2 (2020), s. 195-227.
5. LETTA, Enrico: Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens, April 2024, s. 1-146.
6. MAKSIMOVIĆ SEKULIĆ, Nina: The significance of Directive 2019/1151 in the digitalization of European Union company law. In: Pravo - teorija i praksa, Roč. 40, č. 3 (2023), s. 68-80.
7. MRÁZOVÁ, Žofia – CUKEROVÁ, Dominika: How the Digitalisation Has Changed the Slovak Company Law: Implementation of the Directive 2019/1151 (Digitalisation Directive) and What Next? In: EU AND COMPARATIVE LAW ISSUES AND CHALLENGES SERIES (ECLIC), č. 7 (2023), s. 334-360.
8. MEYER-ERDMANN, Marcus - HOFFMANN, Aline: How a 28th company law regime jeopardises workers' rights, European Economic. In: Employment and Social Policy, 2025, s. 1-11.
9. SCHMIDT, Jessica: The Digitalisation Directive II – a Major Expansion and Upgrade of EU Business Registers. In: European Company and Financial Law Review, Roč. 21, č. 5-6 (2024), s. 563–603.

⁹³ Problematika riešená v príspevku sa týka aj mestských podnikov (MOE), ktoré rovnako potrebujú efektívne postupy pri zakladaní spoločností, využitie digitálnych nástrojov a rýchly prístup k spoľahlivým údajom o spoločnostiach v iných členských štátoch.

10. SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. Bratislava: Nakladatelství C.H.Beck-SK, 1. vydanie, 2024. S. 1-144. ISBN: 978-80-8232-050-6.
11. ŠULEKOVÁ, Žofia: Elektronizácia v korporačnom práve. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.): Právo, obchod, ekonomika VI. Košice: Univerzita P. J. Šafárika v Košiciach, 2016, s. 551-559.
12. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, A Competitiveness Compass for the EU, Brussels, 29.1.2025 COM(2025) 30 final.
13. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The EU Startup and Scaleup Strategy, Choose Europe to start and scale, Brussels, 28.5.2025 COM(2025) 270 final.
14. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The Single Market: our European home market in an uncertain world, A Strategy for making the Single Market simple, seamless and strong, Brussels, 21.5.2025, COM(2025) 500 final.
15. 28. režim – právny rámec EÚ pre podniky, dostupné na: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU_sk.
16. The future of European competitiveness, Luxembourg: Publications Office of the European Union, 2025, s. 1-70, ISBN 978-92-68-22715-2 doi:10.2872/9356120 ES-01-24-000-EN-N.
17. Smernica Európskeho parlamentu a Rady (EÚ) 2019/1151 z 20. júna 2019, ktorou sa mení smernica (EÚ) 2017/1132, pokiaľ ide o používanie digitálnych nástrojov a postupov v rámci práva obchodných spoločností
18. Smernica Európskeho parlamentu a Rady (EÚ) 2025/25 z 19. decembra 2024, ktorou sa menia smernice 2009/102/ES a (EÚ) 2017/1132, pokiaľ ide o ďalšie rozšírenie a zdokonalenie využívania digitálnych nástrojov a postupov v oblasti práva obchodných spoločností.
19. Simplification of registration of companies in the 28th Regime, Towards a single digital company register, Policy Department for Justice, Civil Liberties and Institutional Affairs Directorate-General for Citizens' Rights, Justice and Institutional Affairs PE 776.000 - July 2025.
20. Company law and corporate governance EU rules and activity in this area, Informal Company Law Expert Group, action plan on company law and corporate

governance, https://commission.europa.eu/business-economy-euro/doing-business-eu/company-law-and-corporate-governance_en.

21. Revision of Directive 2019/1151/EU on digital tools and processes in company law, PE 740.247 – April 2023.
22. The Informal Company Law Expert Group (ICLEG), Report on digitalisation in company law, March 2016.
23. Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Digitalizácia justície v Európskej únii – súbor príležitostí, COM/2020/710 final.
24. Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob, COM(2021) 118 final.
25. Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Stratégia pre MSP pre udržateľnú a digitálnu Európu, COM/2020/103 final.
26. Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov, Aktualizácia novej priemyselnej stratégie na rok 2020: budovanie silnejšieho jednotného trhu pre obnovu Európy, COM/2021/350 final.
27. Návrh smernice Európskeho parlamentu a Rady o spoločnostiach s ručením obmedzeným s jediným spoločníkom /* com/2014/0212 final - 2014/0120 (cod) */.

Kontaktné údaje

JUDr. Barbora Grambličková, PhD. LL.M.

barbora.czokolyova@uniba.sk

Katedra obchodného práva a hospodárskeho práva, Právnická fakulta Univerzity Komenského v Bratislave

LEGAL CHALLENGES OF USING AI IN BUSINESS: LIABILITY AND REGULATION¹

Jana Pezlar Selecká²

Abstract: This paper examines the practical use of artificial intelligence (AI) in business and the related legal challenges. It focuses primarily on issues of liability and regulation in the context of the European Union's new Artificial Intelligence Act (AI Act). AI is commonly used for process automation, data analysis, and decision-making, but current legislation does not adequately address the new risks. Key issues include unclear allocation of liability among developers, deployers, and users of AI systems, as well as the low explainability of so-called black-box algorithms. The aim of this paper is to identify these legal gaps and propose solutions to improve legal certainty for businesses and enhance the practical application of the AI Act. The main genesis of the article is the fact that AI is not a perfect or infallible technology, and no developer can guarantee its absolute reliability. This inherent imperfection underscores the importance of law in setting clear and predictable liability rules.

Key words: Artificial Intelligence, business, liability, regulation

Introduction

In recent years, the European Union has increasingly emphasized the digitalization of businesses, recognizing it as a key driver of competitiveness and innovation. A central instrument of this transformation is the Digital Europe Plan³, which outlines strategic measures to foster digital adoption across all sectors. Within this framework, particular focus is placed on supporting the integration of artificial intelligence (therefore referred as AI) systems into small and medium-sized enterprises. While this process offers significant opportunities for efficiency and growth, it also raises complex legal questions, particularly regarding liability and regulation.

AI is not a perfect or infallible technology, and no developer can guarantee its absolute reliability. Unlike conventional software, AI systems often function as "*black*

¹ This work was supported by the Slovak Research and Development Agency under the Contract no. APVV-21-0336.

² Department of Commercial Law and Financial Law, Faculty of Law, Pavol Jozef Šafárik University in Košice.

³ European Commission. The Digital Europe Plan. Available: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme> [Accessed: 20.9.2025].

boxes”,⁴ generating outputs in ways that may be useful yet not always fully explainable or free from error. This inherent imperfection underscores the importance of law in setting clear and predictable liability rules. If businesses and professionals are expected to rely on AI systems, they must be able to do so within a framework that allocates accountability in a transparent and foreseeable manner.

The introduction of AI into business operations challenges traditional legal frameworks that were not designed with such an autonomous and data-driven technologies in mind. Unlike conventional tools, AI systems can generate outcomes in ways that are often unpredictable and not directly attributable to human decision-making. This raises a fundamental question: who should bear liability when an AI-driven system causes harm, financial loss, or a breach of rights? The allocation of responsibility among developers, suppliers, and users of AI remains uncertain, creating significant gaps in legal certainty. Addressing these gaps is essential not only for protecting affected parties, but also for building trust and ensuring the sustainable adoption of AI in the business environment.

A practical illustration of this challenge can be seen in the legal profession. Imagine a lawyer who uses an AI system to generate contracts. If the AI produces an incorrect output and the lawyer fails to thoroughly review it before presenting it to the client, the responsibility formally lies with the lawyer. However, this scenario exposes a deeper legal dilemma: although the lawyer is liable towards the client, the actual error originated in the AI system. This raises a pressing question: *„how should liability be allocated when the AI system itself, rather than the human professional, is the direct source of the mistake?“* Moreover, if the flawed AI output results in financial loss or damage to the lawyer, the issue of whether and how such harm can be recovered becomes crucial.

These challenges highlight the broader problem of integrating AI into business contexts without sufficient legal safeguards. While the European Union has responded by adopting the **Artificial Intelligence Act**⁵ (therefore referred as **AI Act**) as the first comprehensive regulatory framework for AI, the AI Act still leaves many questions unresolved, particularly in the domain of the liability. Businesses need clear and predictable rules on accountability to minimize risks, avoid legal uncertainty, and foster innovation in a responsible manner.

The purpose of this paper is to identify the key challenges associated with regulating artificial intelligence, to analyse the current state of the art in addressing AI liability within the EU legal framework, and to formulate informed opinions on possible

⁴ ALMADA, M. Technical AI Transparency: A Legal View of the Black Box. In: *IEEE*. 2021, p. 1. Available: <https://ssrn.com/abstract=5096913>. [Accessed: 20.9.2025]

⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Available: <https://artificialintelligenceact.eu/ai-act-explorer/>

solutions. In its conclusion, the paper outlines the next steps that should be taken to ensure a more coherent and predictable framework for AI liability, thereby enhancing both legal certainty and responsible innovation.

Artificial Intelligence as a challenge for regulators?

Artificial intelligence represents a fundamentally different category of technology compared to traditional digital tools. Unlike conventional software, which produces predictable results by following fixed instructions, AI systems can autonomously learn, adapt, and generate outputs unforeseen by their developers.⁶ While this capacity for self-improvement makes AI highly valuable in business processes, it simultaneously raises legal and ethical dilemmas, particularly in the allocation of liability.

This section will examine three major challenges associated with AI systems: opacity, unpredictability and autonomy, which represent the core legal and technical issues of AI liability.

The **opacity** of AI systems often described as the "*black box effect*", has already been mentioned in the introduction to this paper. It is necessary to return to this concept here, as it represents one of the central challenges in regulating artificial intelligence. From a technical perspective, opacity in AI derives primarily from the complexity of its models and the scale of data processing they require. Deep neural networks, for example, function as black boxes: their multilayered architectures and billions of parameters make their reasoning processes impenetrable, even to their developers. Such opacity undermines the ability to assign liability with certainty.⁷ As academic Cheong observes, such technical opacity is not merely an engineering challenge but one with direct legal and ethical consequences, as it undermines transparency, complicates accountability, and limits the capacity of regulators and users to evaluate whether AI outputs are fair, lawful, or reliable.⁸

The opacity of AI systems has not only been recognized in academic discourse but also by judicial authorities. The Slovak Constitutional Court ruled that the use of

⁶ BARAISHUK, D. What is Artificial Intelligence? AI vs Traditional Software. In BELITSOFT. 2024. [Online]. Available: <https://belitsoft.com/ai-development/artificial-intelligence-vs-conventional-software> [Accessed: 20.09.2025.]

⁷ IP, Si Hua Robert. Research on Explainability of Deep Neural Networks and Its Applications. In: Highlights in Science, Engineering and Technology – MMADP 2024 [online]. Volume 115, 2024, s. 441. Available at:

https://www.researchgate.net/publication/385501754_Research_on_Explainability_of_Deep_Neural_Networks_and_Its_Applications [Accessed: 21.09.2025.]

⁸ CHEONG, B., CH. Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. In: Frontiers in Human Dynamics [online]. 2024, Vol.2. Available at: <https://www.frontiersin.org/articles/10.3389/fhumd.2024.1421273/full> [Accessed: 21.09.2025.]

machine learning systems in tax administration must be accompanied by ex-ante and ex-post measures to ensure the protection of fundamental rights, notably access to the criteria and logic guiding a decision.⁹ Although the case concerned tax administration, its reasoning resonates broadly: legal systems must guard against automated decision-making processes that are "*inexplicable, unreviewable, and unaccountable*." This principle directly supports the argument for predictable liability frameworks in the AI context.

Another core challenge in regulating artificial intelligence is **unpredictability**. Unlike conventional digital tools, AI systems may generate outputs or behave in ways that are unforeseen even by their developers. This unpredictability stems from several factors: the complexity of machine learning algorithms, the reliance on large and often imperfect datasets, and the adaptive nature of models that evolve with new inputs. As a result, AI may produce outcomes that are not only unexpected but also difficult to reconstruct or explain afterwards.¹⁰

The legal implications of such unpredictability are profound. Traditional liability regimes presume that products or tools function in a foreseeable manner and that errors can be traced back to design defects, negligent use, or faulty data. However, when AI systems act in ways that exceed their programmed parameters, responsibility becomes more difficult to assign. As an example from real world, we refer to well-known Flash Crash¹¹ of May 6, 2010, when algorithmic and high-frequency trading systems interacted in unpredictable ways and triggered a collapse and rapid recovery of U.S. equity markets. The event revealed how autonomous algorithmic decision-making can create systemic risks beyond the anticipation of developers or regulators, raising difficult questions of accountability in highly automated environments.

A third major challenge associated with AI is its **autonomy**. Unlike traditional digital tools, which operate only under direct human control, many AI systems can make decisions and acting without continuous supervision. As systems gain autonomy, they not only execute tasks but also adapt strategies, interact with complex environments, and generate outcomes that were not explicitly foreseen by their developers. This raises a profound regulatory dilemma: legal doctrines of liability

⁹ Slovakian Constitutional Court, PL. ÚS 25/2019-117. [Online]. Available: <https://www.slovlex.sk/pravnepredpisy/SK/ZZ/2021/492/20211217> [Accessed: 20.09.2025.]

¹⁰ D'AMOUR, A. Et al. Inderspecification Presents Challenges for Credibility in Modern Machine Learning. In Journal of Machine Learning Research [online]. 2022. Available: <https://www.jmlr.org/papers/v23/20-1335.html> [Accessed: 21.09.2025.]

¹¹ KIRILENKO, A.: The Flash Crash: High-Frequency Trading in an Electronic Market. In The Journal of Finance [online]. 2017, Vol. 72. Available at: <https://onlinelibrary.wiley.com/doi/10.1111/jofi.12498> [Accessed: 21.09.2025.]

have historically been built upon human control, intention, and foreseeability, whereas autonomous AI systems increasingly operate beyond those assumptions. The problem of autonomy is particularly visible in high-risk domains. In medicine, for example, autonomous diagnostic or robotic systems may take decisions with limited or no human oversight creating uncertainty over who should be liable if harm occurs.¹² The more autonomy AI systems acquire, the more existing frameworks struggle to provide clear rules for accountability.¹³

In scholarly and policy debates, several recurring proposals emerge for addressing the liability implications of autonomous AI. The most common approach is to differentiate between levels of autonomy, with liability frameworks adjusted according to whether systems operate under close human supervision or with significant independence.¹⁴ Another frequently discussed solution is the preservation of human oversight through mechanisms such as “human-in-the-loop” or “human-on-the-loop,” which are seen as essential to maintaining a continuous chain of accountability.¹⁵ Some scholars take a more radical stance, proposing that highly autonomous systems should be granted a distinct legal status, accompanied by sui generis liability regimes. This theme is closely linked to debates on the **personhood of AI**.¹⁶ While consensus on the optimal solution has yet to be reached, these recurring themes reflect a shared recognition that the autonomy of AI systems requires a fundamental rethinking of how responsibility should be allocated in law. In the following parts of this paper, particular attention will be given to the European Union’s approach to these challenges, as embodied in the AI Act and related legislative initiatives.

¹² SAENZ, A. D. Autonomous AI systems in medicine: Liability, regulation, risks. In: *npj Digital Medicine* [online]. 2023, Vol. 6, No. 1, 118. Available at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10558567/> [Accessed: 21.09.2025.]

¹³ BUITEN, Miriam C. The law and economics of AI liability. In: *Computer Law & Security Review* [online]. 2023, Vol. 48, 105779. Available at: <https://www.sciencedirect.com/science/article/pii/S0267364923000055> [Accessed: 21.09.2025.]

¹⁴ SHRESTHA, Sahara. Nature, nurture, or neither?: Liability for automated and autonomous artificial intelligence torts based on human design and influences [online]. *George Mason Law Review*, 2021, 29(1). Available from: https://lawreview.gmu.edu/print_issues/nature-nurture-or-neither-liability-for-automated-and-autonomous-artificial-intelligence-torts-based-on-human-design-and-influences/ [Accessed: 21.09.2025.]

¹⁵ CHIODO, Sergio, Paolo FELLI, Davide GROSSI and Nick TINNEMEIER. Formalising Human-in-the-Loop: Computational Reductions, Failure Modes, and Legal-Moral Responsibility [online]. arXiv, 2025. Available from: <https://doi.org/10.48550/arXiv.2505.10426> [Accessed: 21.09.2025.]

¹⁶ SCHERER, Matthew U. Of wild beasts and digital analogues: the legal status of autonomous systems. *Nev. LJ*, [online] 2018, 19: 259. Available from: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nevlj19&div=9&id=&page=> [Accessed: 21.09.2025.]

From Regulation to Responsibility: The EU's Approach through the AI Act, the Product Liability Directive, and the AI Liability Directive

Having outlined the core challenges of opacity, unpredictability, and autonomy, it becomes clear that traditional liability doctrines are not well-adapted to address the risks posed by artificial intelligence. To mitigate these gaps, the European Union has advanced a multifaceted regulatory response. Three instruments stand out as central pillars of this framework: the **AI Act**,¹⁷ which sets harmonized rules for the development and deployment of AI systems; the **revised Product Liability Directive**¹⁸ (therefore referred as **PLD**), which adapts strict liability rules for defective products to the context of AI; and the **proposed AI Liability Directive**¹⁹ (therefore referred as **AILD**), which facilitates the enforcement of claims by easing the burden of proof in cases involving AI. Together, these initiatives represent the EU's most comprehensive attempt to balance innovation with accountability in the governance of artificial intelligence.

The AI Act represents the world's first comprehensive horizontal framework for regulating artificial intelligence.²⁰ Unlike liability regimes that operate ex post, after harm has already occurred, the AI Act is primarily a preventive instrument. Its central purpose is to reduce risks associated with AI through ex-ante control mechanisms that govern design, development, and deployment before AI systems reach the market.²¹

At the heart of the Act lies its risk-based approach. AI systems are classified according to the risks. They are distinguished to four categories of risks as following:

¹⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2019/2144 and (EU) 2019/216 [online]. In EUR-Lex. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> [Accessed: 25.09.2025.]

¹⁸ Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. In EUR-Lex. Available at: <https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng> [Accessed: 25.09.2025.]

¹⁹ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) In EUR-Lex. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496> [Accessed: 25.09.2025.]

²⁰ BUSCH, Felix, et al. Navigating the European Union Artificial Intelligence Act for Healthcare. npj Digital Medicine [online]. 2024, 7(1). ISSN 2398-6352. Available from: doi:10.1038/s41746-024-01213-6 [Accessed: 25.09.2025.]

²¹ KRETSCHMER, Martin, et al. The risks of risk-based AI regulation: taking liability seriously. SSRN Electronic Journal [online]. 2023. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4622405 [accessed: 25.09.2025].

unacceptable, high, limited, or minimal.²² Unacceptable-risk systems, such as those enabling social scoring by governments, are outright prohibited (Article 5 (1) (c)). High-risk systems, which include applications in areas such as healthcare, education, employment, and critical infrastructure, are subject to extensive obligations designed to ensure safety and trustworthiness (Article 6). These obligations include requirements for data quality, documentation and record-keeping, human oversight, and robustness and accuracy of the system (Article 8-15).

Crucially, the AI Act requires high-risk AI systems to undergo **conformity assessments** prior to being placed on the market. These assessments function as a gatekeeping mechanism: providers must demonstrate compliance with the Act's requirements before deployment (Article 43-51). Moreover, once an AI system is deployed, the Act mandates **post-market monitoring and incident reporting**, creating a continuous feedback loop to identify risks that may not have been foreseen at the development stage (Article 61, 62, 65).

This preventive character is intended to complement, rather than replace, traditional liability regimes. By establishing clear rules before harm occurs, the AI Act aims to enhance legal certainty and foster trust in AI adoption, particularly in business contexts.²³

While the AI Act represents a milestone in regulating artificial intelligence, its preventive orientation underscores the need for complementary instruments.

Whereas the AI Act focuses on ex-ante prevention, **the AILD** was designed to complement it by addressing **ex-post liability**. Proposed in September 2022, the Directive sought to ease the path for victims of harm caused by AI systems by lowering evidentiary hurdles in civil proceedings. Its core innovation lies in facilitating redress rather than creating new liability regimes.²⁴

The Directive introduced two central mechanisms. First, it proposed a **presumption of causality**, allowing courts to infer a causal link between an AI system's output and the damage suffered, provided that the claimant could show a fault on the part of the provider or user. Second, it created **disclosure obligations**, granting victims the right to request access to information about high-risk AI systems from providers and users

²² EBERS, M. Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. *European Journal of Risk Regulation* [online]. 2024, 1–20. ISSN 2190-8249. Available from: doi:10.1017/err.2024.78 [accessed: 27.09.2025].

²³ BOTERO ARCILA, B. AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review* [online]. 2024, 54, 106012. ISSN 0267-3649. Available from: doi:10.1016/j.clsr.2024.106012 [accessed: 27.09.2025].

²⁴ ZIOSI, M. et al. The EU AI Liability Directive (AILD): Bridging Information Gaps. *SSRN Electronic Journal* [online]. 2023. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4470725 [accessed: 27.09.2025]

in order to substantiate their claims.²⁵ These mechanisms were intended to mitigate the “black box” problem by counterbalancing the informational asymmetry between victims and AI developers.

Despite its innovative character, the AILD soon encountered political obstacles. At the **AI Summit in Paris** several Member States expressed reluctance to adopt additional liability legislation alongside the AI Act, arguing that existing instruments such as the revised Product Liability Directive would be sufficient. As a result, the AILD lost political momentum and is no longer regarded as a priority within the EU’s legislative agenda.²⁶

The revised PLD, adopted in 2024, represents the EU’s effort to modernize strict liability rules for defective products in light of digitalization and artificial intelligence. Unlike the AI Act, which operates preventively, and the AILD, which aimed to facilitate procedural access, the PLD directly addresses the **substantive allocation of liability** once harm has occurred.

The Directive broadens the concept of “product” to explicitly cover **software, digital updates, and AI systems**, thereby eliminating earlier uncertainty about whether intangible digital products fall within the liability regime.²⁷ Importantly, it extends liability beyond traditional manufacturers to include **developers, deployers, and providers of software updates**, reflecting the interconnected nature of AI ecosystems. By doing so, the PLD establishes a framework of **shared liability**, where multiple actors in the AI value chain may be held accountable for defects that cause harm.²⁸

A key innovation lies in the treatment of updates and digital services. If harm results from a faulty update or a failure to provide necessary updates, the entity responsible for those updates can be held strictly liable.²⁹ Similarly, providers of AI components that are later integrated into larger systems may also bear liability where their contribution caused or contributed to the defect.³⁰ This reflects a recognition that responsibility in AI cannot always be traced to a single actor but often emerges from the combined actions of several parties.

²⁵ HACKER, P. The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future. SSRN Electronic Journal [online]. 2022. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4279796 [accessed: 27.09. 2025].

²⁶ SOLÁROVÁ, S., HARGAŠ, J. Samit v Paríži odštartoval preteky o to, kto umelej inteligencii dovoli viac. In: *Denník N* [online]. 22. 2. 2024. Available at: <https://dennikn.sk/4481538/samit-v-parizi-odstartoval-preteky-o-to-kto-umelej-inteligencii-dovoli-viac/> [accessed: 27.09. 2025].

²⁷ Article 4 (1). PLD.

²⁸ Article 12. PLD.

²⁹ Article 10. PLD.

³⁰ Recital 24. PLD.

By embracing shared liability, the PLD attempts to balance victim protection with innovation. Victims are ensured a clear path to compensation without having to prove negligence, while businesses face predictable rules that distribute responsibility across the supply chain. However, this also raises questions about how liability will be apportioned in practice among different actors, particularly in cross-border contexts where AI systems are developed, trained, and deployed across multiple jurisdictions.

The PLD thus complements the AI Act's preventive measures and fills the substantive gap left by the stopped AILD. Together, these instruments demonstrate the EU's layered approach: ex-ante prevention (AI Act) and substantive strict liability (PLD). Yet, whether this architecture will deliver coherent and effective outcomes remains subject to ongoing debate.

Conclusion

AI for sure, presents unique legal challenge that traditional liability frameworks were not designed to address. This paper has highlighted three central issues **opacity, unpredictability, and autonomy** which complicate the allocation of responsibility and undermine legal certainty. In response, the European Union has constructed a layered framework combining **ex-ante preventive regulation** (AI Act) and **substantive strict liability** (PLD) for now.

While this architecture is ambitious, its practical application remains uncertain. The AI Act's preventive obligations may reduce risks yet cannot eliminate the possibility of harm. The AILD, intended to lower evidentiary burdens, has lost political momentum, leaving a gap in procedural protection. The PLD offers victims strict liability and introduces shared responsibility across the AI value chain, but translating these rules into concrete judicial practice will be highly complex. Courts will need to determine how liability should be apportioned among developers, deployers, and other actors when harm results from the combined functioning of opaque and adaptive systems.

Thus, the central challenge ahead is not only legislative design but also **judicial interpretation and enforcement**. The substantive allocation of liability in the context of AI will be tested in litigation, and its contours will depend on how courts balance innovation, accountability, and victim protection. As these cases emerge in the near future, they will determine whether the EU's framework can truly provide legal certainty while enabling responsible AI-driven innovation.

References

1. ALMADA, M. Technical AI Transparency: A Legal View of the Black Box. In: IEEE. 2021, p. 1-8. Available: <https://ssrn.com/abstract=5096913>

2. BARAISHUK, D. What is Artificial Intelligence? AI vs Traditional Software. In BELITSOFT. 2024. [Online]. Available: <https://belitsoft.com/ai-development/artificial-intelligence-vs-conventional-software>
3. BOTERO ARCILA, B. AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? Computer Law & Security Review [online]. 2024, 54, 106012. ISSN 0267-3649. Available from: doi:10.1016/j.clsr.2024.106012
4. BUITEN, Miriam C. The law and economics of AI liability. In: Computer Law & Security Review [online]. 2023, Vol. 48, 105779. Available at: <https://www.sciencedirect.com/science/article/pii/S0267364923000055>
5. BUSCH, F. et al. Navigating the European Union Artificial Intelligence Act for Healthcare. npj Digital Medicine [online]. 2024, 7(1). ISSN 2398-6352. Available from: doi:10.1038/s41746-024-01213-6 [viewed 27 September 2025]
6. CHEONG, B., CH. Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. In: Frontiers in Human Dynamics [online]. 2024, Vol.2. Available at: <https://www.frontiersin.org/articles/10.3389/fhumd.2024.1421273/full>
7. CHIODO, M. Et al. Formalising Human-in-the-Loop: Computational Reductions, Failure Modes, and Legal-Moral Responsibility [online]. arXiv, 2025. Available from: <https://doi.org/10.48550/arXiv.2505.10426>
8. D'AMOUR, A. Et al. Inderspecification Presents Challenges for Credibility in Modern Machine Learning. In Journal of Machine Learning Research [online]. 2022. Available: <https://www.jmlr.org/papers/v23/20-1335.html>
9. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. In EUR-Lex. Available at: <https://eur-lex.europa.eu/eli/dir/2024/2853/oj/jeng>
10. EBERS, M. Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. European Journal of Risk Regulation [online]. 2024, 1–20. ISSN 2190-8249. Available from: doi:10.1017/err.2024.78
11. European Commission. The Digital Europe Plan. Available: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>
12. HACKER, P. The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future. SSRN Electronic Journal [online]. 2022. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4279796
13. IP, Si Hua Robert. Research on Explainability of Deep Neural Networks and Its Applications. In: Highlights in Science, Engineering and Technology – MMADP 2024. Volume 115, 2024, s. 441. Available at: https://www.researchgate.net/publication/385501754_Research_on_Explainability_of_Deep_Neural_Networks_and_Its_Applications

14. KIRILENKO, A.: The Flash Crash: High-Frequency Trading in an Electronic Market. In *The Journal of Finance* [online]. 2017, Vol. 72. Available at: <https://onlinelibrary.wiley.com/doi/10.1111/jofi.12498>
15. KRETSCHMER, M. et al. The risks of risk-based AI regulation: taking liability seriously. *SSRN Electronic Journal* [online]. 2023. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4622405
16. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) In *EUR-Lex*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496>
17. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2019/2144 and (EU) 2019/216 [online]. In *EUR-Lex*. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>
18. SAENZ, A. D. Autonomous AI systems in medicine: Liability, regulation, risks. In: *npj Digital Medicine* [online]. 2023, Vol. 6, No. 1, 118. Available at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10558567/>
19. SCHERER, Matthew U. Of wild beasts and digital analogues: the legal status of autonomous systems. *Nev. LJ*, [online] 2018, 19: 259. Available from: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nevlj19&div=9&id=&page=>
20. SHRESTHA, S. Nature, nurture, or neither?: Liability for automated and autonomous artificial intelligence torts based on human design and influences [online]. *George Mason Law Review*, 2021, 29(1). Available from: https://lawreview.gmu.edu/print_issues/nature-nurture-or-neither-liability-for-automated-and-autonomous-artificial-intelligence-torts-based-on-human-design-and-influences/
21. Slovakian Constitutional Court, PL. ÚS 25/2019-117. [Online]. Available: <https://www.slov-lex.sk/pravnepredpisy/SK/ZZ/2021/492/20211217>
22. SOLAROVÁ, S., HARGAŠ, J. Samit v Paríži odštartoval preteky o to, kto umelej inteligencii dovolí viac. In: *Denník N* [online]. 22. 2. 2024. Available at: <https://dennikn.sk/4481538/samit-v-parizi-odstartoval-preteky-o-to-kto-umelej-inteligencii-dovoli-viac/>
23. ZIOSI, Marta, et al. The EU AI Liability Directive (AILD): Bridging Information Gaps. *SSRN Electronic Journal* [online]. ISSN 1556-5068. Available from: doi:10.2139/ssrn.4470725

Contact details

Mgr. Jana Pezlar Selecká

jana.selecka@student.upjs.sk

Department of Commercial and Financial Law, Faculty of Law, Pavol Jozef Šafarik
University in Košice.

UMELÁ INTELIGENCIA, SMART KONTRAKTY A ICH VPLYV NA FIDUCIÁRNE POVINNOSTI KONATEĽA

ARTIFICIAL INTELLIGENCE, SMART CONTRACTS AND THEIR IMPACT ON A DIRECTOR'S FIDUCIARY DUTIES

Peter Šikulínek¹

Abstrakt: Príspevok sa zameriava na vplyv digitalizácie na plnenie fiduciárnych povinností konateľa podľa slovenského práva, so špecifickým dôrazom na využívanie umelej inteligencie a smart kontraktov. Cieľom je preskúmať, do akej miery tieto technológie podporujú alebo zasahujú do výkonu funkcie konateľa a plnení povinností odbornej starostlivosti a lojality. Zistenia poukazujú na riziká spojené s používaním AI nástrojov, medzi ktoré patrí porušenie povinnosti mlčanlivosti pri práci s dôvernými informáciami, efekt „black box“ pri strojovom učení a obmedzené možnosti verifikácie výstupov. Upozorňuje sa na potrebu algoritmickej transparentnosti, kontrolných mechanizmov a porovnania výstupov s inými zdrojmi. V prípade smart kontraktov sa zdôrazňuje ich prínos pre efektívnosť a transparentnosť, ale aj riziká vyplývajúce z chýb kódu, nespoľahlivých oracles a rigidity automatizovaného vykonania. Príspevok uzatvára, že digitalizácia nemení rozsah fiduciárnych povinností, ale pridáva nový rozmer ich výkonu spojený s kontrolou a riadením technológií konateľom. Prínosmi práce sú najmä identifikácia hraníc a podmienok zodpovedného využívania umelej inteligencie a smart kontraktov a formulácia odporúčaní pre vnútropodnikovú reguláciu a korporečnú prax.

Kľúčové slová: umelá inteligencia, smart kontrakty, konateľ

Abstract: The paper focuses on the impact of digitalisation on the performance of directors' fiduciary duties under Slovak law, with a specific emphasis on the use of artificial intelligence and smart contracts. Its aim is to examine to what extent these technologies support or interfere with the exercise of directors' functions and the fulfilment of their duties of care and loyalty. The findings highlight the risks associated with the use of AI tools, including breaches of confidentiality when handling sensitive information, the "black box" effect in

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra obchodného práva a hospodárskeho práva

machine learning, and the limited possibilities of output verification. The paper stresses the need for algorithmic transparency, control mechanisms, and comparison of AI outputs with other sources. As regards smart contracts, it underlines their contribution to efficiency and transparency, but also the risks stemming from coding errors, unreliable oracles, and the rigidity of automated execution. The paper concludes that digitalisation does not alter the scope of fiduciary duties, but adds a new dimension to their performance, linked to directors' responsibility for controlling and managing technologies. The contribution of the paper lies primarily in identifying the limits and conditions of responsible use of artificial intelligence and smart contracts, and in formulating recommendations for internal regulation and corporate practice.

Key words: artificial intelligence, smart contracts, director

Úvod

Digitalizácia a digitálna transformácia podnikateľského prostredia už nejaký čas predstavujú jednu z najzásadnejších premien podnikateľského prostredia. Pre obchodné spoločnosti to neznamena len zavádzanie nových digitálnych technológií (digitalizácia), ale aj stanovenie strednodobých a dlhodobých cieľov na dosiahnutie digitálnej transformácie spoločnosti.

Digitálna transformácia je na rozdiel od digitalizácie komplexný a systematický proces, ktorý predstavuje zásadnú zmenu organizačnej štruktúry, procesov, funkcií a obchodných modelov spoločnosti v dôsledku zavádzania digitálnych technológií, ako sú Internet vecí (IoT), umelá inteligencia (AI), strojové učenie či rozšírená realita. Digitálna transformácia tak presahuje bežnú digitalizáciu, pretože zahŕňa nielen jednotlivé zavádzanie digitálnych nástrojov, ale aj zásadné zmeny v organizačnej kultúre, vzťahoch so stakeholdermi a podnikateľskej stratégii. Zavedenie digitálnych technológií umožňuje spoločnostiam optimalizovať vnútorné procesy, efektívnejšie alokovať zdroje a vytvárať viac výkonné obchodné modely.²

Pokiaľ ide o ekonomicko-strategický rozmer, digitalizácia je priamo spojená s dlhodobou konkurencieschopnosťou spoločnosti, vzhľadom na čo viac a viac spoločností investuje do rozvoja digitálnych zručností členov orgánov a zamestnancov na všetkých úrovniach, napríklad prostredníctvom školení a workshopov, podpory ďalšieho vzdelávania a celkovo vytvárania „digitálnej kultúry“ v spoločnosti.³ Štatutárne orgány by mali zobrať do úvahy, že na naplnenie cieľov

² REIS, João – MELÃO Nuno: Digital transformation: A meta-review and guidelines for future research. In: Heliyon, Roč. 9., č. 7 (2023), s.3.

³ ZHANG, Yaxin – JIN, Shanyue: How Does Digital Transformation Increase Corporate Sustainability? The Moderating Role of Top Management Teams. In: Systems, Roč. 11, č. 7 (2023), s. 355.

digitalizácie, resp. digitálnej transformácie je prínosné, aby mali aspoň všeobecné technologické znalosti a využili ich v rámci obchodného vedenia a v rozhodovacích procesoch, prípadne využili externého poradcu.

Z pohľadu teórií strategického riadenia sa digitalizácia naprieč rôznymi sektormi trhu čoraz častejšie vníma ako kľúčový zdroj konkurenčnej výhody a „*konkurenčná výhoda spoločnosti je silne ovplyvnená jej digitálnou obchodnou stratégiou, ktorú reprezentujú organizačné a manažérske zručnosti, prevádzkové schopnosti, IT zručnosti a schopnosti elektronickej spolupráce.*“⁴ Podľa teórie zdrojov môže spoločnosť dosahovať lepšie výsledky a konkurenčnú výhodu tým, že disponuje a efektívne využíva zdroje, ktoré sú vzácne, jedinečné a ťažko nahraditeľné⁵. S rýchlym rozvojom digitálnych technológií sú nimi práve digitálne zdroje, pričom adaptívne rozhodovanie štatutárnych orgánov a digitalizácia v rámci spoločností umožňuje podnikom rýchlo reagovať na zmeny trhu a rozvoj technológií. Adaptívne rozhodovanie štatutárnych orgánov umožňuje spoločnosti prispôbiť sa situácii na trhu a využiť nové príležitosti, na druhú stranu „*efektivita silných dynamických schopností môže byť ohrozená zlým strategickým vedením a slabou stratégiou.*“⁶

Štatutár musí k digitalizácii a digitálnej transformácii pristupovať v súlade s povinnosťou starostlivosti a lojality, predovšetkým konať na informovanom základe, neporušiť mlčanlivosť, posúdiť špecifiká konkrétnej podnikateľskej činnosti spoločnosti, vyhodnotiť postavenie spoločnosti na trhu, či analyzovať riziká implementácie digitálnych nástrojov. Najprv je potrebné vypracovať stratégiu digitálnej transformácie (digitálnu stratégiu) ako súčasť celkovej obchodnej stratégie, stanoviť priority pre digitalizáciu procesov – od účtovníctva, cez manažérske informačné systémy, HR či produkciu a distribúciu. V rámci digitálnej stratégie by mala spoločnosť zohľadniť, ktoré procesy sú neefektívne (ekonomicky, prevádzkovo...) a v prípade potreby ich nahradiť alebo podporiť umelou inteligenciou, automatizovanými nástrojmi alebo inou digitálnou technológiou, posúdiť právne aspekty digitálnej transformácie, napr. v oblasti ochrany osobných údajov, diskriminácie, AML regulácií a podobne. Integrácia digitálnych technológií by mala prebehnúť v kontexte s už existujúcimi procesmi v spoločnosti a štatutárne orgány by mali vedieť „*rozoznať, čo v rámci digitálnej transformácie (DT) ponechať a čo*

⁴ PRIYANTO, Panji – MURWANINGSARI, Etty – AUGUSTINE, Yvonne: Impact Digital Business Strategy on Competitive Advantage in the Banking Sector. In: European Journal of Business Management and Research, Roč. 8, č. 2 (2023), s. 65.

⁵ BARNEY, Jay: Firm Resources and Sustained Competitive Advantage. In: Journal of Management, Roč. 17, č. 1 (1991), s. 116–117.

⁶ TEECE, David J. – PETERAF, Margaret A. – HEATON, Sohvi: Dynamic Capabilities and Organizational Agility: Risk, Uncertainty and Entrepreneurial Management in the Innovation Economy. In: Tuck School of Business Working Paper, č. 2771245 (2016), s. 27.

zmeniť.⁷ Cieľom by tak nemala byť bezpodmienečná plošná digitalizácia v spoločnosti, ale cieľená a systematická digitalizácia v rámci tých procesov, ktoré štatutárny orgán identifikuje ako neefektívne.

Konkurenčné výhody digitálnej transformácie sa premietajú predovšetkým do optimalizácie podnikových procesov. Správne nastavená a implementovaná digitálna stratégia môže „zvýšiť TFP [celkovú faktorovú produktivitu] podnikov. Pomáha podnikom efektívne zbierať a spracovávať informácie, rozširovať ich efektívnosť z hľadiska rozsahu a dosahovať inteligentnú a efektívnu výrobu založenú na údajoch.“⁸ Zvýšenie celkovej faktorovej produktivity (TFP) v praxi znamená, že podnik dokáže z rovnakého množstva zdrojov (práce, kapitálu, materiálu...) vyprodukovať viac, prípadne lepšie produkty a služby.

V tomto kontexte sa digitalizácia stáva nástrojom na efektívnejšie korporačné riadenie ako aj základným predpokladom riadneho a plnenia fiduciárnych povinností⁹ konateľom. To však neplatí absolútne, keďže spôsob a rozsah, v akom budú nástroje digitalizácie implementované v obchodnej spoločnosti závisí od mnohých premenných, ktoré bude na naplnenie požiadaviek pre riadny výkon funkcie konateľa potrebné analyzovať a vyhodnotiť. V ďalších častiach článku bude pozornosť zameraná na dva okruhy nástrojov digitalizácie, a to nástroje využívajúce umelú inteligenciu a smart kontrakty.

Umelá inteligencia v kontexte povinnosti starostlivosti a lojality

Umelá inteligencia (AI) sa rozdeľuje do troch hlavných kategórií na základe jej „kognitívnych“ schopností a úrovne autonómie. Prvou kategóriou je Narrow AI (slabá AI), ktorá je navrhnutá na plnenie jednej špecifickej úlohy s vopred definovaným rozsahom. Tieto systémy, hoci sú vysoko efektívne vo svojej doméne, nedisponujú vedomím ani všeobecným chápaním sveta, čo obmedzuje ich aplikovateľnosť na riešenie komplexných, neznámych problémov. Ďalšou kategóriou je tzv. General AI (všeobecná AI), ktorá na rozdiel od Narrow AI, predstavuje teoretický koncept systému, ktorý by mal schopnosť učiť sa a aplikovať intelektuálne schopnosti na širokú škálu úloh, podobne ako ľudská inteligencia. Tretia a zatiaľ najvyspelejšia hypotetická forma je Super AI (superinteligencia), ktorá by prekonala ľudský mozog v každom intelektuálnom aspekte, vrátane kreativity, logiky a komplexného

⁷ HANELT, André – BOHNSACK, René – MARZ, David – MARANTE, Cláudia Antunes: A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. In: Journal of Management Studies, Roč. 58, č. 5 (2020), s. 1186.

⁸ LI, Na – WANG, Xiaohong – WANG, Zeren – LUAN, Xiangyu: The Impact of Digital Transformation on Corporate Total Factor Productivity. In: Frontiers in Psychology, Roč. 13 (2022), s. 10.

⁹ Povinnosť konateľa vykonávať svoju pôsobnosť s odbornou starostlivosťou a v súlade so záujmami spoločnosti a všetkých jej spoločníkov podľa § 135a ods. 1 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

rozhodovania.¹⁰ Okrem uvedeného členenia existujú aj ďalšie, založené na rôznych kritériách, napr. funkcionalite, učebnom prístupe a pod.

AI nástroje uľahčujú konateľom vykonávať rozhodnutia na silnom informovanom základe, keďže predstavujú rýchlo dostupný zdroj informácií a tieto veľké dáta (big data) dokážu analyzovať. Spracúvanie takéhoto objemu dát je za hranicami kognitívnych schopností konateľa, preto rozhodovanie založené na dátach s podporou umelej inteligencie sa v korporlačnom riadení javí ako nevyhnutné pre udržanie konkurenčnej výhody pred ostatnými súťažiteľmi na trhu a pomáha konateľom proaktívne sa rozhodovať na základe predikcií založených na dátach z minulosti.¹¹ V praxi konateľ napríklad vie v určitej miere predpokladať vývoj relevantného trhu, predikovať cash-flow na základe účtovných podkladov a ďalších vstupov, odhadovať správanie spotrebiteľov, prípadne AI pomôže konateľovi vysvetliť určitú problematiku, ktorej nerozumie atď.

Používanie AI nástrojov má teda viaceré pozitíva. Z pohľadu povinnosti konateľa konať s odbornou starostlivosťou a v súlade so záujmami spoločnosti a spoločníkov je potrebné okrem vyššie uvedených prínosov využívania AI nástrojov spomenúť aj riziká. Najvýraznejšími sú prílišné spoliehanie sa na výstupy z AI systémov (overreliance), zaujatosť (bias), algoritmické chyby alebo bezpečnostné incidenty. Vzťah medzi uvedenými protipólmi je potrebné regulovať v rámci špecifickej interakcie medzi človekom – konateľom a technológiou - AI systémom.

Štatutárne orgány a členovia manažmentu tak „odmietajú úplne preniesť rozhodovaciu právomoc na inteligentné systémy kvôli zostávajúcim problémom s dôverou, hoci si uvedomujú, že ľudské rozhodnutia môžu byť tiež „čiernymi skrinkami“, pretože ľudia robia čiastočne intuitívne rozhodnutia. Namiesto toho manažéri uprednostňujú postupné rozhodovanie AI a človeka, ktoré ponúka predvýber možností podľa definovaných kritérií pre ľudí, dobrú interpretovateľnosť výsledkov vďaka zapojeniu ľudí a veľký súbor alternatívnych možností vďaka zapojeniu AI.“¹²

Pred implementáciou AI nástroju či využitia informácií a výstupov z tohto systému na rozhodovanie musí konateľ zabezpečiť, aby jeho postup bol v súlade s odbornou starostlivosťou, a to najmä v nasledovných oblastiach:

¹⁰ HAQUE, Huda Shireen: Artificial General Intelligence: How Close Are We Really? In: International Journal of Advanced Research in Science, Engineering and Management, Roč. 12, č. 4 (2025), s. 2584–2586.

¹¹ GANGWAR, Roopal – DASH, Bidya – NANDA, Amitabh – AYYUB, Sheenam: Impact of Artificial Intelligence (AI) Enabled Management Information System (MIS) in Managerial Decision Making: An Empirical Study of Leading Business Organisation. In: Journal of Informatics Education and Research, Roč. 4, č. 2 (2024), s. 1326.

¹² IETZMANN, Christian – DUAN, Yanqing: Artificial Intelligence for Managerial Information Processing and Decision-Making in the Era of Information Overload. In: Proceedings of the 55th Hawaii International Conference on System Sciences 2022 (2022), s. 5931.

- (i) *„Zodpovednosť za výber – pri výbere vhodnej technológie AI musí postupovať s odbornou/náležitou starostlivosťou a uskutočniť výber aspoň na takej úrovni, ako by výber uskutočnila iná rozumne starostlivá osoba;*
- (ii) *Zodpovednosť za zadanie, vedenie a súčinnosť – musí vybratej technológii AI zadefinovať zadanie jasne a zrozumiteľne, poskytnúť všetku potrebnú súčinnosť a dávať jej pokyny, resp. informácie/dáta;*
- (iii) *Zodpovednosť za kontrolu – musí byť schopný dodaný výsledok primerane kontrolovať a rozumne vyhodnocovať, a to nielen osobne, ale aj za pomoci riadne nastavených kontrolných mechanizmov.“¹³*

Uvedené demonštruje, že dynamika vzťahu konateľ-AI nástroj musí napriek nespornému prínosu AI reflektovať fiduciárne povinnosti konateľa. Na ilustráciu možno uviesť implementáciu nového softvérového riešenia s použitím umelej inteligencie, ktorej primárnou funkcionalitou bude automatizácia finančných a HR procesov v spoločnosti. V takomto prípade musí konateľ pri výbere dodávateľa AI softvéru preveriť jeho spoľahlivosť, referencie a úroveň zabezpečenia dát. V praxi sú AI softvéry často prispôbené konkrétnym potrebám a situácii spoločnosti. Štatutárny orgán tak má už v rámci predzmluvných rokovaní zásadnú úlohu špecifikovať podmienky vytvorenia AI softvéru a jeho parametre, dodania softvéru a prípadného servisu (maintenance) s ohľadom na záujmy spoločnosti a spoločníkov. Predovšetkým by mal konateľ poskytnúť presné vstupné údaje, ako napríklad štruktúru účtovných kategórií či pravidlá spracovania pracovnoprávných zmlúv, aby nedochádzalo k chybnjej interpretácii. V ostatných prípadoch, ak spoločnosť nadobúda už vytvorený AI softvér, *„členovia štatutárneho orgánu by mali realizovať prieskum trhu s dostupnými systémami a zvoliť ten, ktorý je schopný obstarávať relevantné informácie na určitej uspokojivej úrovni a v čo najväčšej miere zodpovedá požiadavkám konkrétnej obchodnej spoločnosti. Členovia štatutárneho orgánu by mali byť v podstatnej miere informovaní dodávateľom o funkcionalitách a špecifikách nimi zvoleného systému. Zároveň by mali byť upozornení na riziká a prípadné odchýlky či diskrepancie, ktoré môžu vzniknúť činnosťou daného systému.“¹⁴*

Softvér by mal pred nasadením do produkčného prostredia spoločnosti prejsť jednotlivými fázami testovania. Konateľ by nemal byť nečinný a mal by sa aktívne podieľať na danom procese, predovšetkým zúčastniť sa akceptačného testovania a overiť, či AI softvér spĺňa dohodnuté parametre. Následne je potrebné, aby priebežne overoval správnosť výstupov – napríklad pri automaticky generovaných

¹³ PINTÉROVÁ, Dominika: Vplyv súdnych rozhodnutí na doktrínu obchodnoprávných zmlúv v kontexte umelej inteligencie: výzvy a nové horizonty. In: Míľniky práva v stredoeurópskom priestore 2025. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025, s. 986–987. ISBN 978-80-7160-758-8.

¹⁴ SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. 1. vydanie. Bratislava: C. H. Beck, 2024. 88 s. ISBN 978-80-8232-050-6.

finančných reportoch či mzdových výpočtoch alebo platbách kontroloval nastavenie interných kontrolných mechanizmov (napr. dvojitej autentifikácie). Takýmto postupom konateľ v súlade s odbornou starostlivosťou využíva potenciál AI na zníženie nákladov a zefektívnenie procesov v spoločnosti.

Na druhej strane však implementácia AI v širšom kontexte otvára pre konateľa aj viacero otázok spojených s podnikateľským rizikom a obhájiteľnosti jeho konania v rámci zodpovednosti za škodu. Napríklad, pri rozhodovaní o zavedení vyššie ilustrovaného AI softvéru na automatizáciu HR procesov musí konateľ zvážiť náklady a efektivitu: investícia do licencie, implementácie a následný SLA servis môžu predstavovať vysoké vstupné náklady a odhadovaná návratnosť investície (ROI) sa nemusí dostať. Protipólom v rozhodovaní je očakávaný prínos v podobe úspory mzdových nákladov a presmerovanie kapacít zamestnancov na strategickejšie úlohy - čo môže spoločnosti dlhodobu zvýšiť hodnotu. Existuje aj riziko, že zvolený nástroj nebude fungovať podľa očakávaní konateľa (napr. nesprávne spracovanie dát, kybernetické útoky a iné bezpečnostné incidenty), a tým spoločnosti vznikne škoda, najmä ak dôjde k úniku dôležitých aktív, ktoré má spoločnosť v digitálnej podobe (zdrojové, strojové kódy, know-how..).

Ďalšou praktickou výzvou pre konateľa je otázka zaujatosti a nastavenia algoritmu AI, a tým dôveryhodnosti výstupov. Napríklad, ak v ilustrovanom prípade AI softvér navrhne zmenu v HR procesoch, ktorej cieľom je znížiť prevádzkové náklady, zároveň môže vytvoriť riziko diskriminácie uchádzačov o pracovnú pozíciu v spoločnosti na základe niektorého diskriminačného dôvodu. Spoločnosť by bola vystavená riziku antidiskriminačných sporov a v prípade korporácií patriacich do nadnárodných skupín to môže mať aj vnútropodnikové dopady a sankcie za nedodržiavanie interných smerníc spoločnosti.

Konateľ má preto neľahkú úlohu, pretože musí vyhodnotiť viaceré premenné. Ak AI softvér neimplementuje, riskuje, že spoločnosť bude zbytočne znášať vyššie prevádzkové náklady, pričom ak ho implementuje, nesie riziko, že AI zlyhá a spôsobí škodu spoločnosti alebo zasiahne do dobrej povesti spoločnosti. V tomto svetle môže byť aj rozhodnutie konateľa neimplementovať AI riešenie považované za porušenie povinnosti odbornej starostlivosti, ak existovali objektívne dôvody na základe ktorých mohol konateľ očakávať, že technológia by zefektívnila chod spoločnosti a konateľ zároveň dodržal preventívne a kontrolné mechanizmy na limitáciu rizík implementácie AI. Aj tieto aspekty by mal konateľ zohľadniť pri vypracúvaní digitálnej stratégie.

K rozhodovaniu na informovanom základe s použitím AI

Spôsob používania AI nástrojov je veľmi dôležitý v kontexte riadneho plnenia povinností starostlivosti a lojality. V praxi možno pozorovať, že konatelia alebo

zamestnanci vkladajú dôverné informácie či obchodné tajomstvá do bežne dostupných AI systémov (napríklad Gemini, ChatGPT), či už za účelom získania odporúčaní, doplnenia informácií alebo prekladu textov. V takýchto prípadoch konateľ porušuje povinnosť lojality, najmä povinnosť zachovávať mlčanlivosť. Z pohľadu zamestnancov je nevyhnutné, aby konateľ zaviedol primerané organizačné opatrenia na reguláciu používania AI nástrojov. Existujú dokumentované prípady, kedy súkromná komunikácia v rámci AI systému bola omylom prístupná vo verejnom vyhľadávači. Z toho vyplýva, že relevantné nie je len rozhodnutie „či“ AI nástroj použiť, ale aj „ako“ ho využívať bez porušenia právnych povinností. Práve tieto aspekty by mali byť vhodným spôsobom upravené, napríklad v korporačných dokumentoch, interných smerniciach alebo v zmluve o výkone funkcie konateľa. Použitie AI nástroja na získanie informácií a podkladov pre rozhodnutie a spoliehanie sa výlučne na tieto výstupy nenahrádza využitie externého poradcu v prípade, ak konateľ nedisponuje dostatočnými znalosťami alebo informácie nie je schopný spracovať a vyhodnotiť v súlade s jeho povinnosťami¹⁵. Rozdiel medzi získaním informácií z AI nástroja a od externého poradcu spočíva najmä v tom, že pri poradcovi vie konateľ posúdiť jeho odbornosť (referencie, skúsenosti, licencie) a poradca má zároveň právnu subjektivitu a môže byť za svoje konanie zodpovedný. Pri AI nástrojoch (vrátane ChatGPT) je hodnotenie relevancie odpovedí a vyhodnotenie správnosti informácií zložitejšie, pretože tieto systémy nemajú právnu subjektivitu a nemôžu byť zodpovednostným subjektom¹⁶ a zároveň spravidla fungujú ako „čierna skrinka“ (black box).

Problém čiernej skrinky

Pojem „čierna skrinka“ označuje situáciu, kedy umelá inteligencia, spravidla so strojovým učením (machine learning), má vnútorné procesy učenia ale výsledné modely nie sú sčasti alebo vôbec zrozumiteľné pre človeka. Hoci systém generuje konkrétne výstupy na základe vstupných dát, spôsob, akým k nim dospel je nejasný. Nedostatočné vysvetlenie môže mať významný dopad na spoločnosť, keďže konatelia nie sú schopní vykonávať analýzu rizík alebo hrozieb, čo zvyšuje pravdepodobnosť nežiaduceho správania systému.¹⁷ Na vysvetlenie, resp.

¹⁵ CSACH, Kristián: Digital Corporate Governance in Slovakia. In: Právny obzor, Roč. 105, špeciálne číslo (2022), s. 11–12.

¹⁶ PINTÉROVÁ, Dominika: Vplyv súdnych rozhodnutí na doktrínu obchodnoprávných zmlúv v kontexte umelej inteligencie: výzvy a nové horizonty. In: Míľniky práva v stredoeurópskom priestore 2025. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025, s. 984. ISBN 978-80-7160-758-8.

¹⁷ MESKE, Christian – BUNDE, Enrico – SCHNEIDER, Johannes – GERSCH, Martin: Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities. In: Information Systems Management, Roč. 39, č. 1 (2020), s. 53–54.

interpretáciu algoritmu black box AI modelu sa často používajú špeciálne AI modely, ktoré slúžia ako nástroje interpretácie (tzv. „Explainable AI“ alebo „XAI“), ktoré analyzujú vzťah medzi vstupmi a výstupmi pôvodného modelu a identifikujú, ktoré faktory najviac ovplyvnili rozhodnutie, pričom *„tento model by mal byť schopný napodobňovať správanie čiernej skrinky a zároveň by mal byť zrozumiteľný pre ľudí. Inými slovami, interpretovateľný model aproximujúci čiernu skrinku musí byť globálne interpretovateľný“*¹⁸. Vysvetliteľné modely strojového učenia však často neposkytujú úplne presný pohľad na to, ako pôvodný black box model dospel k svojmu rozhodnutiu.¹⁹ To znamená, že konateľ, ktorý by sa spoliehal na takéto vysvetlenia pri strategických alebo dôležitých finančných rozhodnutiach sa rozhodoval opäť na základe nepresných informácií. Napríklad model predikujúci riziko nezaplatenia splatných pohľadávok môže byť „vysvetlený“ tak, že zobrazuje iba korelácie s určitými vstupmi, pričom skutočné fungovanie algoritmu nedokáže vysvetliť. V praxi to môže viesť napr. k nesprávnemu rozhodnutiu konateľa o investícii bez potrebného (a konateľom už alokovaného) kapitálu. Pre konateľa je preto vhodnejšie používať modely, ktorých logiku je možné už spočiatku priamo sledovať a overiť, čím získa transparentný a spoľahlivý podklad pre rozhodovanie a môže ľahšie uniesť dôkazné bremeno o konaní s odbornou starostlivosťou.

Aj v dôsledku rizík načrtnutých vyššie by konateľ mal výsledky z AI nástroju porovnať s aspoň jedným ďalším zdrojom (interný report, externý poradca) alebo by mal disponovať overenými zdrojmi informácií, z ktorých AI vychádzalo a kriticky vyhodnotiť ich dôveryhodnosť a relevanciu.

Smart kontrakty a podnikateľské riziko

Ďalším nástrojom digitalizácie sú smart kontrakty, ktoré možno definovať ako *„dohody strán, ktoré sú uchovávané v podobe počítačového kódu zaznamenaného v technológii Blockchain, ktorá zabezpečuje nezávislé a automatické vykonanie dohody po naplnení vopred dohodnutých podmienok.“*²⁰ Konkrétne, smart kontrakty sú nasadzované na blockchain vo forme kódu, ktorý obsahuje zmluvné podmienky, spúšťacie podmienky a logiku vykonávania. Keď sú splnené spúšťacie podmienky, inteligentné zmluvy automaticky vykonajú príslušné operácie, ako sú prevody, záznamy údajov atď. ... Smart kontrakty sa široko používajú vo finančnom sektore. Môžu sa používať pri cezhraničných platbách, financovaní dodávateľského reťazca, ekvitem

¹⁸ GUIDOTTI, Riccardo – MONREALE, Anna – RUGGIERI, Salvatore – TURINI, Franco – GIANNOTTI, Fosca – PEDRESCHI, Dino: A Survey of Methods for Explaining Black Box Models. In: ACM Computing Surveys, Roč. 51, č. 5 (2018), s. 12.

¹⁹ RUDIN, Cynthia: Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. In: Nature Machine Intelligence, Roč. 1, č. 5 (2019), s. 208–210.

²⁰ HRABČÁK, Ladislav a kol.: Blockchain technológia ako činiteľ (faktor) ovplyvňujúci súčasnú podobu práva. Košice: ŠafárikPress, 2021. 32 s. ISBN 978-80-8152-983-2.

financovaní a emisii cenných papierov, v poisťovníctve".²¹ Smart kontrakty nie sú nástroje využívajúce umelú inteligenciu, ale kódy, ktoré transparentne automatizujú proces vykonania záväzku, po splnení dohodnutých podmienok a tým eliminujú potrebu intervencie zmluvných strán. Výhodami smart kontraktu sú zníženie rizika neplnenia záväzku, nižšie prevádzkové náklady, a zvýšená efektívnosť obchodných procesov.²² Vo vzťahu k spoločníkom aj zainteresovaným stranám (stakeholders) má implementácia inteligentných zmlúv do vnútropodnikových procesov význam napríklad v tom, že transakcie sa zaznamenávajú na blockchaine ako nezmeniteľné, hashované, záznamy. Takáto transparentnosť môže pôsobiť ako prevencia pred tzv. tunelovaním spoločnosti zo strany konateľa a zároveň poskytuje spoločníkom spoľahlivý podklad na kontrolu výkonu jeho funkcie.

Smart kontrakty operujú výlučne v prostredí blockchainu, ktoré funguje izolovane od externého prostredia, vzhľadom na čo smart kontrakty nemajú schopnosť získavať údaje o vonkajších udalostiach alebo skutočnom stave právnych vzťahov²³, napr. dodanie tovaru alebo služby, stav výmenných kurzov, výsledky súdnych sporov. Na prekonanie danej bariéry sa využívajú tzv. oracles, ktoré sprostredkujú externé dáta do blockchainového systému a umožňujú tak spúšťanie smart kontraktov²⁴. Problémom tohto postupu je, že zdroj vstupných dát môže byť nespoľahlivý alebo zámerne pozmenený a smart kontrakt bude reprodukovat' chybný výstup. Nie sú vylúčené ani chyby kódu spôsobené developermi.

S uvedenou problematikou úzko súvisí aj rigidita vykonania smart kontraktu súvisiaca s problematikou „code is law“²⁵. Kým v bežných právnych vzťahoch má konateľ alebo zmluvné strany možnosť flexibilne reagovať na nové okolnosti a prípadne modifikovať alebo odložiť plnenie zmluvy, smart kontrakt sa po splnení podmienok vykoná automaticky a nezvratne. Premena právnej flexibility medzi zmluvnými stranami (napr. zmluvná podmienka „v primeranej lehote“, „poskytnutie potrebnej súčinnosti“ a pod.) na kód „*znamená jej zredukovanie na formu a hranice programovacieho jazyka. Táto redukcia je zložitá a náročná, ak je vôbec možná.*“²⁶

²¹ WANG, Xiangzhen: Research on the Application of Blockchain Technology and Smart Contracts in the Financial Industry. In: *Frontiers in Business Economics and Management*, Roč. 15, č. 2 (2024), s. 392.

²² Tamtiež.

²³ TAHERDOOST, Hamed: Smart Contracts in Blockchain Technology: A Critical Review. In: *Information*, Roč. 14, č. 117 (2023), s. 7.

²⁴ ANDREI, Alexandru Gabriel: Hybrid Smart Contracts with Decentralized Oracles. In: *Romanian Cyber Security Journal*, Roč. 6, č. 1 (2024), s. 100.

²⁵ DE FILIPPI, Primavera – HASSAN, Samer: Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. In: *First Monday*, Roč. 21, č. 12 (2016).

²⁶ CVETKOVIĆ, Predrag: Liability in the Context of Blockchain-Smart Contract Nexus: Introductory Considerations. In: *Zbornik radova Pravnog fakulteta Niš*, Roč. 59, č. 89 (2020), s. 97.

Po popísaní uvedených rizík je na mieste otázka zodpovednosti konateľa, ak je v dôsledku použitia smart kontraktu spôsobená spoločnosti škoda. Je potrebné poznamenať, že obchodnoprávny záväzok vzniká, mimo iné, z právnych úkonov, najmä zmlúv medzi subjektami práva s právnou subjektivitou. Ak dôjde k chybe algoritmu smart kontraktu alebo sa z iného dôvodu smart kontrakt nevykoná v súlade s dohodou zmluvných strán, platí záväzok dohodnutý medzi zmluvnými stranami a konateľ je v takom prípade povinný postupovať v súlade s ním. Smart kontrakt nemení obsah kontraktu, ale predstavuje spôsob (formu) jeho vykonania, pričom smerodajná je vôľa kontrahentov. Aby konateľ naplnil požiadavku riadneho plnenia svojich fiduciárnych povinností, musí pred implementáciou a počas používania smart kontraktu overiť spoľahlivosť vstupných dát (napr. prostredníctvom overených oracles), monitorovať výstupy, byť pripravený zasiahnuť pri chybných alebo nepredvídaných výsledkoch algoritmu a plniť dohodnutý záväzok.

Záver

Povinnosť odbornej starostlivosti zahŕňa nielen prijímanie rozhodnutí na základe dostupných informácií, ale aj schopnosť kriticky vyhodnotiť ich dôveryhodnosť a relevanciu. Ak sa používa strojové učenie, problémom je často „black box“ efekt. Pri využívaní nástrojov s AI je preto dôležitá algoritmická transparentnosť použitím explainable AI (XAI), pravidelný audit algoritmov nezávislými orgánmi a kontrola výstupov. Nedostatočná transparentnosť a prílišné spoliehanie sa na výstupy AI konateľom môžu viesť k rozhodnutiam, ktoré sú v rozpore s povinnosťou odbornej starostlivosti a poškodzujú záujmy spoločnosti, pretože zodpovednosť za rozhodnutia zostáva na konateľovi, a nie na technológii. Smart kontrakty môžu v obchodnej praxi prispieť k vyššej efektívnosti, transparentnosti a kontrole výkonu funkcie konateľa, avšak ich uplatňovanie je limitované technickými rizikami (chybné vstupy z oracles, chyby kódu) a rigiditou algoritmu a jeho technických hraníc fungovania. Keďže smart kontrakt nemení obsah dohody, ale iba spôsob jej vykonania, konateľ je povinný naďalej zabezpečiť riadne plnenie záväzkov.

Používanie nástrojov s AI nezužuje fiduciárne povinnosti konateľa, naopak, rozširuje ich nový rozmer súvisiaci s kontrolou a riadením technológií. Konateľ by mal mať schopnosť orientovať sa v technológiách a správne ich zapojiť do rozhodovania a vnútropodnikových procesov, alebo využiť externého poradcu. Totiž, aj neimplementovanie digitálnych technológií môže predstavovať konanie v rozpore s fiduciárnymi povinnosťami konateľa, ak by po zohľadnení relevantných prínosov a rizík mohli digitálne technológie priniesť pre spoločnosť hodnotu.

Zoznam použitej literatúry

1. ANDREI, Alexandru Gabriel: Hybrid Smart Contracts with Decentralized Oracles. In: Romanian Cyber Security Journal, Roč. 6, č. 1 (2024).
2. BARNEY, Jay: Firm Resources and Sustained Competitive Advantage. In: Journal of Management, Roč. 17, č. 1 (1991).
3. CSACH, Kristián: Digital Corporate Governance in Slovakia. In: Právny obzor, Roč. 105, špeciálne číslo (2022).
4. CVETKOVIĆ, Predrag: Liability in the Context of Blockchain-Smart Contract Nexus: Introductory Considerations. In: Zbornik radova Pravnog fakulteta Niš, Roč. 59, č. 89 (2020).
5. DE FILIPPI, Primavera – HASSAN, Samer: Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. In: First Monday, Roč. 21, č. 12 (2016).
6. DIETZMANN, Christian – DUAN, Yanqing: Artificial Intelligence for Managerial Information Processing and Decision-Making in the Era of Information Overload. In: Proceedings of the 55th Hawaii International Conference on System Sciences 2022 (2022).
7. GANGWAR, Roopal – DASH, Bidya – NANDA, Amitabh – AYYUB, Sheenam: Impact of Artificial Intelligence (AI) Enabled Management Information System (MIS) in Managerial Decision Making: An Empirical Study of Leading Business Organisation. In: Journal of Informatics Education and Research, Roč. 4, č. 2 (2024).
8. GUIDOTTI, Riccardo – MONREALE, Anna – RUGGIERI, Salvatore – TURINI, Franco – GIANNOTTI, Fosca – PEDRESCHI, Dino: A Survey of Methods for Explaining Black Box Models. In: ACM Computing Surveys, Roč. 51, č. 5 (2018).
9. HANELT, André – BOHNSACK, René – MARZ, David – MARANTE, Cláudia Antunes: A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. In: Journal of Management Studies, Roč. 58, č. 5 (2020).
10. HAQUE, Huda Shireen: Artificial General Intelligence: How Close Are We Really? In: International Journal of Advanced Research in Science, Engineering and Management, Roč. 12, č. 4 (2025).
11. HRABČÁK, Ladislav a kol.: Blockchain technológia ako činiteľ (faktor) ovplyvňujúci súčasnú podobu práva. Košice: ŠafárikPress, 2021. ISBN 978-80-8152-983-2.
12. LI, Na – WANG, Xiaohong – WANG, Zeren – LUAN, Xiangyu: The Impact of Digital Transformation on Corporate Total Factor Productivity. In: Frontiers in Psychology, Roč. 13 (2022).

13. MESKE, Christian – BUNDE, Enrico – SCHNEIDER, Johannes – GERSCH, Martin: Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities. In: *Information Systems Management*, Roč. 39, č. 1 (2020).
14. PINTÉROVÁ, Dominika: Vplyv súdnych rozhodnutí na doktrínu obchodnoprávných zmlúv v kontexte umelej inteligencie: výzvy a nové horizonty. In: *Míľniky práva v stredoeurópskom priestore 2025*. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2025. ISBN 978-80-7160-758-8.
15. PRIYANTO, Panji – MURWANINGSARI, Etty – AUGUSTINE, Yvonne: Impact Digital Business Strategy on Competitive Advantage in the Banking Sector. In: *European Journal of Business Management and Research*, Roč. 8, č. 2 (2023).
16. REIS, João – MELÃO, Nuno: Digital Transformation: A Meta-Review and Guidelines for Future Research. In: *Heliyon*, Roč. 9, č. 7 (2023).
17. RUDIN, Cynthia: Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. In: *Nature Machine Intelligence*, Roč. 1, č. 5 (2019).
18. SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. 1. vydanie. Bratislava: C. H. Beck, 2024. ISBN 978-80-8232-050-6.
19. TAHERDOOST, Hamed: Smart Contracts in Blockchain Technology: A Critical Review. In: *Information*, Roč. 14 (2023).
20. TEECE, David J. – PETERAF, Margaret A. – HEATON, Sohvi: Dynamic Capabilities and Organizational Agility: Risk, Uncertainty and Entrepreneurial Management in the Innovation Economy. In: *Tuck School of Business Working Paper*, č. 2771245 (2016).
21. WANG, Xiangzhen: Research on the Application of Blockchain Technology and Smart Contracts in the Financial Industry. In: *Frontiers in Business Economics and Management*, Roč. 15, č. 2 (2024).
22. ZHANG, Yaxin – JIN, Shanyue: How Does Digital Transformation Increase Corporate Sustainability? The Moderating Role of Top Management Teams. In: *Systems*, Roč. 11, č. 7 (2023). Zhang, Y. and Jin, S. How does digital transformation increase corporate sustainability? the moderating role of top management teams. *Systems*, 11(7), 2023, 355. Dostupné online na: <https://doi.org/10.3390/systems11070355>

Kontaktné údaje

JUDr. Peter Šikulínek

sikulinec2@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra obchodného práva
a hospodárskeho práva

ETICKÉ OTÁZKY V POUŽÍVANÍ AI PRI OBCHODNÝCH ČINNOSTIACH¹

ETHICAL QUESTIONS IN THE USE OF AI IN BUSINESS ACTIVITIES

Andrej Oriňak²

Abstrakt: V predkladanom príspevku sa zameriavame na skúmanie etických aspektov využívania umelej inteligencie v podnikaní v súvislosti s digitalizáciou hospodárskeho prostredia a obchodným právom. Cieľom je preskúmať, akým spôsobom reaguje právny poriadok na dynamický rozvoj umelej inteligencie, a či sú súčasne formované aj súvisiace etické štandardy. Zameriavame sa na analýzu rovnováhy medzi inováciami a relevantnou právnou úpravou. Túto tému považujeme za aktuálnu predovšetkým z dôvodu presvedčenia, že je potrebné kontrolovať nástroje umelej inteligencie a zabezpečiť, aby subjekty v podnikateľskom prostredí boli chránené pred diskrimináciou či zásahmi do ich práva na súkromie. Téma článku je výrazne interdisciplinárna, keďže prepája skúmanie súčasných právnych noriem, súčasné procesy digitalizácie a nástroje umelej inteligencie. Analyzovali sme najmä oblasť e-commerce, oblasť finančných služieb či dodávateľské reťazce. Výsledky výskumu naznačujú, že s využívaním umelej inteligencie v podnikaní môže byť spojených hneď niekoľko významných rizík. Medzi tieto riziká možno zaradiť hrozbu úniku a zneužitia osobných údajov, ako aj pomerne známu diskrimináciu algoritmami (bias). Patrí sem tiež komplikovaná kontrola procesov, ktorými umelá inteligencia pracuje, inými slovami, problém predstavuje aj transparentnosť modelov umelej inteligencie. Ďalšou významnou výzvou v tejto súvislosti je neukončená a nejednoznačne uzavretá otázka zodpovednosti za úkony umelej inteligencie. V neposlednom rade sme sa zaoberali aj otázkou nezamestnanosti v súvislosti s automatizáciou, teda, či umelá inteligencia skutočne intenzívne ohrozuje počet pracovných miest na trhu. Záverom príspevku zdôrazňujeme potrebu systematického prístupu, najmä čo sa týka implementácie etických smerníc, pravidelných kontrol a školení zamestnancov, ktorí vo svojej práci využívajú skúmané modely. Výsledky výskumu indikujú, že podnikatelia implementujúci umelú inteligenciu do svojho podnikania by mali dbať najmä na kvalitné zabezpečenie ochrany osobných údajov, voľbu čo najviac vysvetliteľných

¹ Príspevok spracovaný v rámci plnenia grantových úloh projektu APVV-21-0336 „Analýza súdnych rozhodnutí metódami umelej inteligencie“.

² Katedra obchodného práva a hospodárskeho práva, Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach

modelov umelej inteligencie, či nastavenie interných smerníc zodpovednosti pri využívaní modelov umelej inteligencie.

Kľúčové slová: umelá inteligencia, etika, podnikanie, algoritmická zaujatosť, transparentnosť, ochrana dát

Abstract: In this paper, we focus on examining the ethical aspects of the use of artificial intelligence in business in relation to the digitization of the economic environment and commercial law. The aim is to examine how the legal system responds to the dynamic development of artificial intelligence and whether related ethical standards are also being formed. We focus on analyzing the balance between innovation and relevant legal regulation. We consider the topic to be particularly relevant because we believe that artificial intelligence tools need to be controlled and that entities in the business environment need to be protected from discrimination or interference with their right to privacy. The topic of the article is distinctly interdisciplinary, as it links the examination of current legal norms, current digitization processes, and artificial intelligence tools. We analyzed in particular the areas of e-commerce, financial services, and supply chains. The results of the research indicate that the use of artificial intelligence in business may be associated with several significant risks. These include the threat of personal data leaks and misuse, as well as the well-known issue of algorithmic bias. Another challenge is the relatively complicated process of monitoring the processes used by artificial intelligence, in other words, the transparency of artificial intelligence models. Another significant challenge in this regard is the not entirely clear question of who is responsible for the actions of artificial intelligence. Last but not least, we also addressed the issue of unemployment in relation to automation, i.e., whether artificial intelligence really poses such a serious threat to the number of jobs on the market. In conclusion, we emphasize the need for a systematic approach, especially with regard to the implementation of ethical guidelines, regular checks, and regular training for employees who use the models under investigation in their work. The results of the research indicate that entrepreneurs implementing the use of artificial intelligence in their businesses should pay particular attention to ensuring high-quality personal data protection, choosing the most explainable artificial intelligence models possible, and setting internal guidelines for responsibility when using artificial intelligence models.

Key words: artificial intelligence, ethics, business, algorithmic bias, transparency, data protection

Úvod

V súčasnej dynamickej digitálnej ére sa umelá inteligencia (AI) etablovala ako transformačná sila, ktorá zásadne mení obchodné činnosti naprieč širokým spektrom odvetví.³ Od marketingu a financií cez riadenie ľudských zdrojov až po komplexné dodávateľské reťazce, AI systémy sú nasadzované s cieľom zvýšiť efektivitu, optimalizovať rozhodovacie procesy a poskytovať personalizované zákaznícke skúsenosti.⁴ Tento nárast adopcie AI prináša firmám výrazné ekonomické prínosy, ako sú zlepšenie prognóz, automatizácia opakujúcich sa úloh a generovanie cenných poznatkov z rozsiahlych súborov dát.⁵ Napríklad, reklama využívajúca AI algoritmy umožňuje organizáciám cielene zobrazovať personalizované reklamy v najrelevantnejších miestach a časoch pre cieľové publikum, čím sa zvyšuje efektívnosť marketingových kampaní.⁶ Digitálna transformácia je katalyzátorom pre inovácie obchodných modelov, čo podčiarkuje strategickú hodnotu AI.⁷

So vzrastajúcim nasadzovaním AI technológií však súčasne vyvstávajú zložité etické otázky a výzvy, ktoré si vyžadujú okamžitú a systematickú pozornosť. Integrácia AI do obchodného prostredia prináša so sebou riziká spojené s algoritmickou zaujatosťou, nedostatočnou transparentnosťou rozhodovacích procesov, výzvami v oblasti ochrany súkromia a údajov, a vplyvom na zamestnanosť a pracovnú silu. Tieto etické dilemy môžu v prípade zanedbania viesť k vážnym dôsledkom, vrátane podkopania dôvery verejnosti, vzniku právnych problémov (napr. žaloby za diskrimináciu) a potenciálne spôsobiť spoločenské nerovnosti.⁸

Téma predkladaného príspevku je interdisciplinárna, keďže spája skúmanie súčasných právnych noriem s dynamicky sa vyvíjajúcimi digitálnymi procesmi a nástrojmi AI, využívanými v podnikaní. Cieľom predkladaného príspevku je identifikovať a analyzovať kľúčové etické výzvy spojené s používaním umelej inteligencie v obchodných činnostiach, s dôrazom na právne, spoločenské a technologické aspekty. V príspevku analyzujeme existujúce stratégie, ktoré by

³ ADAMA, Henry Ejiga – OKEKE, Chukwuekem David: Digital transformation as a catalyst for business model innovation: A critical review of impact and implementation strategies. In: Magna Scientia Advanced Research and Reviews, roč. 10, č. 2 (2024), s. 256.

⁴ KUMAR, V. – ASHRAF, Abdul Rehman – NADEEM, Waqar: AI-powered marketing: What, where, and how? In: International Journal of Information Management, (2024), s. 17.

⁵ KUMAR, V. – ASHRAF, Abdul Rehman – NADEEM, Waqar: AI-powered marketing: What, where, and how? In: International Journal of Information Management, (2024), s. 19.

⁶ KUMAR, V. – ASHRAF, Abdul Rehman – NADEEM, Waqar: AI-powered marketing: What, where, and how? In: International Journal of Information Management, (2024), s. 21 – 23.

⁷ ADAMA, Henry Ejiga – OKEKE, Chukwuekem David: Digital transformation as a catalyst for business model innovation: A critical review of impact and implementation strategies. In: Magna Scientia Advanced Research and Reviews, roč. 10, č. 2 (2024), s. 256.

⁸ IVCHYK, Vasyl: Towards ethical and sustainable development in business management with AI. In: Grail of Science, roč. 40 (2024), s. 76.

umožnili podnikateľským subjektom zodpovedne implementovať AI technológie tak, aby bola zachovaná podpora inovácie bez ohrozenia základných etických princípov, ako sú spravodlivosť, transparentnosť, ochrana súkromia a ľudská dôstojnosť.

Výskumná otázka a hypotézy

V kontexte bezprecedentného rozmachu umelej inteligencie a jej implementácie do obchodných činností považujeme za kľúčové nielen využiť jej potenciál, ale aj komplexne pochopiť a riešiť etické dôsledky, ktoré z tohto vývoja vyplývajú. Identifikáciu a zmierňovanie týchto rizík považujeme za nevyhnutné, najmä s ohľadom na udržateľný rozvoj AI v podnikateľskom prostredí. Na základe analýzy literatúry formulujeme nasledovnú výskumnú otázku:

„Aké sú kľúčové etické výzvy spojené s používaním umelej inteligencie v obchodných činnostiach a ako môžu podniky efektívne zabezpečiť minimalizáciu týchto rizík?“

Za účelom podrobného preskúmania výskumnej otázky sme stanovili tri vedecké predpoklady:

Hypotéza č. 1: *„Implementácia rozmanitých a reprezentatívnych tréningových dát v systémoch AI výrazne znižuje výskyt algoritmickej zaujatosti v obchodných rozhodovacích procesoch.“*

Hypotéza č. 2: *„Využívanie vysvetliteľných modelov AI a jasných mechanizmov zodpovednosti v obchodných činnostiach zvyšuje dôveru zákazníkov a zamestnancov v AI systémy.“*

Hypotéza č. 3: *„Investície podnikov do rekvalifikácie a vzdelávania zamestnancov v oblasti AI znižujú obavy z prepúšťania a zvyšujú produktivitu práce v dôsledku adaptácie na AI technológie.“*

Metodológia

V predkladanom príspevku sme využili prístup systematickej literárnej rešerše a konceptuálnej analýzy na preskúmanie etických otázok spojených s používaním AI v obchodných činnostiach. Cieľom bolo syntetizovať existujúce vedecké poznatky a identifikovať kľúčové etické výzvy a možné riešenia. Primárnymi zdrojmi dát pre túto analýzu boli vedecké publikácie, najmä recenzované články z časopisov, konferenčné príspevky a odborné správy, ktoré sa zaoberajú etikou AI v kontexte podnikania a digitálnych technológií.

Teoretické východiská a súčasný stav skúmanej problematiky

Na základe preskúmanej literatúry sme identifikovali päť kľúčových etických výziev spojených s implementáciou AI do podnikania:

Algoritmická zaujatosť

Jednou z najvýznamnejších etických výziev je algoritmická zaujatosť, ktorá môže viesť k nespravodlivým a diskriminačným výsledkom. Algoritmy AI sa učia na rozsiahlych súboroch dát, ktoré môžu neúmyselne, alebo aj zámerne, obsahovať skryté či zjavné predsudky, odrážajúce spoločenské nerovnosti alebo historickú diskrimináciu.⁹ Príkladom je proces náboru zamestnancov: ak bol algoritmus trénovaný na historických dátach, ktoré uprednostňovali uchádzačov určitého pohlavia, rasy alebo veku, môže tento systém pokračovať v týchto diskriminačných trendoch.¹⁰ Výskum ukazuje, že AI systémy používané pri náboře uprednostňovali mená spájané s bielou rasou v 85,1% prípadov a mená spájané s ženským pohlavím len v 11,1% prípadov. V niektorých situáciách boli muži afro-amerického pôvodu znevýhodnení oproti bielym mužom až v 100% prípadov.¹¹ Konkrétnym príkladom je HireVue Iris, nástroj na nábor, ktorý využíva analýzu výrazov tváre na predikciu krásy, veku a pohlavia kandidátov, čo môže viesť k zaujatosti.¹² Podobne, v oblasti úverového hodnotenia hypotekárne algoritmy odmietajú úvery ľuďom z menších výrazne častejšie ako bielym žiadateľom, aj keď majú podobné finančné profily.¹³ Problémom je aj tzv. proxy bias, kedy AI môže identifikovať iné premenné, ktoré slúžia ako náhrada za vylúčené citlivé dáta (napr. pohlavie), čím sa zaujatosť prenáša ďalej.¹⁴ Typy zaujatosti môžu zahŕňať dizajnovú zaujatosť (chyby v návrhu modelu), kontextuálnu zaujatosť (nesprávna interpretácia kontextu aplikácie) a aplikačnú zaujatosť (nesprávna aplikácia algoritmu).¹⁵ Dôsledkom algoritmickej zaujatosti je nielen nespravodlivé zaobchádzanie s jednotlivcami, ale aj potenciálne poškodenie reputácie spoločnosti, straty príjmov a právne sankcie. Pre minimalizáciu zaujatosti je nevyhnutné aktívne pracovať na jej identifikácii a eliminácii predsudkov, používať

⁹ IVCHYK, Vasyl: Towards ethical and sustainable development in business management with AI. In: Grail of Science, roč. 40 (2024), s. 78.

¹⁰ IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 67.

¹¹ WILSON, Kyra – CALISKAN, Aylin: Gender, Race, and Intersectional Bias in Resume Screening via Language Model Retrieval. In: arXiv preprint, (2024), s. 7 – 10.

¹² FERNÁNDEZ-MARTÍNEZ, Carmen – FERNÁNDEZ, Alberto: AI and recruiting software: Ethical and legal implications. In: Paladyn, Journal of Behavioral Robotics, roč. 11, č. 1 (2020), s. 199 – 200.

¹³ IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 67.

¹⁴ IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 66.

¹⁵ KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 5.

rozmanité a vyvážené dátové sady a implementovať metódy pre nepretržité monitorovanie a korigovanie algoritmov.¹⁶

Transparentnosť, vysvetliteľnosť a zodpovednosť

Ďalším kľúčovým etickým problémom je nedostatočná transparentnosť a vysvetliteľnosť rozhodnutí generovaných AI systémami. Algoritmy AI sú často označované ako „čierne skrinky“ (*black boxes*), kde je proces rozhodovania neprehľadný a ťažko pochopiteľný pre ľudských používateľov. Táto neprehľadnosť môže viesť k nedôvere zo strany zákazníkov a zamestnancov, ktorí nevedia, ako boli prijaté rozhodnutia, ktoré ich ovplyvňujú.¹⁷ Prípad Denise, ktorej banka zamietla žiadosť o životné poistenie systémom AI v priebehu minút bez jasného vysvetlenia, je konkrétnym príkladom, kedy nedostatok transparentnosti viedol k otázkam o použitých dátach a procese rozhodovania, s vyhlídkou na právne kroky pre potenciálnu diskrimináciu podľa EÚ zákonov.¹⁸ Navyše, ak AI systém urobí chybu alebo diskriminačné rozhodnutie, je ťažké určiť, kto nesie zodpovednosť – či už vývojár, prevádzkovateľ, manažér, alebo dokonca samotný systém. Prípad smrteľnej nehody autonómneho vozidla Uber v roku 2018, kde auto nezistilo chodca používajúceho priechod a bezpečnostný vodič sa nedíval na cestu, je ilustratívnym príkladom dilemy zodpovednosti.¹⁹ Pre zabezpečenie transparentnosti a zodpovednosti musia spoločnosti implementovať interpretovateľné modely AI (tzv. Explainable AI – XAI), ktoré umožňujú vysvetliť, ako bolo konkrétne rozhodnutie prijaté.²⁰

Ochrana súkromia a osobných údajov

AI systémy sú vysoko závislé od rozsiahlych súborov dát, vrátane citlivých osobných údajov. Ich zhromažďovanie, ukladanie, spracovanie a prepojenie otvára vážne otázky týkajúce sa ochrany súkromia a potenciálneho zneužitia dát. Spotrebitelia sa čoraz viac obávajú toho, ako sa používajú ich osobné údaje, najmä s nárastom AI a

¹⁶ IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 67.

¹⁷ IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 64 – 65.

¹⁸ KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 9.

¹⁹ VIEWEG, Stefan H.: AI for the Good: Artificial Intelligence and Ethics. Cham: Springer International Publishing, 2021. s. 229. ISBN 978-3-030-66912-6.

²⁰ VIEWEG, Stefan H.: AI for the Good: Artificial Intelligence and Ethics. Cham: Springer International Publishing, 2021. s. 171. ISBN 978-3-030-66912-6.

rozsiahlych dát, ktoré firmám umožňujú získať o svojich zákazníkoch veľmi veľa informácií.²¹ Riziká úniku dát, krádeže identity a neoprávneného prístupu sú reálne a môžu mať pre jednotlivcov aj podniky katastrofálne následky. Príkladom je škandál Cambridge Analytica a Facebook z roku 2018, ktorý zahŕňal neoprávnené zhromažďovanie a použitie osobných dát miliónov používateľov Facebooku na psychografické profilovanie a cieľnú politickú reklamu.²² Podobne, prípady ako vydieranie pacientov vo Fínsku, ku ktorému došlo po krádeži záznamov o terapii hackermi v roku 2020, demonštrujú vážne dôsledky nedostatočnej ochrany dát.²³ AI môže s presnosťou až 80% odvodiť citlivé vlastnosti (ako politické názory alebo sexuálnu orientáciu) zo zdanlivo nevinných údajov. Psychologické cielenie pomocou AI dokáže vytvárať psychologické profily používateľov pre efektívnu cieľnú reklamu a predpovedať dokonca aj príjmy z Facebookových profilov.²⁴ Takzvaný „paradox personalizácie“ odráža dilemu, v ktorej zákazníci musia vyvážiť svoje obavy o súkromie s výhodami plynúcimi z personalizovaných odporúčaní a ponúk.²⁵ Často sa to prejavuje aj tak, že spotrebitelia falšujú informácie, aby získali späť určitú kontrolu nad svojimi údajmi a zmiatli inzerentov.²⁶ Regulačné rámce, ako napríklad Všeobecné nariadenie o ochrane údajov (GDPR) v EÚ, sa snažia riešiť tieto problémy stanovením prísnych pravidiel pre zaobchádzanie s osobnými údajmi, vrátane práv na vymazanie údajov a prenosnosť dát. Spoločnosti musia preto nielen dodržiavať právne predpisy, ale aj prekročiť očakávania zákazníkov v oblasti súkromia, aby si udržali dôveru a zabezpečili zodpovedné používanie dát.²⁷

Vplyv na pracovnú silu a zamestnanosť

Integrácia umelej inteligencie do riadenia podniku má zásadný vplyv na pracovnú silu, pričom tento vplyv je často ambivalentný. Automatizácia rutinných úloh prostredníctvom AI vedie k výrazným zmenám na trhu práce, najmä v sektoroch, kde prevládajú opakujúce sa činnosti, ako je výroba, administratíva či služby. Stroje a algoritmy dnes dokážu vykonávať úlohy, ktoré predtým vyžadovali ľudský zásah, a to

²¹ KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 1 – 4.

²² KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 10.

²³ KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 10 – 12.

²⁴ Ibidem.

²⁵ KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 1 – 4.

²⁶ Ibidem.

²⁷ Ibidem.

s vyššou rýchlosťou a nižšími nákladmi. Tento trend spôsobuje obavy z možného zániku pracovných miest a zvyšuje riziko nezamestnanosti podmienenej technológiami. Súčasne však vznikajú nové pracovné príležitosti v oblastiach, ktoré si vyžadujú špecializované zručnosti, najmä v oblasti vývoja, správy a tréningu AI systémov. Výskumy ukazujú, že technologický pokrok môže viesť k priamemu vytlačaniu pracovníkov z tradičných pozícií, avšak zároveň podporuje vznik nových profesií a zvyšuje dopyt po kvalifikovanej pracovnej sile. Kľúčovým faktorom pre minimalizáciu negatívnych dopadov je investícia do vzdelávania a rekvalifikácie zamestnancov, ktorá umožní adaptáciu na meniace sa požiadavky trhu práce.²⁸

Environmentálny dopad AI

Umelá inteligencia, napriek svojmu digitálnemu charakteru, má značný a rastúci environmentálny dopad. Tento dopad zahŕňa:

- **Spotreba energie:** Tréning a prevádzka AI modelov vyžaduje značné množstvo energie, najmä v dátových centrách. Štúdie potvrdzujú rýchly nárast energetických nárokov v dôsledku AI, pričom veľké modely (napr. GPT-5) spotrebúvajú obrovské množstvá elektriny, čo prispieva k vyšším emisiám uhlíka.²⁹
- **Emisie:** Analýzy ukazujú, že dvadsať najväčších AI systémov môže spoločne vyprodukovať až 102,6 milióna ton ekvivalentu CO₂ ročne.³⁰
- **Vodný odpad:** Masívne tréningovanie komplexných AI modelov vyžaduje značné množstvo vody na chladenie serverov v dátových centrách, čo predstavuje ďalší environmentálny problém.³¹
- **Elektronický odpad:** Rýchla výmena použitého hardvéru v dôsledku rozvoja AI je významným zdrojom elektronického odpadu, pričom odhady hovoria o 16 miliónoch ton e-odpadu generovaného AI medzi rokmi 2020 a 2030.³²

Na základe identifikovaných etických výziev sme identifikovali nasledovné riešenia pre podniky, ktoré sa snažia o zodpovedné využívanie AI:

²⁸ KHOGALI, Hisham O. – MEKID, Samir: The blended future of automation and AI: Examining some long-term societal and ethical impact features. In: *Technology in Society*, roč. 73 (2023), s. 6 – 8.

²⁹ LUCCIONI, Alexandra – STRUBELL, Emma – CRAWFORD, Kate: From Efficiency Gains to Rebound Effects: The Problem of Jevons' Paradox in AI's Polarized Environmental Debate. In: *arXiv preprint*, (2025), s. 2.

³⁰ YU, Yang – WANG, Jiahui – LIU, Yu – YU, Pingfeng – WANG, Dongsheng – ZHENG, Ping – ZHANG, Meng: Revisit the environmental impact of artificial intelligence: the overlooked carbon emission source? In: *Frontiers of Environmental Science & Engineering*, (2024), s. 1.

³¹ KSHETRI, Nir: The Environmental Impact of Artificial Intelligence. In: *IT Professional*, roč. 26, (2024), s. 9 – 13.

³² WANG, Peng – ZHANG, Ling-Yu – TZACHOR, Asaf – MASANET, Eric – CHEN, Wei-Qiang: E-waste challenges of generative artificial intelligence. In: *Nature Computational Science*, (2024), s. 3.

Vývoj a implementácia etických rámcov a interných politík

Spoločnosti by mali vyvinúť jasné a prispôsobiteľné etické usmernenia pre AI, ktoré presahujú minimálne právne požiadavky.³³ Tieto rámce by mali byť založené na spomenutých princípoch (prospešnosť, neškodnosť, autonómia, spravodlivosť a vysvetliteľnosť) a mali by byť integrované do všetkých fáz životného cyklu vývoja AI. Koncept „Etiky prostredníctvom dizajnu“ (Ethics by Design) je kľúčový, zabezpečujúc, že etické úvahy sú zakomponované od počiatkovej fázy dizajnu až po nasadenie a prevádzku AI systémov.³⁴ To znamená, že vývojári a manažéri by mali pri navrhovaní algoritmov aktívne zvažovať potenciálne etické dôsledky a navrhovať systémy tak, aby boli od základov etické, namiesto toho, aby sa etické problémy riešili až dodatočne.³⁵ Pre praktické rozhodovanie môžu podniky využiť nástroje ako etický kompas, ktorý zahŕňa testy legality, mediálnej publicity (tzv. „frontpage test“), morálnej akceptácie blízkymi osobami (tzv. „mama test“) a „zápachový test“ na posúdenie, či rozhodnutie nezaváňa neetickým správaním.³⁶ Koncept Corporate Digital Responsibility (CDR) zdôrazňuje, že výkonnosť firmy v CDR sa hodnotí v oblastiach stratégie a riadenia, zmien a transformácie, a hodnôt a princípov.³⁷

Nepretržité monitorovanie a audit AI systémov

Firmy musia implementovať robustné mechanizmy na nepretržité monitorovanie a audit algoritmov AI, aby identifikovali a korigovali algoritmickú zaujatosť a zabezpečili spravodlivé výsledky. Tento proces by mal zahŕňať nielen technické audity dát a algoritmov (napr. na odhaľovanie zaujatosti), ale aj etické preskúmania, do ktorých sú zapojení rôzni stakeholderi, vrátane etikov, právnikov a zástupcov komunity. Príkladom je zavedenie interného audítorského agenta, ktorý by kontroloval profily pre nábor zamestnancov, najmä tie s citlivými charakteristikami ako vek či pohlavie, aby sa predišlo diskriminácii.³⁸

³³ HICKMAN, Eleanore – PETRIN, Martin: Trustworthy AI and Corporate Governance: The EU's Ethics Guidelines. In: European Business Organization Law Review, roč. 22, (2021), s. 4 – 6.

³⁴ FLORIDI, Luciano – COWLS, Josh: A Unified Framework of Five Principles for AI in Society. In: Harvard Data Science Review, roč. 1, č. 1, (2019), s. 3 – 11.

³⁵ BREY, Philip – DAINOW, Brandt: Ethics by design for artificial intelligence. In: AI and Ethics, roč. 4, (2024), s. 3 – 4.

³⁶ VIEWEG, Stefan H.: AI for the Good: Artificial Intelligence and Ethics. Cham: Springer International Publishing, 2021. s. 70. ISBN 978-3-030-66912-6.

³⁷ LOBSCHAT, Lara – MUELLER, Benjamin – EGGERS, Felix – BRANDIMARTE, Laura – DIEFENBACH, Sarah – KROSCHKE, Mirja – WIRTZ, Jochen: Corporate Digital Responsibility. In: Journal of Business Research, roč. 122, (2021), s. 7 – 10.

³⁸ VIEWEG, Stefan H.: AI for the Good: Artificial Intelligence and Ethics. Cham: Springer International Publishing, 2021. s. 169 – 170. ISBN 978-3-030-66912-6.

Vzdelávanie a rekvalifikácia zamestnancov

Na zmiernenie obáv z prepúšťania a maximalizáciu potenciálu AI by mali podniky investovať do komplexných programov vzdelávania a rekvalifikácie pre svojich zamestnancov. Tieto programy by mali byť zamerané na rozvoj digitálnych zručností a schopností potrebných pre prácu s AI, ako aj na podporu kritického myslenia, adaptability a kreativity. Cieľom je umožniť zamestnancom prejsť od rutinných úloh k úlohám, ktoré si vyžadujú ľudskú intuíciu, empatiu a strategické myslenie. To si vyžaduje manažérsku podporu a vytváranie kultúry celoživotného učenia v rámci celej organizácie.³⁹

Záver

Používanie umelej inteligencie v obchodných činnostiach predstavuje obrovský potenciál pre inovácie a rast, ale zároveň so sebou prináša aj značné etické výzvy. Ako ukázala táto komplexná analýza, hlavné etické otázky sa týkajú algoritmickej zaujatosti a spravodlivosti, transparentnosti a zodpovednosti, ochrany súkromia a údajov, vplyvu na pracovnú silu a zamestnanosť, manipulácie spotrebiteľov a environmentálneho dopadu AI. Každá z týchto oblastí si vyžaduje proaktívny a systematický prístup zo strany podnikov, aby sa minimalizovali riziká a zabezpečilo zodpovedné nasadzovanie AI technológií. Hypotézy sme vyhodnotili nasledovne:

- H₁ (Algoritmická zaujatosť): Na základe výsledkov možno konštatovať, že algoritmická zaujatosť je reálnym a významným problémom v obchodných rozhodovacích procesoch. Jej zmiernenie je priamo závislé od kvality a rozmanitosti tréningových dát a neustáleho monitoringu algoritmov. Zistenia poukazujú na riziko prenášania historických predsudkov prostredníctvom proxy premenných a na štatisticky významnú zaujatosť v aplikáciách ako nábor zamestnancov.
- H₂ (Transparentnosť a zodpovednosť): Analýzou literatúry bolo možné potvrdiť kľúčovú úlohu transparentnosti a jasných mechanizmov zodpovednosti pri budovaní dôvery v AI systémy. Vysvetliteľné modely AI (XAI) a jasné definovanie zodpovednosti za rozhodnutia sú nevyhnutné pre ich široké spoločenské prijatie a etickú prevádzku, ako ukázali prípady netransparentných rozhodnutí AI.
- H₃ (Vplyv na pracovnú silu a školenie): Možno konštatovať, že proaktívne investície do rekvalifikácie a vzdelávania zamestnancov sú účinným nástrojom na znižovanie obáv z automatizácie a na adaptáciu pracovnej sily

³⁹ IVCHYK, Vasyli: Towards ethical and sustainable development in business management with AI. In: Grail of Science, roč. 40 (2024), s. 81.

na nové role v prostredí ovplyvnenom AI. To umožňuje využiť AI ako nástroj na vylepšenie ľudských schopností, nie len na nahradenie pracovných miest. Dôkladné dodržiavanie etických smerníc, investície do transparentných a spravodlivých AI systémov a neustála podpora ľudského rozvoja sú nevyhnutné pre dlhodobý úspech a udržateľnosť podnikov v ére AI. Len takto možno dosiahnuť strategické ciele a zároveň si udržať dôveru a podporu spoločnosti.

Zoznam použitej literatúry

1. ADAMA, Henry Ejiga – OKEKE, Chukwuekem David: Digital transformation as a catalyst for business model innovation: A critical review of impact and implementation strategies. In: Magna Scientia Advanced Research and Reviews, roč. 10, č. 2 (2024), s. 256.
2. BREY, Philip – DAINOW, Brandt: Ethics by design for artificial intelligence. In: AI and Ethics, roč. 4, (2024), s. 3 – 4.
3. FERNÁNDEZ-MARTÍNEZ, Carmen – FERNÁNDEZ, Alberto: AI and recruiting software: Ethical and legal implications. In: Paladyn, Journal of Behavioral Robotics, roč. 11, č. 1 (2020), s. 199 – 200.
4. FLORIDI, Luciano – COWLS, Josh: A Unified Framework of Five Principles for AI in Society. In: Harvard Data Science Review, roč. 1, č. 1, (2019), s. 3 – 11.
5. HICKMAN, Eleanore – PETRIN, Martin: Trustworthy AI and Corporate Governance: The EU's Ethics Guidelines. In: European Business Organization Law Review, roč. 22, (2021), s. 4 – 6.
6. IVCHYK, Vasyl: Towards ethical and sustainable development in business management with AI. In: Grail of Science, roč. 40 (2024), s. 76 – 81.
7. IVCHYK, Vasyl – SHMATKO, Nataliia: Examining the Ethical Considerations of Using Artificial Intelligence in Business Management. In: Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління, roč. 35, č. 74 (2024), s. 64 – 67.
8. KARAMI, Amin – SHEMSHAKI, Milad – GHAZANFAR, Mustansar Ali: Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing. In: Data Intelligence, (2024), s. 1 – 12.
9. KHOGALI, Hisham O. – MEKID, Samir: The blended future of automation and AI: Examining some long-term societal and ethical impact features. In: Technology in Society, roč. 73 (2023), s. 6 – 8.
10. KSHETRI, Nir: The Environmental Impact of Artificial Intelligence. In: IT Professional, roč. 26, (2024), s. 9 – 13.
11. KUMAR, V. – ASHRAF, Abdul Rehman – NADEEM, Waqar: AI-powered marketing: What, where, and how? In: International Journal of Information Management, (2024), s. 17 – 23.

12. LOBSCHAT, Lara – MUELLER, Benjamin – EGGERS, Felix – BRANDIMARTE, Laura – DIEFENBACH, Sarah – KROSCHE, Mirja – WIRTZ, Jochen: Corporate Digital Responsibility. In: Journal of Business Research, roč. 122, (2021), s. 7 – 10.
13. LUCCIONI, Alexandra – STRUBELL, Emma – CRAWFORD, Kate: From Efficiency Gains to Rebound Effects: The Problem of Jevons' Paradox in AI's Polarized Environmental Debate. In: arXiv preprint, (2025), s. 2.
14. VIEWEG, Stefan H.: AI for the Good: Artificial Intelligence and Ethics. Cham: Springer International Publishing, 2021. s. 70 – 229. ISBN 978-3-030-66912-6.
15. WANG, Peng – ZHANG, Ling-Yu – TZACHOR, Asaf – MASANET, Eric – CHEN, Wei-Qiang: E-waste challenges of generative artificial intelligence. In: Nature Computational Science, (2024), s. 3.
16. WILSON, Kyra – CALISKAN, Aylin: Gender, Race, and Intersectional Bias in Resume Screening via Language Model Retrieval. In: arXiv preprint, (2024), s. 7 – 10.
17. YU, Yang – WANG, Jiahui – LIU, Yu – YU, Pingfeng – WANG, Dongsheng – ZHENG, Ping – ZHANG, Meng: Revisit the environmental impact of artificial intelligence: the overlooked carbon emission source? In: Frontiers of Environmental Science & Engineering, (2024), s. 1.

Kontaktné údaje

Mgr. Andrej Oriňak

andrej.orinak@student.upjs.sk

Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta

Katedra obchodného a hospodárskeho práva

DIGITALIZÁCIA V OBLASTI INSOLVENČNÉHO PRÁVA

DIGITALIZATION IN THE FIELD OF INSOLVENCY LAW

Aneta Kšenžighová¹

Abstrakt: Predložený príspevok sa zaoberá problematikou digitalizácie a elektronizácie, ktoré sa od zavedenia registra úpadcov systematicky dotýkajú aj oblasti insolvenčného práva. Rozsah údajov zverejňovaných v registri úpadcov sa legislatívnymi zásahmi za obdobie predchádzajúcich ôsmich rokov kontinuálne rozširoval, pričom ďalšiu významnú zmenu v tejto oblasti prináša od 01. októbra 2025 pripravovaný insolvenčný register, ktorý nahradí register úpadcov. Dôraz príspevku je kladený na komparáciu rozsahu a charakteru zverejňovaných údajov slovenského registra úpadcov s obdobnými registrami v okolitých krajinách, poukazuje na jeho význam, štruktúru, prínos a možnosti jeho praktického využitia. Vďaka digitalizácii, ktorá umožňuje široký geografický dosahu údajov, sa zverejňované údaje stávajú ľahko dostupnými, je možné ich jednoduchým spôsobom nielen získavať, spracovávať ale aj zneužívať. Z tohto dôvodu vzhľadom na neustále narastajúci rozsah údajov sprístupňovaných v registri úpadcov resp. pripravovanom insolvenčnom registri, poukazujeme na nástrahy spojené s digitalizáciou údajov, na nejasnú hranicu medzi digitalizáciou údajov v insolvenčnom práve a ochranou osobných údajov, ktorá je tak vystavovaná novým druhom hrozieb a na potrebu venovať zvýšenú pozornosť aj problematike nevyhnutnosti, účelnosti a rozsahu zverejňovania informácií o fyzických a právnických osobách, ktoré sú súčasťou insolvenčných spisov, sprístupňovaných registrom úpadcov, resp. insolvenčným registrom.

Kľúčové slová: register úpadcov, insolvenčný register, digitalizácia, elektronizácia, osobné údaje.

Abstract: This paper deals with the issue of digitalization and electronization, which, since the implementation of the bankruptcy register, have also systematically affected the area of insolvency law. The scope of data published in the bankruptcy register has been continuously expanded through legislative interventions over the past eight years, with another significant change in this area coming on October 1, 2025, when the planned insolvency register will

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Katedra obchodného práva a hospodárskeho práva.

replace the bankruptcy register. The article focuses on comparing the amount and type of information published in the Slovak bankruptcy register with similar registers in neighboring countries, highlighting its importance, structure, benefits, and practical uses. Thanks to digitalization, which allows for a wide geographical reach of data, the published data becomes easily accessible and can be easily obtained, processed, and misused. For this reason, given the continuously growing scope of data made available in the register of bankruptcies or the planned insolvency register, we point out the pitfalls associated with data digitization, the unclear boundary between data digitization in insolvency law and personal data protection, which is thus exposed to new types of threats, and the need to give increased attention to the issue of the necessity, purposefulness, and scope of disclosure of information about natural and legal persons that are part of insolvency files made available by the bankruptcy register or the insolvency register.

Key words: bankruptcy register, insolvency register, digitalization, electronization, personal data.

Úvod

Súčasný svet sa rýchlo mení. Nové technológie, digitalizácia, elektronizácia, či umelá inteligencia sú v súčasnosti propagované ako nástroje prinášajúce inovácie v mnohých oblastiach nášho života. Rýchle tempo digitalizácie a jej prenikanie aj do oblastí, kde sa digitalizácia pôvodne neočakávala, sú sprevádzané sociálnymi a legislatívnymi zmenami, ktoré sa snažia identifikovať, pochopiť a následne reagovať na jej účinky.² S rýchlym tempom zmien je úzko spojená aj nevyhnutnosť dynamického a čo možno najjednoduchšieho prístupu k informáciám, k čomu vo významnej miere prispieva aj efektívna digitalizácia súdnych konaní. Digitalizácia a elektronizácia sa preto v súčasnosti dotýka mnohých odvetví práva a výnimkou nie je ani oblasť insolvenčného práva. Frekventovanou témou obdobia tvorby tohto článku sa stáva aj pripravovaný register predinsolvenčných, likvidačných a insolvenčných konaní (ďalej ako „*insolvenčný register*“), ktorý má od 1. októbra 2025 nahradiť aktuálne ešte aktívny register úpadcov.

² MADLEŇÁK, Adam – ŠVEC, Marek: The right to communicate on digital platforms and its impact on boosting their global reach. In: Globalization and its socio-economic consequences: 22th international scientific conference. Žilina: Žilinská univerzita v Žiline, 2022, s. 872-880. ISBN 978-80-8154-332-6.

Vývoj digitalizácie insolvenčného práva v podmienkach Slovenskej republiky

Éra digitalizácie v insolvenčnom práve sa v podmienkach Slovenskej republiky začala v roku 2016³, a to vytvorením informačného systému označeného ako register úpadcov, prostredníctvom ktorého nepochybne dochádzalo k postupnému zvyšovaniu transparentnosti a verejnej kontroly v predmetnej oblasti. Udialo sa tak pod vplyvom európskej právnej úpravy. Povinnosť zavádzať na svojom území jeden alebo viacero registrov, v ktorých sa uverejňujú informácie, týkajúce sa insolvenčných konaní vyplývala členským štátom EÚ priamo z Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní⁴ (ďalej ako „*Nariadenie o insolvenčnom konaní*“), ktoré zároveň stanovilo minimálny rozsah informácií, ktoré sú členské štáty povinné vo svojich insolvenčných registroch sprístupňovať.

Prax totiž ukázala, že publicita informácií a rozhodnutí v insolvenčnom konaní využívaním offline metód informovania veriteľov, iných zainteresovaných strán a širokej verejnosti o začatí, ukončení a ďalších dôležitých krokoch v konkurznom konaní nefungovali v cezhraničnom kontexte uspokojivo. Nariadenie Rady (ES) č. 1346/2000 z 29. mája 2000 o konkurznom konaní (ďalej ako „*Nariadenie 1346/2000*“) sa ešte muselo potýkať s klasickými offline metódami zverejňovania rôznych údajov (napr. oznámením v novinách, oznámením v úradnom vestníku, vyvesením oznámení na súdnych nástenkách, zasielaním individuálnych oznámení známym veriteľom).⁵ Takýto systém zabezpečovania publicity informácií o insolvenčných konaniach podľa Nariadenia 1346/2000 nebol pre členské štáty povinný a už vôbec nie jednoduchý.⁶ Postupne, najmä vďaka technologickému pokroku, sa oznamovanie prostredníctvom online registrov platobnej neschopnosti stalo dominantnou metódou sprístupňovania informácií o insolvenčných konaniach v celej Európe. Povinnosť členských štátov vytvoriť elektronické registre úpadcov bol prvým krokom k následnému vzájomnému prepojeniu týchto registrov tak, aby bolo umožnené vyhľadávanie informácií vo všetkých úradných jazykoch Európskej únie prostredníctvom Európskeho portálu elektronickej justície.⁷

³ Register úpadcov bol vytvorený s účinnosťou k 1. júlu 2016.

⁴ Článok 24 Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní.

⁵ VEDER, Michael: *Article 24— Establishment of insolvency registers* In: *Commentary on the European Insolvency Regulation*. Second Edition. Online. Oxford: Oxford University Press, 2022. s. 384–389. ISBN 978-01-91915-06-2.

⁶ IKRÉNI, Ivan: Nariadenie o insolvenčnom konaní. Komentár. Bratislava: C. H. Beck, 2020, s. 410 -411. ISBN 978-80-89603-82-4.

⁷ Európsky portál elektronickej justície je dostupný na nasledovnom webovom sídle: https://e-justice.europa.eu/home_sk [cit. 2025-09-17].

Register úpadcov⁸, upravený v § 10a Zákona č. 7/2005 Z. z. o konkurze a reštrukturalizácii a o zmene a doplnení niektorých zákonov (ďalej ako „ZKR“ alebo „zákon“) poskytuje v období tvorby tohto článku komplexné informácie o prebiehajúcich konkurzných a reštrukturalizačných konaniach. Zákon register definuje ako informačný systém verejnej správy, ktorý je sprístupnený na webovom sídle Ministerstva spravodlivosti Slovenskej republiky.⁹ Správcom a prevádzkovateľom tohto systému je Ministerstvo spravodlivosti Slovenskej republiky.

Prístup do registra nepodlieha prihláseniu ani žiadnym poplatkom.

Prínosom registra úpadcov je nielen koncentrácia všetkých údajov o jednotlivých konkurzných a reštrukturalizačných konaniach¹⁰, ktoré boli do jeho zavedenia

⁸ Register úpadcov bol do ZKR zvedený Zákonom č. 390/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 420/2004 Z. z. o mediácii a o doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, a to s účinnosťou od 01.01.2016. Plne funkčným sa stal až od 01.07.2016, kedy sa jeho informačný záber rozšíril, ale iba na konania začaté po 30.06.2016.

⁹ Register úpadcov je verejne dostupný na nasledovnom webovom sídle: <https://ru.justice.sk/ru-verejnost-web/> [cit. 2025-09-17].

¹⁰ Podľa znenia § 10a ods. 2, písm. a) ZKR, údaje o konaniach podľa tohto zákona sa s účinnosťou od 1.1.2018 zverejňujú v nasledovnom rozsahu: „1. označenie súdu, 2. spisová značka konania, 3. meno a priezvisko sudcu konajúceho vo veci, 4. označenie navrhovateľa a dlžníka, ak ide o 4.1 fyzickú osobu, meno, priezvisko, dátum narodenia a bydlisko, 4.2 fyzickú osobu podnikateľa, obchodné meno, meno a priezvisko, ak sa líši od obchodného mena, identifikačné číslo alebo iný identifikačný údaj a miesto podnikania, 4.3 právnickú osobu, obchodné meno, identifikačné číslo alebo iný identifikačný údaj a sídlo, 5. označenie ustanoveného správcu alebo povereného správcu, 6. adresa kancelárie ustanoveného správcu alebo adresa kancelárie povereného správcu, 7. dátum začatia konkurzného konania, dátum začatia reštrukturalizačného konania alebo dátum poskytnutia ochrany pred veriteľmi, 8. dátum vyhlásenia konkurzu, dátum povolenia reštrukturalizácie alebo dátum určenia splátkového kalendára, 9. dátum zrušenia konkurzu alebo dátum skončenia reštrukturalizácie, 10. informácia o tom, či ide o malý konkurz, 11. údaje o uplatnených pohľadávkach v rozsahu obsahových náležitostí zoznamu pohľadávok, 12. údaje o uplatnených pohľadávkach proti podstate v rozsahu obsahových náležitostí evidencie pohľadávok proti podstate, 13. informácia o zostavení návrhu splátkového kalendára správcom, 14. údaje o majetku dlžníka v rozsahu obsahových náležitostí súpisu majetku podstát, 15. údaje o schôdzi veriteľov a údaje o zasadnutí veriteľského výboru pri konkurze podľa druhej časti tohto zákona v rozsahu miesto, čas a predmet rokovania schôdze veriteľov, meno a priezvisko veriteľa, ak ide o fyzickú osobu, alebo obchodné meno veriteľa, ak ide o právnickú osobu, informácia o tom, či veriteľ je členom veriteľského výboru, informácia o rozsahu hlasovacích práv veriteľa a zápisnica zo zasadnutia veriteľského výboru, 16. údaje o schôdzi veriteľov pri konkurze podľa štvrtej časti tohto zákona v rozsahu miesto, čas a predmet rokovania schôdze veriteľov, 17. rozvrh výťažku, 18. dátum rozhodnutia o oddĺžení, ak bol vyhlásený konkurz alebo určený splátkový kalendár podľa štvrtej časti tohto zákona, 19. informácia o zavedení dozornej správy, 20. informácie o lehotách pre účastníkov konania na vykonanie úkonov v konaniach podľa tohto zákona, 21. informácia o tom, či ide o hlavné insolvenčné konanie, vedľajšie insolvenčné konanie alebo o územné insolvenčné konanie podľa osobitného predpisu, 22. informácia o možnosti podať opravný prostriedok podľa osobitného predpisu, 23. miera uspokojenia zabezpečených veriteľov

zverejňované výlučne v obchodnom vestníku, ale *ex lege* poskytuje aj zoznam úpadcov v konkurze, zoznam dlžníkov v reštrukturalizačnom konaní, zoznam dlžníkov v konaniach vedených podľa štvrtej časti ZKR, ďalšie informácie o konaniach podľa ZKR zverejnené v obchodnom vestníku, či informácie o službách obstarávaných správcami.¹¹

Proces digitalizácie v oblasti insolvenčného práva sa samotným zavedením registra úpadcov neskončil. Rozsah v registri zverejňovaných údajov sa jednotlivými novelizáciami ZKR postupne rozširoval. S účinnosťou od 1.3.2017¹² bola Ministerstvu spravodlivosti SR zavedená povinnosť zverejňovať údaje o priemernej miere uspokojenia zabezpečených a nezabezpečených veriteľov v konaní podľa druhej a tretej časti ZKR. Povinne zverejňovanými sa stali aj štatistické údaje o konaniach podľa ZKR, údaje o priemernej dĺžke konania a nákladoch týchto konaní.¹³ Ide o veľmi dôležité údaje, ktoré poskytujú obraz o efektivite súdneho konania.¹⁴

Register úpadcov v súčasnosti poskytuje aj informačnú databázu o správcoch, taktiež komplexné informácie o konaniach jednotlivým správcom pridelených, pričom v rámci tejto časti registra nachádzame aj údaje o správcoch už vyčiarknutých zo zoznamu správcov.¹⁵ Konkrétne insolvenčné konania je možné z hľadiska ich druhu v registri úpadcov vyhľadávať aj podľa konajúcich súdov. Pre jeho užívateľov je užívateľsky komfortné aj rýchle vygenerovanie výpisu z registra úpadcov, potvrdzujúceho skutočnosť, či je, alebo nie je určitá fyzická či právnická osoba vedená v registri úpadcov¹⁶. Za negatívum však možno považovať skutočnosť, že vytvorením registra úpadcov došlo k vzniku systému duplicitného sprístupňovania rovnakých

a nezabezpečených veriteľov v konaniach vedených podľa druhej a tretej časti tohto zákona, 24. miera uspokojenia veriteľov v konaniach vedených podľa štvrtej časti tohto zákona."

¹¹ § 10a ods. 2 ZKR.

¹² Zákon č. 377/2016 Z. z., ktorým sa mení a dopĺňa zákon č. 7/2005 Z. z. o konkurze a reštrukturalizácii a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa dopĺňa zákon č. 327/2005 Z. z. o poskytovaní právnej pomoci osobám v materiálnej núdzi a o zmene a doplnení zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení zákona č. 8/2005 Z. z. v znení neskorších predpisov, účinný dňa 01.03.2017.

¹³ KUBINEC, Martin: Oddĺženie fyzickej osoby – neštandardné riešenie dlhovej pasce na slovenský spôsob. In: Neštandardné legislatívne zásahy štátu v neštandardných situáciách. Pocta profesorovi Milanovi Ďuricovi. Banská Bystrica: Belianum, 2023. s. 240 – 259. ISBN 978-80-557-2059-3.

¹⁴ ĎURICA, Milan: Zákon o konkurze a reštrukturalizácii, 4. vydanie. Bratislava: C. H. Beck, 2021. s. 47 – 53. ISBN 978-80-7400-846-7.

¹⁵ K podmienkam výkonu funkcie správcu: PATAKYOVÁ, Mária – MAMOJKA, Mojmír – DURAČINSKÁ, Jana: Hospodárske právo II. diel. Bratislava: Wolters Kluwer SR s.r.o., 2019. 309 s. ISBN 978-80-571-0090-4.

¹⁶ Pre získanie výpisu je potrebné navštíviť nasledovné webové sídlo: <https://ru.justice.sk/ru-verejnost-web/pages/vypis/vypisZRegistra.xhtml> [cit. 2025-09-17].

informácií súčasne v registri úpadcov aj v obchodnom vestníku. Túto duplicitu sa počas celej doby existencie registra úpadcov nepodarilo odstrániť.

Zásadnejšie zmeny z hľadiska rozsahu a charakteru údajov, zverejňovaných v registri úpadcov, zaviedol zákon č. 111/2022 Z. z. o riešení hroziaceho úpadku a o zmene a doplnení niektorých zákonov (ďalej ako „ZRHU“), ktorým došlo s účinnosťou od 17. júla 2022 k novelizácii ZKR. Postupná a systematická digitalizácia insolvenčného konania sa tak markantne dotkla aj spôsobu prihlasovania pohľadávok veriteľov v konkurznom aj v reštrukturalizačnom konaní. V oboch konaniach v súčasnosti podáva veriteľ prihlášku pohľadávky prostredníctvom na to určeného elektronického formulára¹⁷, použitím portálu slovensko.sk, priamo do elektronickej schránky príslušného správcu. Prihláška pohľadávky musí byť autorizovaná.¹⁸ Od 17. júla 2022 sa taktiež návrhy na vyhlásenie konkurzu a rovnako aj návrhy na povolenie reštrukturalizácie podávajú výlučne elektronickými prostriedkami do elektronickej schránky súdu, zároveň musia byť navrhovateľom autorizované, inak sa na ne neprihliada¹⁹. Autorizácia elektronického podania sa vykonáva niektorým zo spôsobov upravených v zákone č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)²⁰. Návrh na oddĺženie konkurzom, ako aj návrh na určenie splátkového kalendára podľa štvrtej časti ZKR sa podávajú výhradne elektronicky už od 1. januára 2018.²¹ Zoznam pohľadávok vedený správcom²² je už taktiež plne digitalizovaný a správca je povinný zostavovať, aktualizovať a viesť zoznam pohľadávok v registri úpadcov²³, ktorý je verejne prístupnou databázou údajov²⁴.

Podľa článku 24 ods. 1 Nariadenia o insolvenčnom konaní by mali členské štáty na svojom území viesť aspoň jeden register, v ktorom sa bezprostredne po začatí konkurzného konania zverejňujú informácie o konkurznom konaní. Povinnosť členských štátov zaviesť systém elektronického podávania a doručovania

¹⁷ § 25 Vyhláška č. 665/2005 Z. z. Ministerstva spravodlivosti Slovenskej republiky, ktorou sa vykonávajú niektoré ustanovenia zákona č. 7/2005 Z. z. o konkurze a reštrukturalizácii a o zmene a doplnení niektorých zákonov.

¹⁸ § 28 ods. 2 ZKR.

¹⁹ Bližšie pozri § 12 ods. 1 a § 112 ods. 1 ZKR.

²⁰ Bližšie pozri § 23 zákona o e-Governmente.

²¹ Zavedené Zákonom č. 264/2017 Z. z., ktorým sa mení a dopĺňa zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

²² DZIMKO, Jakub: Oddĺženie fyzickej osoby. 1. vydanie. Bratislava : C. H. Beck, 2024. s. 86. ISBN 978-80-8232-060-5.

²³ Podľa prechodných ustanovení ZKR (§ 206n ods. 4 ZKR) v konkurzoch vyhlásených a reštrukturalizáciách povolených do 16. júla 2022 zabezpečí správca zverejnenie zoznamu pohľadávok v registri úpadcov najneskôr do 31. januára 2023. Od zverejnenia zoznamu pohľadávok v registri úpadcov sa zoznam pohľadávok vedie prostredníctvom registra úpadcov.

²⁴ § 31 ZKR, § 123 ZKR.

dokumentov v rámci reštrukturalizačných, konkurzných a oddlžovacích konaní nevyplýva ani z Nariadenia o insolvenčnom konaní, ani zo Smernice Európskeho parlamentu a Rady (EÚ) 2019/1023 z 20. júna 2019 o rámcoch preventívnej reštrukturalizácie, o oddlžení a diskvalifikácii a o opatreniach na zvýšenie účinnosti reštrukturalizačných, konkurzných a oddlžovacích konaní a o zmene smernice (EÚ) 2017/1132 (ďalej ako „Smernica o reštrukturalizácii a insolvencii“)²⁵. Možno teda konštatovať, že Slovensko v oblasti insolvenčných konaní zavádza elektronizáciu iniciatívne v oblastiach, ktoré nie sú nadnárodnou úpravou vyžadované. Uvedené sa v plnom rozsahu dotýka aj sprístupňovania informácií o fyzických osobách. Aby bolo možné poskytnúť dostatočnú ochranu informácií, týkajúcich sa fyzických osôb, ktoré nie sú samostatne zárobkovo činné osoby, mal by mať slovenský register úpadcov, rovnako ako aj registre ostatných členských štátov možnosť podmieniť prístup k informáciám zadaním doplňujúcich kritérií vyhľadávania, ako je napríklad osobné identifikačné číslo dlžníka, adresa, dátum narodenia alebo obvod príslušného súdu, alebo podmieniť prístup podaním žiadosti príslušnému orgánu alebo overením oprávneného záujmu²⁶, čo však v slovenských podmienkach nie je realizované a zvýšenú ochranu tohto typu údajov register úpadcov neposkytuje.

Následne, v roku 2023, došlo zákonom č. 309/2023 Z. z. o premenách obchodných spoločností a družstiev a o zmene a doplnení niektorých zákonov k novelizovaniu ZKR a zavedeniu insolvenčného registra, ktorý má od 01. októbra 2025 nahradiť súčasný primárny zdroj informácií o konkurzných a reštrukturalizačných konaniach, t. j. register úpadcov. Insolvenčný register je zákonom charakterizovaný ako centralizovaný elektronický systém pre vedenie konkurzného konania, reštrukturalizačného konania, konania o oddlžení, konania o verejnej preventívnej reštrukturalizácii a konania o likvidácii a dodatočnej likvidácii.²⁷ Jeho súčasťou sa stanú aj údaje, ktoré boli zverejnené v registri úpadcov a v obchodnom vestníku podľa

²⁵ Recitál 91 Smernice o reštrukturalizácii a insolvencii: „Účastníci reštrukturalizačných, konkurzných a oddlžovacích konaní by nemali byť povinní používať prostriedky elektronickej komunikácie, ak takéto použitie nie je podľa vnútroštátneho práva povinné, pričom nie je dotknutá možnosť členských štátov zaviesť povinný systém elektronického podávania a doručovania dokumentov v rámci reštrukturalizačných, konkurzných a oddlžovacích konaní. Členské štáty by mali mať možnosť vybrať si prostriedok elektronickej komunikácie. Príklady takýchto prostriedkov by mohli zahŕňať špecializovaný systém na elektronické zasielanie takýchto dokumentov alebo používanie elektronickej pošty, pričom nie je dotknutá možnosť členských štátov zaviesť prvky na zaistenie bezpečnosti elektronického zasielania, ako napríklad elektronický podpis alebo dôveryhodné služby, ako sú elektronické doručovacie služby pre registrované zásielky v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 (17).“

²⁶ Recitál 79 Nariadenia o insolvenčnom konaní.

²⁷ Dôvodová správa k zákonu č. 298/2024 Z. z., ktorým sa mení zákon č. 309/2023 Z. z. o premenách obchodných spoločností a družstiev a o zmene a doplnení niektorých zákonov v znení zákona č. 530/2023 Z. z. a ktorým sa menia niektoré zákony.

predpisov účinných do jeho zavedenia.²⁸ Primárnym cieľom zákonodarcu pri zavádzaní nového registra bolo zjednotiť a elektronizovať insolvenčné procesy, zabezpečiť odstránenie elektronických bariér podnikania, zvýšiť transparentnosť, zrýchliť konania, ako aj znížiť čas a náklady potrebné na ukončenie podnikania. Údaje zverejňované v insolvenčnom registri by mali prispieť aj k zlepšeniu zberu údajov a kvality dát potrebných pre hodnotenie dotknutých procesov.

Insolvenčný register bude od svojho vzniku poskytovať evidenciu údajov o konkurzných konaniach a udalostiach, ktoré v nich nastali od vydania uznesenia o začatí konkurzného konania až po jeho ukončenie, ak ide o malý konkurz, od vydania uznesenia o vyhlásení malého konkurzu až po jeho ukončenie, údaje o reštrukturalizačných konaniach a udalostiach, ktoré v nich nastali od vydania uznesenia o začatí reštrukturalizačného konania až po jeho ukončenie, údaje o konaniach o oddlžení a udalostiach, ktoré v nich nastali od vydania uznesenia o vyhlásení konkurzu alebo uznesenia o povolení splátkového kalendára až po jeho ukončenie. Insolvenčný register bude nad rámec registra úpadcov poskytovať údaje o verejnej preventívnej reštrukturalizácii a udalostiach, ktoré nastali vo verejnej preventívnej reštrukturalizácii od vydania uznesenia o povolení verejnej preventívnej reštrukturalizácie až po jej ukončenie, údaje o likvidácii a dodatočnej likvidácii od vydania uznesenia súdu o ustanovení likvidátora až po jej ukončenie, ako aj ďalšie informácie o vyššie menovaných konaniach.²⁹

Evidencia insolvenčného registra bude vedená o fyzickej osobe v rozsahu meno, priezvisko, dátum narodenia a bydlisko, o fyzickej osobe – podnikateľovi v rozsahu obchodné meno, meno a priezvisko, ak sa líši od obchodného mena, identifikačné číslo organizácie alebo identifikačný údaj vydaný zahraničným registrom alebo zahraničnou evidenciou a miesto podnikania, o právnickej osobe v rozsahu obchodné meno, identifikačné číslo organizácie alebo identifikačný údaj vydaný zahraničným registrom alebo zahraničnou evidenciou a sídlo.³⁰ Údaje zverejnené v insolvenčnom registri nebude potrebné pred orgánmi verejnej moci a v obchodnom styku preukazovať.³¹

Cieľom zavedenia registra je prispieť k vytvoreniu transparentného a efektívneho procesného rámca predinsolvenčných, insolvenčných a reštrukturalizačných konaní.

Insolvenčné registre v okolitých krajinách

Vlastnosti insolvenčných registrov sa v jednotlivých štátoch líšia. Zatiaľ čo v niektorých členských štátoch existujú registre špeciálne určené na insolvenčnú, v

²⁸ § 206q Prechodné ustanovenia k úpravám účinným od 1. Októbra 2025.

²⁹ § 203b ZKR v znení účinnom od 01.10.2025.

³⁰ § 203b ods. 3 ZKR.

³¹ § 203b ods. 7 ZKR.

iných sú údaje týkajúce sa insolventnosti uvedené v registroch, ktoré spracovávajú aj iné typy údajov, a existujú aj markantné rozdiely v povahe sprístupnených údajov a informácií.³²

V Maďarsku zriadený insolvenčný register obsahuje údaje všetkých hospodárskych subjektov a mimovládnych organizácií, voči ktorým sa po 26. júni 2018 v Maďarsku začalo konkurzné konanie.³³

Nad rámec Nariadením o insolvenčnom konaní vyžadovaných informácií, maďarský insolvenčný register poskytuje aj nasledovné údaje:

- začatie a ukončenie odporovacích žalôb v súvislosti s majetkom dlžníka, názov príslušného súdu a číslo konania,
- začatie a ukončenie žalôb na určenie zodpovednosti členov štatutárneho orgánu dlžníka, bývalých členov štatutárneho orgánu, členov jeho právnickej osoby alebo majiteľov za činnosti z ich strany, ktoré viedli k poškodeniu záujmov veriteľov, názov príslušného súdu a číslo konania,
- informácia, či sa konanie viedlo vo forme zjednodušenej likvidácie.³⁴

Okrem povinných prvkov Nariadenie o insolvenčnom konaní umožňuje členským štátom uverejňovať dodatočné informácie v registri, ktoré Maďarsko využilo. V registri však nenachádzame informácie o konkurzoch fyzických osôb, ani podrobne štruktúrované informácie o prihlásených pohľadávkach a majetku úpadcu tak, ako to poskytuje slovenský register úpadcov.

V Poľsku sa až do 1. decembra 2021 dokumentácia týkajúca sa konkurzných a reštrukturalizačných konaní spracovávala v papierovej forme a oznámenia vyžadované zákonom sa uverejňovali v celoštátnom úradnom vestníku. Prvé práce na vývoji centrálného registra konkurzov a reštrukturalizácii sa v Poľsku začali už v novembri 2016. Register však nebol spustený, pretože bolo potrebné ho rozšíriť tak, aby umožňoval úplnú digitalizáciu reštrukturalizačných a konkurzných konaní. V roku 2018 tak bol Sejmu Poľskej republiky predložený návrh zákona o Národnom registri dlžníkov³⁵ (ďalej ako „KRZ“), ktorý nadobudol účinnosť o dva roky po jeho prijatí. Na oneskorenie spustenia registra mali vplyv okrem iného aj dočasné protipandemické opatrenia. Dlho očakávaný register dlžníkov začal fungovať 1. decembra 2021 a bol

³² TAJTI, Tibor: A new frontier: The challenges surrounding the deepening impact of data protection regulations on bankruptcy law. In: *Pravni zapisi*. Year XIV, Volume 2 (2023), p. 238-296. eISSN 2406-1387.

³³ Maďarský register konkurzov je k dispozícii na webovom sídle: <https://fizeteskeptelenseg.im.gov.hu/>. [cit. 2025-09-17].

³⁴ Zákon XLIX z roku 1991 o konkurznom a likvidačnom konaní. Dostupný na: <https://net.jogtar.hu/jogszabaly?docid=99100049.tv> [cit. 2025-09-17].

³⁵ Poľský celoštátny register dlžníkov je označený ako „*Krajowy Rejestr Zadłużonych (KRZ)*“ a v anglickej verzii ako „*National Debtors' Register (NDR)*“.

označovaný ako digitálny prevrat v poľskom justičnom systéme³⁶. Register je verejný a rovnako ako na Slovensku ho vedie Ministerstvo spravodlivosti. Poľský register dlžníkov zverejňuje údaje o prebiehajúcich reštrukturalizačných a konkurzných konaniach.³⁷ Nad rámec týchto informácií poskytuje aj údaje o konaniach o zákaze vykonávania podnikateľskej činnosti a tzv. neúspešných exekúciách, t. j. exekučných konaniach, v rámci ktorých bol výkon rozhodnutia zastavený z dôvodu nemajetnosti dlžníka, vrátane exekúcií na výživné a vymáhanie pohľadávok štátneho rozpočtu. V Českej republike zriadený insolvenčný register³⁸, spravovaný Ministerstvom spravodlivosti ČR, slúži na zaistenie maximálnej publicity insolvenčného konania a doručovanie väčšiny súdnych rozhodnutí a iných písomností. Insolvenčný register obsahuje zoznam správcov konkurznej podstaty, zoznam dlžníkov a konkurzné spisy. Pre každého dlžníka sa vedie jeden insolvenčný spis.³⁹ Vďaka prístupnému insolvenčnému registru má široká verejnosť prakticky okamžité informácie o tom, ktorý subjekt sa v insolvenčnom konaní, prípadne v úpadku nachádza.⁴⁰ Prostredníctvom registra sú zverejňované rozhodnutia insolvenčného súdu vydané v insolvenčnom konaní a v incidenčných sporoch, podania ktoré sa vkladajú do súdneho spisu, ako aj ďalšie informácie, pokiaľ tak ustanoví insolvenčný zákon alebo rozhodnutie insolvenčného súdu.⁴¹ Dlžník, jeho veritelia aj verejnosť majú možnosť sledovať priebeh konania krok za krokom prostredníctvom diaľkového prístupu.⁴² Česká právna úprava však poskytuje zvýšenú ochranu osobných údajov fyzických osôb, pretože na žiadosť môže insolvenčný súd rozhodnúť, že niektoré z osobných údajov žiadateľa, obsiahnuté v podaní, nebudú v insolvenčnom registri verejne prístupné.⁴³ Na rozdiel od slovenskej právnej úpravy, do insolvenčného registra sa počas nevyhnutnej doby nevkladajú ani podania a písomnosti, ktorých okamžité

³⁶ ZAREMBA, Ulyana: Evolution of the preventive restructuring framework in Poland. In: Thematic Collection of Works From the International Scientific Conference The reform of legislation on restructuring, reorganisation and insolvency in the light of european tendencies. Pale: GRAFOMARK d.o.o, Laktaši, 2023. p. 87 – 104. ISBN 978-99938-57-72-3.

³⁷ ADAMUS, Rafal: Liquidation of the Bankruptcy Estate in Poland. In: Bratislava Law Review. Bratislava: Comenius University Bratislava, Faculty of Law, Vol. 4, No 1 (2020). p.115-130. ISSN 2644-6359.

³⁸ Insolvenčný register je v Českej republike zriadený od roku 2014, pôvodne obsahoval stručné informácie o tom, či bolo voči určitej osobe vedené insolvenčné konanie, bez podrobných informácií o priebehu konania a bez zverejňovania príslušných dokumentov.

³⁹ § 419 ods. 2 zákona č. 182/2006 Sb. o úpadku a spôsoboch jeho řešení (insolvenční zákon).

⁴⁰ SPRINZ, Petr – JIRMÁSEK, Tomáš a kol.: Insolvenční zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2019, 1177 s. ISBN 978-80-7400-753-8.

⁴¹ Insolvenční rejstřík. Dostupné na internete: <https://portal.gov.cz/informace/insolvenčni-rejstrik-INF-128>. [cit. 2025-09-17].

⁴² KOZÁK, Ján – BROŽ, Jaroslav a kol.: Insolvenční zákon. Komentář. 5. vydání. Praha: Wolters Kluwer ČR, 2019, s. 1580. ISBN 978-80-7598-578-1.

⁴³ § 422 zákona č. 182/2006 Sb. o úpadku a způsobech jeho řešení (insolvenční zákon).

zverejnenie by marilo účel konania ako aj utajované informácie.⁴⁴ Na žiadosť vydá Ministerstvo spravodlivosti ČR alebo insolvenčný súd úradne overený výstup z informačného systému verejnej správy obsahujúci údaje z insolvenčného registra alebo informáciu o tom, že požadovaný údaj nie je vedený v insolvenčnom registri.⁴⁵ Insolvenčný register bol v Českej republike vo verzii údajov vyžadovaných Nariadením o insolvenčnom konaní sprístupnený v júni 2020, čím nahradil, resp. zdokonalil insolvenčný register zavedený v online priestore už v roku 2016. Následne bol register rozširovaný o nové funkcionality, vrátane formulárov na zahájenie jednotlivých konaní, ktoré v súčasnosti ponúka.

Komparáciou údajov, poskytovaných insolvenčnými registrami susedných krajín (t. j. krajín V4) možno skonštatovať, že digitalizácia v tejto oblasti práva je v súčasnosti vo všetkých porovnávaných krajinách realizovaná nad rámec požiadaviek na prístup k údajom vyžadovaným Nariadením o insolvenčnom konaní. Nespornými výhodami progresívne prebiehajúcej digitalizácie údajov a elektronizácie postupov v insolvenčnom práve je zvýšenie transparentnosti konkurzných a reštrukturalizačných konaní prostredníctvom online prístupu k údajom a súdnym spisom a zároveň urýchlenie konaní, odstránenie časových prieťahov pri doručovaní korešpondencie a zároveň uľahčenie prístupu širokej verejnosti k spisom reštrukturalizačných a konkurzných konaní. Možno sa domnievať, že práve tieto dôvody sú hlavným motivátorom digitalizácie stále narastajúceho okruhu údajov i insolvenčných a súvisiacich konaní v komparovaných krajinách. Sprístupňované informácie môžu vyrovnávať informačnú asymetriu medzi dlžníkom, veriteľmi, prípadne ďalšími potenciálnymi účastníkmi trhu a môžu tak významne ovplyvňovať rozhodovanie jednotlivých subjektov.⁴⁶

Publicita údajov registra úpadcov, ktorú elektronizácia konaní poskytuje nesporne prispieva k hospodárnosti konania, formálnemu zjednodušeniu konania a tým jeho zrýchleniu, a teda nižším nákladom na strane štátu aj veriteľov. Účinné a harmonizované pravidlá insolvenčného práva a jasné pravidlá platobnej neschopnosti sú v širšom kontexte považované aj za kľúčové kritériom pre cezhraničných investorov.⁴⁷

⁴⁴ § 432 zákona č. 182/2006 Sb. o úpadku a spôsoboch jeho řešení (insolvenční zákon).

⁴⁵ § 419 ods. 4 zákona č. 182/2006 Sb. o úpadku a spôsoboch jeho řešení (insolvenční zákon).

⁴⁶ SPRINZ, Petr – JIRMÁSEK, Tomáš a kol.: Insolvenční zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2019, 1177 s. ISBN 978-80-7400-753-8.

⁴⁷ DIDEA, Ionel – ILIE, Diana Maria: Increasing Legal Certainty for Cross - Border Investments by Making National Insolvency Procedures More Efficient and Effective. In: [International Investment Law Journal](#). Issue No. 1, Vol. 4/2024, s. 30-70.

Nástrahy digitalizácie v oblasti insolvenčného práva

Digitalizácia údajov a zavádzanie nových informačných technológií má neodškriepiteľne pozitívny dopad na fyzické aj právnické osoby. Zároveň možno na technický pokrok nahliadať i cez optiku väčšej zraniteľnosti dotknutých osôb.⁴⁸ Preto je zásadné pokročiť aj v oblasti kybernetickej a informačnej bezpečnosti, pretože zlepšenie jej úrovne má schopnosť posilniť oslabenú dôveru slovenských občanov v moderné technológie.⁴⁹

Vďaka rozšírenému geografickému dosahu údajov, ktoré sa stávajú ľahko dostupnými, je možné ich jednoduchým spôsobom nielen získať, spracovávať ale aj zneužívať. Z tohto dôvodu, najmä s prihliadnutím na neustále narastajúci rozsah údajov sprístupňovaných v registri úpadcov resp. pripravovanom insolvenčnom registri vzniká veľmi tenká a nejasná hranica medzi digitalizáciou údajov v insolvenčnom práve a ochranou osobných údajov⁵⁰, ktorá je vystavovaná novým druhom hrozieb. Vzťah medzi transparentnosťou a verejnosťou insolvenčných konaní na jednej strane a zásahom do práv veriteľov, či samotných úpadcov v súvislosti s verejnou dostupnosťou údajov o nich na strane druhej, bude podľa nášho názoru ešte oblasťou vyvolávajúcou nielen právne polemiky, ale možno aj súdne konania.

Charakter insolvenčného registra ako oficiálneho a verejne prístupného elektronického spisu nutne vedie k dôsledkom, ktoré nemožno opomenúť. Jedným z nich je skutočnosť, že ako verejnosť, tak i podnikateľské subjekty iba čiastočne rozlišujú stav zapísania dlžníka do insolvenčného registra v reakcii na podanie insolvenčného návrhu, a teda zahájenia insolvenčného konania, od stavu preukázaného a súdom konštatovaného úpadku.⁵¹ V určitom množstve prípadov totiž nie je preukázaný úpadok dlžníka, informácie uvádzané v návrhu na vyhlásenie konkurzu sa preukážu ako nepresné, nedostatočné, či dokonca nepravdivé. Vývoj

⁴⁸ ŠVEC, Marek – HORECKÝ, Ján – MÉSZÁROS, Peter: Impact of Digitalization, Platformisation (and other factors) on Labour Law and the Labour Market. 1st edition. Hürth : Wolters KluwerDeutschland, 2023, 130 s. ISBN 978-3-452-30406-3.

⁴⁹ TREŠČÁKOVÁ, Diana – HUČKOVÁ, Regina: Neštandardná situácia ako hnací motor pre digitalizáciu a modernizáciu podnikania. In: Neštandardné legislatívne zásahy štátu v neštandardných situáciách. Pocta profesorovi Milanovi Ďuricovi. Banská Bystrica: Belianum, 2023. s 358. ISBN 978-80-557-2059-3.

⁵⁰ CUKEROVÁ, Dominika – MRÁZOVÁ, Žofia: The digital transformation of Slovak insolvency law: a review of digital changes and challenges. In: Evolution of Private Law. Nex technologies. Katovice: IUS PUBLICUM Publishing House , 2025. s. 12-25. ISBN 978-83-66922-31-0.

⁵¹ SCHÖNFELDOVÁ, Dagmar – SCHÖNFELD, Jaroslav: Vliv zásady publicity na ekonomiku dlužníka a možnosti korekce dopadů pomocí postupů public relations. In: Insolvenční praxe (Problémy a výzvy pro léta dvacátá). 1. vydání. Praha : C. H. Beck, 2020, s. 88. ISBN 978-80-7400-780-4.

legislatívy však ukazuje⁵², že po každom novom pokuse o odstránenie šikanózných návrhov sa objavili vždy prepracovanejšie postupy, ako zásadu publicity zneužiť buď v rámci konkurenčného boja alebo v rámci vynútenia plnenia.⁵³

V súvislosti s uvedenými polemikami sa naskytá legitímna otázka, komu majú byť údaje z insolvenčných registrov prístupné, v akom rozsahu a na aké účely? Obdobnú otázku riešil Súdny dvor Európskej únie vo veci plošného odhaľovania informácií o konečných užívateľoch výhod, pričom jeho rozhodnutie v spojených veciach C-37/20 WM a C-601/20 Sovim SA/Luxemburg Business Register zo dňa 22. novembra 2022 obmedzuje možnosť verejnej dostupnosti údajov o konečných užívateľoch výhod.⁵⁴ Súdny dvor Európskej únie vzal do úvahy verejný záujem sledovaný zverejňovaním údajov o konečných užívateľoch výhod vo vzťahu k boju proti praniu špinavých peňazí na jednej strane a zásah do základných práv na súkromie a ochranu osobných údajov a potencionálne riziká a nebezpečenstvá, ktoré z takéhoto zásahu vyplývajú, na strane druhej. Poukázal na to, že negatíva, ktoré plošné zverejňovanie identity konečného užívateľa výhod prináša, značne prevyšujú verejný záujem spoločnosti na odkrývaní totožnosti utajovaných beneficentov. Súdny dvor Európskej únie považoval takýto zásah do práva na súkromie za príliš ofenzívny, ktorý nebol proporcionálny k úžitkom, ktoré takéto intervencie do práv prinášajú (riziko vydierania, zastrašovania, obťažovania, alebo iného druhu násillia). Rozhodnutie Súdneho dvora Európskej únie je záväzné pre všetky členské štáty, preto už v súčasnosti nenájdeme v registri právnických osôb plošne sprístupnené údaje o konečných užívateľoch výhod.

Nemožno opomínať ani to, že vplyv a dosah umelej inteligencie sú všadeprítomné⁵⁵. Zatiaľ však nezasahuje do procesných a ani rozhodovacích úkonov súdov, hoci polemiky o súčasných a potenciálnych budúcich schopnostiach umelej inteligencie

⁵² Podľa ustanovenia § 11 ods. 4 ZKR: „Ak súd konkurzné konanie začaté na základe návrhu veriteľa na vyhlásenie konkurzu zastaví z dôvodu osvedčenia platobnej schopnosti dlžníka, veriteľ zodpovedá dlžníkovi, ako aj iným osobám za škodu, ktorá im v súvislosti s účinkami začatia konkurzného konania vznikla, ibaže preukáže, že pri podávaní návrhu na vyhlásenie konkurzu postupoval s odbornou starostlivosťou. Táto zodpovednosť sa rovnako vzťahuje aj na štatutárny orgán alebo člena štatutárneho orgánu, ktorý rozhodol v mene veriteľa o podaní návrhu na vyhlásenie konkurzu.“

⁵³ SCHÖNFELDOVÁ, Dagmar – SCHÖNFELD, Jaroslav: Vliv zásady publicity na ekonomiku dlužníka a možnosti korekce dopadů pomocí postupů public relations. In: Insolvenční praxe (Problémy a výzvy pro léta dvacátá). 1. vydání. Praha : C. H. Beck, 2020, s. 89. ISBN 978-80-7400-780-4.

⁵⁴ KUBINEC, Martin – UŠIAKOVÁ, Lenka – DZIMKO, Jakub - KRIŠTIAKOVÁ Klára: Vplyv rozhodnutia Súdneho dvora Európskej únie vo veci plošného odhaľovania informácií o konečných užívateľoch výhod na právny poriadok Slovenskej republiky. In: Právny obzor : teoretický časopis pre otázky štátu a práva, Roč. 106, č. 5 (2023), s. 447-460.

⁵⁵ K využitiu umelej inteligencie v kontexte arbitráže pozri: WASIQ, Dar - PRAŠTALO, Boris: The investor state arbitration legitimacy crisis: could AI be its future savior (or resurrector)? In: Právni zapisi. Year XIV, Volume 1 (2023), p. 21-58.

v týchto oblastiach už existujú. Stretávame sa s názormi, že práve oblasť konkurzného práva môže byť novými technológiami ovplyvnená rýchlejšie ako iné oblasti práva, a to z dôvodu, že konkurzné právo úzko súvisí s účtovníctvom a financiami, a teda s oblasťami, v ktorých sú už v súčasnosti vo veľkej miere systémy umelej inteligencie využívané⁵⁶. Svoje miesto si nové informačné technológie už našli napríklad v oblasti predikcie hroziaceho úpadku⁵⁷, či v systémoch zameraných na urýchlenie insolvenčných konaní, čo môže sekundárne prispieť k vyššej miere uspokojenia veriteľov. Záverom si dovoľíme položiť otázku pre ďalšiu polemiku, či vstup umelej inteligencie do plne digitalizovaných a elektronizovaných insolvenčných konaní bude v budúcnosti schopný v plnej miere nahradiť úlohu konkurzného správcu?

Záver

Narastajúca digitalizácia v oblasti insolvenčného práva umožňuje rýchly prístup k informáciám o insolvenčných konaniach, či k štatistickým údajom o nich. Zároveň vytvára podmienky pre nové nástrahy spojené s digitalizáciou údajov. Vzniká tenká hranica medzi digitalizáciou údajov v insolvenčnom práve a ochranou osobných údajov, ktorá je tak vystavovaná novým druhom hrozieb.

Analýzou rozsahu a charakteru údajov sprístupňovaných v registri úpadcov a novom insolvenčnom registri sme dospeli k názoru, že je potrebné venovať zvýšenú pozornosť aj problematike nevyhnutnosti, účelnosti a rozsahu zverejňovania informácií o fyzických a právnických osobách, ktoré sú súčasťou sprístupňovaných insolvenčných spisov. Naskytá sa otázka, či je nevyhnutné plošne sprístupňovať v insolvenčnom registri tak veľké množstvo údajov. Údaje, uvádzané napríklad v prihláške pohľadávky veriteľa môžu obsahovať citlivé účtovné, či obchodné informácie. Nevyriešenou je tiež otázka nutnosti sprístupňovať v plnom rozsahu už ukončené konania a po aký dlhý čas, pretože právna úprava sa tejto problematike, resp. právu na zabudnutie legálne zverejnenej informácie v oblasti insolvenčného práva na Slovensku doposiaľ nevenuje.⁵⁸ Odpovede na nastolené otázky prinesie až ďalšia precizácia právnej úpravy, prípadne rozhodovacia činnosť súdov.

⁵⁶ HENKEL, Christoph: Chapter 20: The impact of artificial intelligence on insolvency law and practice. In: Research Handbook on Corporate Restructuring, Glos: Edward Elgar Publishing Limited, 2021. p. 377-399 eISBN: 9781786437471.

⁵⁷ Aplikácia Finanční zdraví dostupná na Webovom sídle: <https://eformulare.justice.cz/msp-financni-zdravi/form/uvod>. [cit. 2025-09-17].

⁵⁸ K právu na zabudnutie bližšie: PL. ÚS 10/2014, PL. ÚS 13/2020, Google Spain SL a Google Inc. Proti Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

Zoznam použitej literatúry

1. ADAMUS, Rafal: Liquidation of the Bankruptcy Estate in Poland. In: Bratislava Law Review. Bratislava: Comenius University Bratislava, Faculty of Law, Vol. 4, No 1 (2020), s.115-130.
2. CUKEROVÁ, Dominika – MRÁZOVÁ, Žofia: The digital transformation of Slovak insolvency law: a review of digital changes and challenges. In: Evolution of Private Law. Nex technologies. Katovice: IUS PUBLICUM Publishing House , 2025. s. 12-25. ISBN 978-83-66922-31-0.
3. DIDEA, Ionel – ILIE, Diana Maria: Increasing Legal Certainty for Cross - Border Investments by Making National Insolvency Procedures More Efficient and Effective. In: [International Investment Law Journal](#). Issue No. 1, Vol. 4/2024, p. 30-70.
4. ĎURICA, Milan: Zákon o konkurze a reštrukturalizácii, 4. vydanie. Bratislava: C. H. Beck, 2021. 1496 s. ISBN 978-80-7400-846-7.
5. DZIMKO, Jakub: Oddĺženie fyzickej osoby. 1. vydanie. Bratislava : C. H. Beck, 2024. 235 s. ISBN 978-80-8232-060-5.
6. HENKEL, Christoph: Chapter 20: The impact of artificial intelligence on insolvency law and practice. In: Research Handbook on Corporate Restructuring, Glos: Edward Elgar Publishing Limited, 2021. 584 s. eISBN: 9781786437471.
7. IKRÉNI, Ivan: Nariadenie o insolvenčnom konaní. Komentár. Bratislava: C. H. Beck, 2020. 1016 s. ISBN 978-80-89603-82-4.
8. KOZÁK, Ján – BROŽ, Jaroslav a kol: Insolvenční zákon. Komentář . 5. vydání. Praha: Wolters Kluwer ČR, 2019. s. 1580. ISBN 978-80-7598-578-1.
9. KUBINEC, Martin: Oddĺženie fyzickej osoby – neštandardné riešenie dlhovej pasce na slovenský spôsob. In: Neštandardné legislatívne zásahy štátu v neštandardných situáciách. Pocta profesorovi Milanovi Ďuricovi. Banská Bystrica: Belianum, 2023. s 240 – 259. ISBN 978-80-557-2059-3.
10. KUBINEC, Martin – UŠIAKOVÁ, Lenka – DZIMKO, Jakub - KRIŠTIAKOVÁ Klára: Vplyv rozhodnutia Súdneho dvora Európskej únie vo veci plošného odhaľovania informácií o konečných užívateľoch výhod na právny poriadok Slovenskej republiky. In: Právny obzor : teoretický časopis pre otázky štátu a práva, Roč. 106, č. 5 (2023), s. 447-460.
11. MADLEŇÁK, Adam – ŠVEC, Marek: The right to communicate on digital platforms and its impact on boosting their global reach. In: Globalization and its socio-economic consequences: 22th international scientific conference. Žilina: Žilinská univerzita v Žiline, 2022. s. 872-880. ISBN 978-80-8154-332-6.
12. PATAKYOVÁ, Mária – MAMOJKA, Mojmir – DURAČINSKÁ, Jana: Hospodárske právo II. diel. Bratislava: Wolters Kluwer SR s.r.o., 2019. 309 s. ISBN 978-80-571-0090-4.

13. SCHÖNFELDOVÁ, Dagmar – SCHÖNFELD, Jaroslav: Vliv zásady publicity na ekonomiku dlužníka a možnosti korekce dopadů pomocí postupů public relations. In: Insolvenční praxe (Problémy a výzvy pro léta dvacátá). 1. vydání. Praha : C. H. Beck, 2020. 210 s. ISBN 978-80-7400-780-4.
14. SPRINZ, Petr – JIRMÁSEK, Tomáš a kol.: Insolvenční zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2019. 1177 s. ISBN 978-80-7400-753-8.
15. TAJTI, Tibor: A new frontier: The challenges surrounding the deepening impact of data protection regulations on bankruptcy law. In: Právni zapisi. Year XIV, Volume 2 (2023), s. 238-296.
16. TREŠČÁKOVÁ, Diana – HUČKOVÁ, Regina: Neštandardná situácia ako hnací motor pre digitalizáciu a modernizáciu podnikania. In: Neštandardné legislatívne zásahy štátu v neštandardných situáciách. Pocta profesorovi Milanovi Ďuricovi. Banská Bystrica: Belianum, 2023. s 353 – 364. ISBN 978-80-557-2059-3.
17. VEDER, Michael: *Article 24— Establishment of insolvency registers* In: *Commentary on the European Insolvency Regulation*. Second Edition. Online. Oxford: Oxford University Press, 2022. 1136 s. ISBN 978-01-91915-06-2.
18. WASIQ, Dar - PRAŠTALO, Boris: The investor state arbitration legitimacy crisis: could AI be its future savior (or resurrector)?. In: Právni zapisi. Year XIV, Volume 1 (2023), p. 21-58. eISSN 2406-1387.
19. ZAREMBA, Ulyana: Evolution of the preventive restructuring framework in Poland. In: Thematic Collection of Works From the International Scientific Conference The reform of legislation on restructuring, reorganisation and insolvency in the light of european tendencies. Pale: GRAFOMARK d.o.o, Laktaši, 2023. s. 87 – 104.

Kontaktné údaje

JUDr. Aneta Kšenžighová, PhD., MBA

ksenzighova1@uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Katedra obchodného práva a hospodárskeho práva

DIGITALIZÁCIA INSOLVENČNÉHO KONANIA PROSTREDNÍCTVOM INSOLVENČNÉHO REGISTRA

DIGITALIZATION OF INSOLVENCY PROCEEDINGS THROUGH THE INSOLVENCY REGISTER

Martin Spišák¹

Abstrakt: Elektronizácia a digitalizácia sú trendmi súčasnosti a budúcnosti, pričom sa nevyhli ani obchodnému a konkurznému právu. Zavedenie elektronizácie a digitalizácie sa stáva nevyhnutým a efektívnym spôsobom napredovania. Autor sa v príspevku venuje novému Insolvenčnému registru, ktorý by mal elektronickou formou sprístupniť a zjednodušiť prístup k informáciám týkajúcich sa predinsolvenčných, insolvenčných a likvidačných konaní. Vyvstáva tu niekoľko otázok. Dôjde tak k nahradeniu aktuálneho Registra úpadcov? Bude nový Insolvenčný register prepojený s Obchodný vestníkom? Aké výhody prinesie? Čo bude jeho obsahom? Cieľom príspevku je analyzovať pozitívne a negatívne aspekty nového Insolvenčného registra, ktorý má byť v prevádzke od 01.10.2025, vo svetle doterajšej praxe konkurzného konania, efektívnosti a transparentnosti. Autor sa pokúsi zachytiť dosah nového Insolvenčného registra na súdy, správcov konkurznej podstaty, úpadcov či veriteľov a posúdi, či bude prínosom. Insolvenčný register nadväzuje na elektronizáciu vo verejnej a štátnej správe, pričom odráža potrebu aplikácie právnych noriem Európskej únie, ktorá harmonizuje elektronické registre jej členských štátov.

Kľúčové slová: konkurz, insolvenčné konanie, insolvenčný register, transparentnosť

Abstract: Electronization and digitalization are trends of the present and the future, and commercial and insolvency law has not escaped them. The introduction of electronicization and digitalization is becoming an inevitable and necessary way of progressing. The author of the article discusses the new Insolvency Register, which should make information regarding pre-insolvency, insolvency and liquidation proceedings available and simplify access to them in electronic form. Several questions arise here. Will this replace the current Register of Bankrupts? Will the new Insolvency Register be linked to the

¹ Univerzita Komenského v Bratislave, Katedra obchodného a hospodárskeho práva

Commercial Gazette? What benefits will it bring? What will its content be? The aim of the article is to analyze the positive and negative aspects of the new Insolvency Register, which should be in operation from 01.10.2025, in light of the current practice of bankruptcy proceedings, efficiency and transparency. The author will attempt to capture the impact of the new Insolvency Register on courts, bankruptcy trustees, bankrupts, and creditors and assess whether it will be beneficial. The insolvency register follows the process of electronic registration to apply the legal standards of the European Union, which harmonizes the electronic registers of its member states.

Key words: Bankruptcy proceedings, insolvency proceedings, insolvency register, transparency

Úvod

Digitalizácia vo verejnej a štátnej správe je obrovským trendom, ktorý postupuje a nedá sa zabrzdiť. Zapojenie výpočtovej techniky a moderných technológií do práce a agendy súdov, advokátov, orgánov činných v trestnom konaní, notárov, exekútorov, okresných úradov a aj iných orgánov nepochybne uľahčilo a zvýšilo efektivitu práce mnohým ľuďom, pričom zároveň došlo aj ku zvýšeniu transparentnosti postupov a konaní v štátnej správe. Postupne pribudla elektronizácia Obchodného registra, Obchodného vestníka, eTrhoviska, Elektronického súdneho spisu, Slovenska (www.slovensko.sk) či Finančnej správy Slovenskej republiky. Nakoniec sme sa dočkali od 01.01.2016 a 01.07.2016 (spustenie bolo postupné) aj Registra úpadcov, ktorý síce konkurzné konanie digitalizoval, však nezaviedol jeho úplnú elektronizáciu. To má nastať až spustením Insolvenčného registra.

Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní v čl. 24 bode 1 ustanovilo povinnosť pre členské štáty Európskej únie vytvoriť a viesť register, ktorý obsahuje informácie o insolvenčnom konaní, vrátane špecifikácie týchto údajov. V ďalšom čl. 25 sa zaviedla povinnosť vzájomného prepojenia týchto registrov, t.j. vytvorenie decentralizovaného systému.²

Nariadenie predpokladá, že insolvenčné registre budú verejne dostupné, inak sa nezlepší poskytovanie informácií príslušným veriteľom a súdom a nezabráni sa začatiu súbežných insolvenčných konaní. Predchádzajúce uverejnenie povinných

² Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní

informácií nie je podmienkou pre automatické uznávanie zahraničných insolvenčných konaní podľa čl. 19 Nariadenia (recitál 75).³

Register úpadcov

Register úpadcov je informačný systém verejnej správy prístupný na webovom sídle Ministerstva vnútra Slovenskej republiky. Na webovej stránke Ministerstva spravodlivosti Slovenskej republiky sa uvádza: „*Informačný systém Register úpadcov obsahuje informácie o konkurzných a reštrukturalizačných konaniach podľa § 10a ods. 2 zákona č. 7/2005 Z. z. o konkurze a reštrukturalizácii a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Údaje v Registri úpadcov vznikajú kombináciou dát z informačných systémov súdov, Obchodného vestníka a Registra správcov.*“⁴

Profesor Ďurica uvádza: „*V záujme zvýšenia transparentnosti konaní upravených v KR a kontroly činnosti jednotlivých procesných subjektov (správca, súd a veriteľské orgány) bol zavedený register úpadcov, ktorý poskytuje kompletné informácie o konkurznom konaní, o reštrukturalizačnom konaní a o konaní o oddĺžení. Ide o rozšírenú formu zverejňovania relevantných skutočností, ktorá bola do prijatia tejto právnej úpravy zabezpečená zverejňovaním súdnych rozhodnutí a iných písomností súdu, správcu a veriteľských orgánov v Obchodnom vestníku. Povinnosť zriadiť insolvenčný register vyplýva pre členské štáty z nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní. Toto nariadenie v čl. 24 stanovuje údaje, ktoré musia byť zverejnené v insolvenčnom registri. V čl. 25 vyžaduje nariadenie vzájomné prepojenie insolvenčných registrov jednotlivých členských štátoch. Tento článok sa uplatňuje v členských štátoch od 26. júna 2019. Vytvorenie, údržba a budúci vývoj systému vzájomného prepojenia sa financuje zo všeobecného rozpočtu Únie (čl. 26). Členské štáty musia zabezpečiť bezplatný prístup k insolvenčným registrom.*“⁵

Register úpadcov obsahoval údaje o konkurznom alebo reštrukturalizačnom konaní, vrátane oddĺženia (napr. konajúci konkurzný súd, sudca, správca, navrhovateľ, dlžník, spisová značka konania, dátum začatia konania, dátum skončenia konania a ďalšie) ako aj údaje týkajúce sa veriteľov (uplatnené pohľadávky, pohľadávky proti podstate, lehoty na vykonanie úkonov).⁶

Po novele zákonom č. 377/2016 Z. z. sa zverejňovali aj údaje o priemernej miere uspokojenia zabezpečených a nezabezpečených veriteľov v konaní podľa druhej a tretej časti zákona č. 7/2005 Z. z. (ďalej len „Zákona č. 7/2005 Z. z.“), ako aj ďalšie

³ IKRÉNYI, Ivan. Čl. 24 Vytvorenie insolvenčných registrov. In: IKRÉNYI, Ivan. Nariadenie o insolvenčnom konaní. 1. vydanie. Bratislava: C. H. Beck, 2020, s. 413. ISBN: 978-80-89603-82-4.

⁴ <https://ru.justice.sk/ru-verejnost-web/public/oRegistriUpadcov.xhtml>

⁵ ĎURICA, Milan. § 10a [Register úpadcov]. In: ĎURICA, Milan. Zákon o konkurze a reštrukturalizácii. 4. vydanie. Praha: C. H. Beck, 2021, s. 52. ISBN: 978-80-7400-846-7.

⁶ ĎURICA, Milan. § 10a [Register úpadcov]. In: ĎURICA, Milan. Zákon o konkurze a reštrukturalizácii. 4. vydanie. Praha: C. H. Beck, 2021, s. 52. ISBN: 978-80-7400-846-7.

štatistické údaje o konaniach podľa Zákona č. 7/2005 Z.z. Zákonom č. 264/2017 Z. z. došlo k podstatnému rozšíreniu údajov, ktoré sa zverejňujú v Registri dlžníkov. Ide predovšetkým o informácie o zasadnutiach schôdze veriteľov a veriteľského výboru, rozvrhu výťažku, informácie o cezhraničných konkurzoch a ďalších.⁷

V zásade sa preto v Registri úpadcov zverejňovali informácie o:

- konkurznom konaní,
- reštrukturalizácii,
- oddĺžení (týka sa len fyzických osôb),
- incidenčných sporoch (vyvolané konkurzom, napr. o vylúčenie majetku zo súpisu),
- informáciách z agend spravovaných súdmi a ministerstvom.

Do samotného Registra úpadcov bolo možné sa prihlásiť prostredníctvom občianskeho preukazu s čipom a čítačky kariet. Nebolo však možné priamo komunikovať so správcom konkurznej podstaty a konkurzným súdom. To bolo možné len prostredníctvom portálu www.slovenko.sk a na to určených formulárov alebo prostredníctvom všeobecného podania. Časť Registra úpadcov bola verejná a druhá časť bola prístupná len pre správcov konkurznej podstaty a súdy.

Nový Insolvenčný register

Od 01.10.2025 má byť v prevádzke nový Insolvenčný register na základe novely zákona č. 309/2023 Z. z. o premenách obchodných spoločností a družstiev a o zmene a doplnení niektorých zákonov. Pôvodne mal byť tento zákon účinný od 01.08.2023, avšak údajne termín nebol naplnený z dôvodu nezrovnalostí vo verejnom obstarávaní, čo znamenalo posunutie termínu spustenia jeho prevádzky. Tento informačný systém bol vytvorený na základe realizácie plánu Obnovy a odolnosti, v rámci mílnika č. 14 – Zlepšenie podnikateľského prostredia, konkrétne realizáciou investície č. 2: Digitalizácia procesov insolvenčného konania.⁸ Insolvenčný register je upravený v § 203b Zákona č. 7/2005 Z. z.

Insolvenčný register nahradí kompletne Register úpadcov, nakoľko s účinnosťou od 01.10.2025 zo Zákona č. 7/2005 Z. z. bude táto právna úprava úplne odstránená. Zároveň v dôvodovej správe absentuje akékoľvek odôvodnenie ustanovení týkajúcich sa Insolvenčného registra, preto z tejto dôvodovej správy čerpať nemôžeme. Pokladáme za zvláštne a nedostatočné, že sa navrhovateľ zákona vôbec neodôvodnil prijatie Insolvenčného registra v dôvodovej správe.

⁷ ĎURICA, Milan. § 10a [Register úpadcov]. In: ĎURICA, Milan. Zákon o konkurze a reštrukturalizácii. 4. vydanie. Praha: C. H. Beck, 2021, s. 53. ISBN: 978-80-7400-846-7.

⁸ <https://www.justice.gov.sk/tlacovespravy/register-predinsolvencných-likvidacných-a-insolvencných-konaní/>

Tak ako Register úpadcov, aj Insolvenčný register bude informačným systémom verejnej správy, ktorý obsahuje údaje podľa Zákona č. 7/2005 Z. z., a ktorého správcom a prevádzkovateľom je Ministerstvo spravodlivosti Slovenskej republiky a bude sprístupnený na jeho webovom sídle. Celkovo je hlavná časť Insolvenčného registra rozdelená na 11 okien, ktoré umožňujú vyhľadať konania, majetok na predaj, obstarávacie služby, správcov, konkurzné súdy, štatistické informácie REPLIK výpis z REPLIK, podania – formuláre, nástroje včasného varovania, sudcov a dashboard. Po otvorení jednotlivých konaní však nie je umožnený prístup k jednotlivým dokumentom resp. súborom. Je možné zistiť množstvo insolvenčných konaní, kto sú správcovia, spisové značky, údaje dlžníkov, konkurznú podstatu, schôdze veriteľov a iné. V jednotlivých konaniach, resp. spisoch sú všetky informácie, vrátane označenia lehôt v konaní napr. na prihlásenie pohľadávok alebo ich popretie a podobne.

Výhody Insolvenčného registra:

- i. vyššia transparentnosť – všetky informácie budú dostupné na jednom mieste,
- ii. rýchlejšie konania – elektronizácia procesov urýchli priebeh konaní,
- iii. nižšie náklady – rýchlejšie konania znamenajú nižšie náklady,
- iv. odstránenie elektronických bariér – jednotný systém zabráni vzniku elektronických bariér podnikania,
- v. vytvorenie transparentného a efektívneho procesného rámca pre predinsolvenčné, insolvenčné a reštrukturalizačné konania.⁹

V Insolvenčnom registri sa evidujú nasledujúce údaje:

- i. o konkurznom konaní a udalostiach, ktoré nastali v konkurznom konaní od vydania uznesenia o začatí konkurzného konania až po jeho ukončenie; ak ide o malý konkurz, od vydania uznesenia o vyhlásení malého konkurzu až po jeho ukončenie,
- ii. o reštrukturalizačnom konaní a udalostiach, ktoré nastali v reštrukturalizačnom konaní od vydania uznesenia o začatí reštrukturalizačného konania až po jeho ukončenie,
- iii. o konaní o oddlžení a udalostiach, ktoré nastali v konaní o oddlžení od vydania uznesenia o vyhlásení konkurzu alebo uznesenia o povolení splátkového kalendára až po jeho ukončenie,
- iv. o verejnej preventívnej reštrukturalizácii a udalostiach, ktoré nastali vo verejnej preventívnej reštrukturalizácii od vydania uznesenia o povolení verejnej preventívnej reštrukturalizácie až po jej ukončenie,
- v. o likvidácii a dodatočnej likvidácii od vydania uznesenia súdu o ustanovení likvidátora až po jej ukončenie,
- vi. ďalšie informácie o konaniach podľa bodov i. až v.

⁹ <https://havrilla.sk/novy-insolvencny-register-ako-vam-zjednodusi-podnikanie-od-oktobra-2025/>

Insolvenčný register zároveň predstavuje publikačnú platformu, na ktorej sa s účinnosťou od 1. októbra 2025 zverejňujú oznamy a iné zverejnenia súvisiace s insolvenčnými konaniami, predinsolvenčnými konaniami, ako aj s likvidáciami. V tejto súvislosti sa vyššie uvedené oznamy a iné zverejnenia už nebudú zverejňovať v príslušných kapitolách Obchodného vestníka. Výnimku tvoria oznamy a iné zverejnenia, ktoré súvisia s konkurzmi a vyrovnaniami podľa zákona č. 328/1991 Zb. o konkurze a vyrovnaní v znení neskorších predpisov, ktoré sa aj naďalej budú zverejňovať v Obchodnom vestníku, v kapitole „Konkurzy a vyrovnania“.¹⁰

Už tu vidíme rozdiel oproti Registru úpadcov, nakoľko obsahom Insolvenčného registra budú všetky údaje v uvedených konaniach, nielen niektoré a navyše aj údaje o preventívnej reštrukturalizácii, likvidácií a dodatočnej likvidácii obchodných spoločností, ktoré v Registri úpadcov zverejňované neboli.

Tento krok považujeme za správny, nakoľko podľa nášho názoru zvýši transparentnosť a prehľadnosť likvidačných konaní na jednom konkrétnom digitálnom mieste, prístupnom pre všetkých, pokiaľ majú prístup k internetu a počítaču alebo smartphonu. Predpokladáme, že tieto údaje, resp. zverejnené dokumenty budú samostatne vyčlenené alebo ich bude možné filtrovať podľa druhu zverejnenia alebo budú v samostatných foldroch/zložkách. Uvedené vyplýva z § 203b ods. 8 podľa ktorého údaje zverejnené v Insolvenčnom registri majú štruktúrovanú podobu, ktorá umožňuje ich vyhľadávanie a automatizované spracovanie.

Obchodný zákonník v početných ustanoveniach (napr. § 27, 67h, 75c, 147, a pod.) ukladá zákonnú povinnosť publicity (zverejnenia) niektorých, zákonom určených údajov o podnikateľoch alebo o niektorých právnych skutočnostiach, s cieľom dosiahnuť maximálnu informovanosť tretích osôb o takýchto údajoch, vrátane ich vzniku, zmeny alebo zániku. Najvýraznejšie sa táto povinnosť prejavuje v úprave obchodného registra (§ 27), ale aj v prípade iných údajov, napr. v procese likvidácie obchodnej spoločnosti alebo družstva (§ 70 a nasl.), pri znížení základného imania kapitálovej obchodnej spoločnosti, pri verejnej výzve na upisovanie akcií v akciovej spoločnosti, pri vyhlásení akcií za neplatné, pri prerozdelení kapitálových fondov medzi spoločníkov (akcionárov), či vo vzťahu k iným zákonom – napr. podľa zákona o konkurze a reštrukturalizácii, a pod.¹¹

Podľa § 769 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník (ďalej len „ObZ“) ak ide o likvidáciu alebo dodatočnú likvidáciu obchodnej spoločnosti alebo družstva, v ktorej ustanovil likvidátora súd, povinnosť zverejnenia údajov je splnená ich

¹⁰<https://www.justice.gov.sk/tlacovespravy/register-predinsolvenčných-likvidacných-a-insolvenčných-konaní/>

¹¹ KUBINEC, Martin. § 769 [Povinnosť zverejnenia v Obchodnom vestníku. In: LUKÁČKA, Peter, HUČKOVÁ, Regina, KUBINEC, Martin a kol. Obchodný zákonník. 1. vydanie. Praha: C. H. Beck, 2025, s. 1827. ISBN: 978-80-7699-013-5.

zverejnením prostredníctvom registra predinsolvenčných, likvidačných a insolvenčných konaní podľa všeobecného predpisu o konkurznom konaní.

Podľa § 769 ods. 1 ObZ ak odsek 2 neustanovuje inak, povinnosť zverejnenia údajov ustanovená týmto zákonom je splnená ich zverejnením v Obchodnom vestníku.

Z uvedeného vyplýva, že iba likvidátor ustanovený súdom je povinný zverejňovať údaje v Insolvenčnom registri. Inak sa údaje, resp. príslušné zverejnenia podľa ObZ pri likvidácii obchodnej spoločnosti alebo družstva zverejňujú v Obchodnom vestníku, čo platí pre likvidátorov ustanovených valných zhromaždením obchodných spoločností.

Údaje zverejnené v Insolvenčnom registri sa logicky týkajú určitých subjektov, preto Zákona č. 7/2005 Z. z. upravuje aj rozsah týchto údajov. Ide o:

- i. pri fyzickej osobe: meno, priezvisko, dátum narodenia a bydlisko,
- ii. pri fyzickej osobe podnikateľovi: obchodné meno, meno a priezvisko, ak sa líši od obchodného mena, identifikačné číslo organizácie alebo identifikačný údaj vydaný zahraničným registrom alebo zahraničnou evidenciou a miesto podnikania,
- iii. pri právnickej osobe: obchodné meno, identifikačné číslo organizácie alebo identifikačný údaj vydaný zahraničným registrom alebo zahraničnou evidenciou a sídlo.

Úpadcov preto bude možné konkrétne identifikovať podľa ich dostupných identifikačných údajov. Ako je zvykom napr. pri Registri konečných užívateľov výhod, rodné číslo sa uvádzať nebude, čo považujeme za prirodzené, keďže ide o citlivý osobný údaj a nezverejňuje sa ani v Obchodnom registri (okrem výpisu pre právne úkony, kde sa nachádza) alebo Registri konečných užívateľov výhod.

Elektronické dokumenty bude v Insolvenčnom registri uverejňovať súd, správca konkurznej podstaty alebo likvidátor. A výlučne iba tieto subjekty budú oprávnené zverejňovať elektronické dokumenty v Insolvenčnom registri, t.j. nie iný účastník. Uvedené subjekty budú zverejňovať svoje vlastné elektronické dokumenty, ale zároveň budú zverejňovať aj elektronické dokumenty, ktoré im budú doručené, t.j. účastníkov konania a iných osôb, ak udalosti vznikajúce na ich základe alebo v súvislosti s nimi sú evidované v Insolvenčnom registri, alebo ak elektronický dokument obsahuje údaje evidované v Insolvenčnom registri. Elektronický dokument doručený súdu ako príslušnému orgánu v konaní, eviduje a zverejňuje v Insolvenčnom registri tento súd, inak ho eviduje a zverejňuje v Insolvenčnom registri správca alebo likvidátor. Zverejnenie elektronického dokumentu však nemá vplyv na účinky jeho doručenia príslušnému orgánu.

To vnímame ako pozitívne i ako negatívne. Na jednej strane sa zabezpečí elektronický prístup do kompletného konkurzného spisu a nebude potrebné chodiť nahliadať do fyzického spisu. To znamená, že sa síce sa zabezpečí zverejňovanie všetkých dokumentov v Insolvenčnom registri, čo je nepochybne obrovská výhoda,

avšak súčasne to spôsobí veľkú a zrejme aj neprimeranú administratívnu záťaž najmä pre súdy a pre samotných správcov konkurznej podstaty. Tí budú pod tlakom (najmä časovým), aby všetky dokumenty týkajúce sa konkurzných konaní zverejňovali v Insolvenčnom registri. Problematické to bude najmä vzhľadom na skutočnosť, že podľa novej právnej úpravy, bude mať súd, správca konkurznej podstaty a likvidátor iba jeden pracovný deň na zverejnenie rozhodnutia alebo elektronického dokumentu po tom, ako sa dozvedeli o skutočnosti, s ktorou je spojené zverejnenie. Rozhodnutie súdu sa zverejní najneskôr deň nasledujúci po dni jeho vydania. Primárne sa však má elektronický dokument alebo rozhodnutie zverejniť bezodkladne. To kladie zvýšené administratívne nároky na súdy a správcov konkurznej podstaty, ktorý prichádzajú do kontaktu s desiatkami či stovkami dokumentov alebo rozhodnutí denne. Takáto krátka lehota na zverejnenie je jasným signálom na zvýšenie transparentnosti a dôveryhodnosti Insolvenčného registra. Rozumieme jej účelu, vhodnejšia by však bola lehota o dĺžke dvoch pracovných dní.

Zároveň poukazujeme na ust. § 199 ods. Zákona č. 7/2005 Z. z. ak tento zákon neustanovuje inak, za deň doručenia súdneho rozhodnutia alebo inej písomnosti sa považuje nasledujúci deň po zverejnení súdneho rozhodnutia alebo inej súdnej písomnosti v insolvenčnom registri. Rovnako písomnosti, ktoré sa podľa tohto zákona zverejňujú v insolvenčnom registri, sa považujú na účely tohto zákona za zverejnené nasledujúci deň po ich zverejnení v insolvenčnom registri.

Zákon č. 7/2005 Z. z. neobsahuje žiadnu sankciu za nedodržanie lehoty na zverejnenie rozhodnutia alebo elektronického dokumentu bezodkladne alebo do jedného pracovného dňa. Následkom však bude, že pokiaľ nebude dokument zverejnený, nenadobudne účinky doručenia voči účastníkom insolvenčného konania. Zároveň však teoreticky je možné podať žalobu na súd alebo správcu konkurznej podstaty v prípade, ak by nezverejnením rozhodnutia alebo elektronického dokumentu v Insolvenčnom registri došlo ku vzniku škody dotknutému subjektu, napr. veriteľovi.

Úplne novým (a podľa nášho názoru aj zaujímavým) inštitútom a súčasne povinnosťou bude posudzovanie dokumentov, ktoré sa doručujú súdu, správcovi konkurznej podstaty a likvidátorovi, pretože títo *ex lege* musia posudzovať im doručené dokumenty a posúdiť, či nejde o hrubo urážlivé podanie alebo či zverejnením takéhoto dokumentu nie je porušená povinnosť mlčanlivosti o údajoch chránených podľa osobitného predpisu alebo iná zákonom ustanovená alebo štátom uznaná povinnosť mlčanlivosti. Podľa poznámky pod čiarou č. 33o môže ísť napr. o Obchodný zákonník, zákon č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov, zákon č. 171/1993 Z. z. v znení neskorších predpisov, zákon č. 483/2001 Z. z. v znení neskorších predpisov, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov, zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) v znení neskorších predpisov,

zákon č. 563/2009 Z. z. v znení neskorších predpisov, zákon č. 500/2022 Z. z. o Vojenskom spravodajstve.

Zároveň zákonodarca stanovil, že ak nastanú pochybnosti o zverejnení obsahu elektronického dokumentu alebo jeho, rozhodne súd. Ak ide o záväzný pokyn príslušného orgánu správcovi, zverejňuje sa len informácia o vydaní záväzného pokynu.

Zastávame názor, že text Zákona č. 7/2005 Z. z. nie je dostatočne presný, ale je naopak vágny. Po prvé nie je zrejmé, čo sa má na mysli pod pojmom hrubo urážlivé podanie. Môžeme sa len predpokladať, že ide o podanie, ktoré obsahuje vulgarizmy alebo uráža súd, správcu konkurznej podstaty, likvidátora alebo iných účastníkov súvisiaceho konania. Poništ sa domnieva, že existujú dva druhy podaní, ktoré obsahujú urážlivý jazyk. Prvou kategóriou sú podania napr. v konaní o ochranu osobnosti z dôvodu, že tieto musia konkrétne označiť skutkové tvrdenia (aj keď sú urážlivé). Druhým prípadom sú podania s urážlivým, ofenzívnym jazykom a vulgarizmami, čo nemá nič spoločné s uplatňovaním práva strany sporu. Ide o podania, ktoré osočujú protistranu či iné osoby, samotné súdy a iné štátne orgány.¹² Čo všetko však možno zahrnúť pod pojem „hrubo urážlivé podanie“? Podľa nášho názoru môže ísť nielen o podanie, ktoré obsahuje vulgarizmy, ale ktoré celkovo svojim textom aj bez použitia pejoratívnych výrazov v značnej a neprimeranej miere znevažuje fyzické či právnické osoby alebo štátne orgány. Myslíme si, že sa takéto podanie sa samozrejme musí vecne týkať insolvenčného konania, ale súčasne sa hrubo urážlivá časť nemusí týkať sudcu, súdu, správcu konkurznej podstaty, úpadcu a pod. Takéto podanie bude pravdepodobne narúšať občiansku česť alebo dobrú povesť.

V konečnom dôsledku vyhodnotenie konkrétneho elektronického dokumentu však bude na oprávnenom subjekte, pričom bude musieť zohľadniť samotný elektronický dokument, ako aj konanie a okolnosti prípadu. Avšak, ak bude elektronický dokument skutočne obsahovať vulgarizmy alebo niekoho výslovne urážať, bude potrebné tento dokument vyhodnotiť ako hrubo urážlivý a nebude možné ho v Insolvenčnom registri zverejniť. Ak by bolo podanie v tomto ohľade sporné, rozhodne súd. Bude preto potrebné, aby správca konkurznej podstaty alebo likvidátor vec zaslal, resp. postúpil miestne príslušnému súdu na posúdenie. Text zákona však neuvádza, čo ak ani samotný súd prvej inštancie si nebude istý urážlivosťou elektronického dokumentu. Myslíme si, že nebude možné postúpiť veci na nadriadený súd, ale súd prvej inštancie bude musieť vec sám dôsledne posúdiť. Rovnako nie je uvedené, akou formou má súd rozhodnúť v danej veci. Nakoľko však

¹² Poništ, V.: Urážlivý jazyk podaní v civilnom sporovom konaní. In Bulletin slovenskej advokácie. Roč. XXVI, č. 1-2, (2020), s. 14. ISSN: ISSN 1335-107.

nejde o rozhodnutie vo veci samej a má procesný charakter, máme za to, že súd rozhodne uznesením. Zákon však nestanovuje lehotu, v ktorej ma súd rozhodnúť.

Údaje zverejnené v Insolvenčnom registri nebude potrebné pred orgánmi verejnej moci a v obchodnom styku preukazovať. To znamená, že zo zákona pôjde o skutočnosti vyplývajúce z činnosti samotného súdu podľa § 186 ods. 1 Civilného sporového poriadku Z. z.: *„Skutočnosti všeobecne známe alebo známe súdu z jeho činnosti, ako aj právne predpisy zverejnené alebo oznámené v Zbierke zákonov Slovenskej republiky a právne záväzné akty Európskych spoločenstiev a právne záväzné akty Európskej únie, ktoré boli zverejnené v Úradnom vestníku Európskych spoločenstiev a v Úradnom vestníku Európskej únie, sa nedokazujú.“* Postačí preto len odkázanie na ne a nebude potrebné ich v súdnom konaní a aj v obchodnom styku dokazovať.

Taktiež boli prijaté aj prechodné ustanovenia v § 206q Zákona č. 7/2005 Z. z., podľa ktorých konanie, ktoré sa začalo a právoplatne neskončilo do 30. septembra 2025, sa dokončí podľa tohto zákona v znení účinnom do 30. septembra 2025. Zároveň súčasťou Insolvenčného registra vedeného podľa predpisov účinných od 1. októbra 2025 sú aj údaje, ktoré boli zverejnené v registri úpadcov a v Obchodnom vestníku podľa predpisov účinných do 30. septembra 2025.

Preto budú „staré“ konkurzy a reštrukturalizácie naďalej podliehať starej právnej úprave. Avšak súdy a správcovia konkurznej podstaty budú musieť v Insolvenčnom registri zverejniť aj údaje nachádzajúce sa v Registra úpadcov. To je ďalšia zvýšená administratívna záťaž, pričom podľa našich informácií od správcov títo nevedia, kedy tieto údaje zverejnia v Insolvenčnom registri, nakoľko do neho týždeň pred spustením nemajú prístup. Pritom fakticky nebude možné pri veľkom počte insolvenčných konaní nahráť všetky údaje do Insolvenčného registra súčasne zo dňa na deň.

Insolvenčný register má byť v prevádzke od približne 14.00 hod 01.10.2025.¹³

Komparácia s českou právnou úpravou a právo Európskej únie

V Českej republike je Insolvenční rejstřík upravený v zákone č. 182/2006 Zb. o úpadku a způsobech jeho řešení (insolvenční zákon) (ďalej len „Zákon č. 182/2006 Zb.“). Právna úprava je obsiahnutá v šiestich ustanoveniach, teda je konkrétnejšia. Insolvenční rejstřík je informačným systémom verejnej správy v zmyslu zákona č. 365/2000 Sb., o informačných systémoch verejnej správy a o zmene niektorých ďalších zákonov, ve znění pozdějších předpisů.¹⁴

¹³ <https://www.justice.gov.sk/tlacovespravy/register-predinsolvenčných-likvidacných-a-insolvenčných-konaní/>

¹⁴KOTOUČOVÁ, Jiřina, MORAVEC, Tomáš. § 419 [Účel a obsah insolvenčního rejstříku]. In: MORAVEC, Tomáš, KOTOUČOVÁ, Jiřina a kol. Insolvenční zákon. 4. vydání. Praha: C. H. Beck, 2021, s. 1749. ISBN: 978-80-7400-849-8.

Rozdiel medzi Insolvenčným rejstříkem a Insolvenčným registrom spočíva v tom, že priamo v Zákone č. 182/2006 Zb. ja uvedené, že tento obsahuje insolvenčný spis a každý má právo do neho nahliadať a robiť si kópie a výpisy. Dokonca je možné požiadať o úradne overený výstup z informačného systému obsahujúci údaje z Insolvenčného rejstříku alebo informáciu, že sa tam požadovaný údaj nie je. Informácie o dlžníkovi súd do rejstříku zapíše do 7 dní od začatia insolvenčného konania a údaje sa do neho zapisujú v chronologickom poradí a ide o tieto informácie:

1. rozhodnutia insolvenčného súdu v konkurznom konaní a incidenčných sporoch,
2. všetky podania ohľadom dlžníka,
3. ďalšie informácie o ktorých tak ustanoví zákon alebo insolvenčný súd.

Fyzická osoba môže kedykoľvek požiadať, aby sa niektoré osobné údaje v Insolvenčnom rejstříku nezverejňovali, okrem mena a priezviska. Na nevyhnutnú dobu sa nezverejňujú ani podania, ktorých okamžité zverejnenie zmarilo účel insolvenčného konania.

Teda Insolvenčný register obsahuje navyše informácie o preventívnych reštrukturalizáciách, reštrukturalizáciách a likvidáciách obchodných spoločností. Rozdiel je tiež v tom, že sa posudzuje podania z hľadiska toho, či obsahuje hrubo urážlivé podania, čo v českej právnej úprave absentuje.

Zákon č. 7/2005 Z. z. je oproti nariadeniu Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní značne konkrétnejší. Ani v jednom právnom predpise nie je Insolvenčný register upravený výslovne podrobne. Je však zjavné, že slovenský zákonodarca išiel nad rámec toho, čo nariadenie požadovalo. Obsahuje viac informácií rovnako ako je tomu v prípade Insolvenčného rejstříku, teda rozsah zverejnených informácií je širší a obsahuje posúdenie hrubo urážlivého konania.

Česká právna úprava tiež obsahuje vyškrtnutie zo zoznamu dlžníkov, ktorý je zverejnený v Insolvenčnom rejstříku, a to v prípade, že uplynie päť rokov od právoplatnosti rozhodnutia, ktorým sa skončilo insolvenčné konanie.

Záver

Novela zákona č. 309/2023 o premenách obchodných spoločností a družstiev a o zmene a doplnení niektorých zákonov prináša Insolvenčný register, ktorý kompletne zdigitalizuje insolvenčné konanie.

Môžeme len dúfať, že jeho prepracovanosť a funkcionálnosť sú dostatočne dobre spracované, aby ponúkli súdom správcom konkurznej podstaty, likvidátorom a všetkým ostatným subjektom, ktoré ho budú využívať kvalitný nástroj na správu a zverejňovanie elektronických údajov týkajúcich sa insolvenčného konania.

Naplnenie cieľov, ktoré boli dané zavedením Insolvenčného registra ukáže až čas. Nateraz sa domnievame, že najmä pokiaľ ide o dostupnosť, prehľadnosť, prístup, množstvo informácií, možnosť komunikácie s insolvenčným súdom (prepojenie na www.slovensko.sk), tak tieto boli naplnené.

Predpokladáme, že insolvenčné konanie bude transparentnejšie, rýchlejšie a vyhľadávanie informácií jednoduchšie a dostupné komplexne na jednom mieste. Najmä sprístupní spis dištančne a elektronicky subjektom, ktoré budú potrebovať doň nahliadnuť a sprístupní všetky údaje o insolvenčnom konaní. Avšak až samotná prax ukáže, ako bude Insolvenčný register technicky fungovať a ako to budú zvládať súdy a správcovia konkurznej podstaty. Súdom a správcom konkurznej podstaty pribudnú nové právne povinnosti v súvislosti so zverejňovaním elektronických dokumentov v Insolvenčnom registri.

Nemožno opomenúť ani likvidácie obchodných spoločností, no doposiaľ v systéme Insolvenčného registra nie je ani jediný záznam k tejto agende, čo je prekvapujúce.

Zoznam použitej literatúry

1. ĎURICA, Milan. § 10a [Register úpadcov]. In: ĎURICA, Milan. Zákon o konkurze a reštrukturalizácii. 4. vydanie. Praha: C. H. Beck, 2021. ISBN: 978-80-7400-846-7.
2. IKRÉNYI, Ivan. Čl. 24 Vytvorenie insolvenčných registrov. In: IKRÉNYI, Ivan. Nariadenie o insolvenčnom konaní. 1. vydanie. Bratislava: C. H. Beck, 2020, s. 413. ISBN: 978-80-89603-82-4.
3. KOTOUČOVÁ, Jiřina, MORAVEC, Tomáš. § 419 [Účel a obsah insolvenčního rejstříku]. In: MORAVEC, Tomáš, KOTOUČOVÁ, Jiřina a kol. Insolvenční zákon. 4. vydání. Praha: C. H. Beck, 2021, s. 1749. ISBN: 978-80-7400-849-8.
4. KUBINEC, Martin. § 769 [Povinnost zveřejnění v Obchodnom vestníku]. In: LUKÁČKA, Peter, HUČKOVÁ, Regina, KUBINEC, Martin a kol. Obchodný zákonník. 1. vydanie. Praha: C. H. Beck, 2025, s. 1827. ISBN: 978-80-7699-013-5.
5. Poništ, V.: Urážlivý jazyk podaní v civilnom sporovom konaní. In Bulletin slovenskej advokácie. Roč. XXVI, č. 1-2, (2020), s. 14. ISSN: ISSN 1335-107.
6. Zákon č. 7/2005 Z. z. o konkurze a reštrukturalizácii a o zmene a doplnení niektorých zákonov
7. Zákon č. 513/1991 Zb. Obchodný zákonník
8. Zákon č. 160/2015 Z. z. Civilný sporový poriadok
9. Zákon č. 182/2006 Zb. o úpadku a spôsoboch jeho řešení (insolvenční zákon)
10. Nariadenia Európskeho parlamentu a Rady (EÚ) 2015/848 z 20. mája 2015 o insolvenčnom konaní
11. <https://ru.justice.sk/ru-verejnost-eb/public/oRegistriUpadcov.xhtml>

12. <https://www.justice.gov.sk/tlacovespravy/register-predinsolvenčných-likvidacných-a-insolvenčných-konaní/>
13. <https://havrilla.sk/novy-insolvenčný-register-ako-vam-zjednoduší-podnikanie-od-októbra-2025/>

Kontaktné údaje

JUDr. Martin Spišák

spisak24@uniba.sk

Univerzita Komenského v Bratislave, Katedra obchodného práva a hospodárskeho práva

PRÁVA PODNIKATELE V POSTAVENÍ PRODÁVAJÍCÍHO VE VZTAHU KE ŠKODĚ ZPŮSOBENÉ INFORMACÍ POSKYTNUTOU CHATOVACÍM ROBOTEM KUPUJÍCÍMU PŘI NÁKUPU ZBOŽÍ ONLINE

THE RIGHTS OF THE ENTREPRENEUR AS A SELLER IN RELATION TO DAMAGE CAUSED BY INFORMATION PROVIDED BY A CHATBOT TO THE BUYER DURING ONLINE SHOPPING

Pavla Tloušťová¹

Abstrakt: Současná doba je charakterizována prudkým rozvojem pokročilých technologií a nakupováním na internetu (online). Počítačové softwary používané pro online nakupování jsou aktuálně vyvíjené s prvky umělé inteligence, které mají za cíl nahrazovat intelektuální činnost lidí. Provozovatelé internetových obchodů (e-shopů) tak kupujícím při výběru zboží nabízejí služby tzv. chatovacího robota, který nahrazuje osobu prodavače, jak ji známe z kamenných obchodů. Příspěvek se zabývá analýzou odpovědnosti umělé inteligence užití pro provoz chatovacího robota při prodeji zboží v e-shopu podnikatele. Analyzovány jsou nároky tohoto podnikatele podle českého práva ve vztahu ke škodě způsobené (opakovanou) chybnou informací poskytnutou chatovacím robotem kupujícím při nákupu zboží online. Výsledkem právní analýzy je zjištění, že uplatňování nároků na náhradu škody podle právního řádu České republiky bude úkolem spíše nelehkým. Podnikatelé tak mohou upřednostnit sjednání vyvážené smlouvy o vývoji software s prvky umělé inteligence a servisní smlouvy (SLA) na provoz tohoto software v závodě podnikatele po ukončení vývoje a testování. Zkoumaná oblast přináší vhled do problematiky práv podnikatele užívající software s prvky umělé inteligence v podnikání. Tím příspěvek rozšiřuje většinu dosavadních analýz týkajících se ošetření práv společností vyvíjející software s prvky umělé inteligence nebo práv spotřebitelů. Příspěvek je zpracován analytickou a popisnou metodou.

Klíčová slova: umělá inteligence, e-shop, chatbot, škoda, odpovědnost

Abstract: The current era is characterized by the rapid development of advanced technologies and shopping on the Internet (online). Computer

¹ Západočeská univerzita v Plzni, Fakulta právnická

software used for online shopping is currently being developed with elements of artificial intelligence, which aim to replace human intellectual activity. Operators of online stores (e-shops) thus offer buyers the services of a so-called chat robot when choosing goods, which replaces the salesperson, as we know it from brick-and-mortar stores. The article deals with the analysis of the liability of artificial intelligence used to operate a chat robot when selling goods in an entrepreneur's e-shop. The claims of this entrepreneur under Czech law in relation to damage caused by (repeated) incorrect information provided by the chat robot to the buyer when purchasing goods online are analyzed. The result of the legal analysis is the finding that making claims for compensation for damages under the legal system of the Czech Republic will be a rather difficult task. Entrepreneurs may therefore prefer to negotiate a balanced contract for the development of software with artificial intelligence elements and a service agreement (SLA) for the operation of this software in the entrepreneur's business after the completion of development and testing. The area under study provides insight into the issues of the rights of entrepreneurs using software with artificial intelligence elements in their business. In this way, the contribution expands most of the previous analyses concerning the treatment of the rights of companies developing software with artificial intelligence elements or the rights of consumers. The contribution is prepared using an analytical and descriptive method.

Key words: artificial intelligence, e-shop, chatbot, damage, liability

Úvod

Současná doba je charakteristická dynamickým rozvojem pokročilých technologií a současně nakupováním zboží v internetových obchodech (e-shopech), tj. online. Zejména mladá generace již tento způsob nakupování zboží preferuje před nakupováním v kamenných obchodech. Výhodou je větší nabídka zboží, úspora času při jejich výběru a nižší ceny. Podle společnosti Shoptet, a.s., která v rámci projektu Ceska-ecommerce.cz dlouhodobě mapuje trendy a analyzuje data o českém e-commerce trhu, je v České republice v roce 2025 provozováno 67.305 e-shopů generující roční obrat ve výši 194 miliard Kč, což dosahuje podílu elektronického prodeje zboží ve výši 20,5 % na celkovém maloobchodním obratu. Uvedený počet e-shopů provozovaných podnikateli v České republice je nejvyšším v celé Evropě.² Internetový obchod (e-shop) je charakterizovaný absencí lidského pomocníka (prodáváče) zákazníkovi s výběrem zboží. Naprostá většina zákazníků internetových obchodů je v rámci svých kognitivních funkcí schopna si nabízené zboží prohlédnout,

² <https://www.ceska-ecommerce.cz/#prehled-o-trhu> [cit. 2025-9-20]

nastudovat jeho popis a vlastnosti a vybrat si to, které má zájem koupit. Takoví kupující zvládnou nákupním procesem projít bez asistence třetí osoby. Rostoucí rozsáhlá nabídka různého druhu zboží některých internetových nákupních galerií³ i skutečnost, že v e-shopu lze nyní nakupovat i vysoce specializované, technické výrobky, však přinesla potřebu nabídnout poradce pro výběr zboží tak, aby kupující vybral takové zboží, které preferuje a zejména, aby přes velkou nabídku zboží v každé z kategorií, internetový obchod neopustil bez realizace žádné koupě. Prodávající podnikatelé proto pro nákupní proces v e-shopu často nabízejí zákazníkům využití chatovacího robota (chatbota), který jim má poradit s výběrem zboží, požaduje-li tak zákazník.

Tento příspěvek se zabývá otázkou provozu chatbota v rámci elektronického obchodu z pohledu poskytovaných informací zákazníkům. Chatbot je software vyvinutý s funkcemi umělé inteligence, a proto od něj provozovatel e-shopu (prodávající) očekává pozitivní přínos v podobě zákaznické spokojenosti s jeho poradenskými službami poskytovanými zákazníkům. Lze jistě konstatovat, že podnikatel od užití chatbota také očekává stabilní či zvyšující se tržby generované internetovým obchodem. Co když tomu tak není a chatbot způsobuje svojí činností provozovateli e-shopu škodu?

Tento příspěvek analyzuje, jaké právní nároky může provozovatel e-shopu uplatnit podle českého práva ve vztahu ke škodě, kterou mu svojí činností způsobil chatbot chybnými informacemi poskytovanými kupujícím při nákupu zboží online. Uplatňování nároků na náhradu škody vzniklé korporacím při jejich podnikání je v českém řádu dosud spíše obtížná disciplína.

Pro zpracování tohoto příspěvku byla použita analytická a popisná metoda.

Pojem umělá inteligence

Podle Johna McCarthyho, který pojem umělá inteligence v roce 1955 zakotvil⁴, je umělá inteligence věda a technika vytváření inteligentních strojů, zejména inteligentních počítačových programů.⁵ Avšak byl to Alan M. Turing, který je považován za „vynálezce“ oblasti umělé inteligence na základě jeho článku nazvaného „Výpočetní stroje a inteligence“.⁶ V tomto článku se Turing zabýval otázkou, zda mohou stroje myslet. McCarthy předpověděl, že inteligence strojů na

³ Např. www.alza.cz; www.allegro.cz

⁴ MCCARTHY, John; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C.E.A. Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. In: Stanford University. 31.8.1955. Online. Dostupné na: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> [cit. 2025-09-26]

⁵ MCCARTHY, John: What is Artificial Intelligence? Článek. Str. 2. Revidováno 12. listopadu 2007. Online. Dostupné z: <https://www-formal.stanford.edu/jmc/whatisai.pdf> [cit. 2025-09-26]

⁶ TURING, Alan M.: Computing Machinery and Intelligence. In: Mind. 1950. Ročník LIX, Číslo 236, Str. 433 – 460. Online. Dostupné z: <http://dx.doi.org/10.1093/mind/lix.236.433> [cit. 2025-09-26]

lidské úrovni bude dosažena sestavením velkého počtu programů takového druhu, které lidé sestavují a vložením rozsáhlého objemu informací v jazycích, které jsou nyní používány pro vyjádření znalostí. Dále předpověděl, že umělá inteligence může být a používána, mezi jiným, i pro počítačové vidění jako „trojrozměrná informace, která není pouhou sadou dvojrozměrných vidění“.⁷

Podle Štědrone⁸ procházel vývoj umělé inteligence třemi etapami. První etapu lze nazvat romantickou (1956 – 1965), další dobou ledovou (1965 – 1980) a poslední dobou aplikací.

Již v prvopočátcích vývoje umělé inteligence panovaly obavy, aby nedošlo k situaci, kdy se umělá inteligence postaví proti člověku. Proto vznikly za přispění spisovatele Isaaca Asimova tyto tři zákony robotiky, které položily základ pro požadavky na vývoj robotů a umělé inteligence obecně:

1. Robot nesmí ublížit člověku nebo svou nečinností dopustit, aby bylo člověku ublíženo.
2. Robot musí uposlechnout příkazů člověka, kromě případů, kdy jsou tyto příkazy v rozporu s prvním zákonem.
3. Robot musí chránit sám sebe před poškozením, kromě případů, kdy je tato ochrana v rozporu s prvním, nebo druhým zákonem.⁹

Nakupování zboží online – právní základ

Podle českého právního řádu se proces nakupování zboží online, tj. v internetových obchodech – e-shopech, řídí ustanovením § 1731 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník“). Prodávající, kterým je podnikatel – tj. právnická osoba nebo podnikající fyzická osoba, činí vystavením zboží na internetu v internetovém obchodě, tj. v e-shopu, kupujícímu nabídku (ofertu) s určenou cenou za nabízené zboží s úmyslem uzavřít s kupujícím kupní smlouvu. Nabídka musí obsahovat podstatné náležitosti kupní smlouvy dle ustanovení § 2079 a násl. občanského zákoníku včetně ujednání taxativně vyžadovaných pro distanční prodej zboží spotřebitelům¹⁰ dle ustanovení § 1810 a násl. občanského zákoníku jako strany slabší oproti prodávajícímu vystupujícímu

⁷ MCCARTHY, John; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C.E.A.: Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. In Stanford University. 31.8.1955. Online. Dostupné na: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> [cit. 2025-09-26]

⁸ ŠTĚDRŇ, B. a kol. Právo a umělá inteligence. Plzeň: Aleš Čeněk, 2020, s. 109 [cit. 2025-09-27]

⁹ Ibid. s. 112.

¹⁰ Dle ustanovení § 419 občanského zákoníku je spotřebitel každý člověk, který mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání uzavírá smlouvu s podnikatelem nebo s ním jinak jedná.

v roli profesionála a strany silnější.¹¹ Zboží v e-shopu může nakupovat být buď podnikatel nebo spotřebitel (dále společně jen „kupující“).

Vložením nabízeného zboží do „košíku“ v rámci e-shopu a odesláním objednávky zboží dochází ze strany kupujícího k přijetí (akceptaci) nabídky na nákup zboží. Kupní smlouva je tak mezi prodávajícím a kupujícím uzavřena dle podmínek nabízených prodávajícím a akceptovaným kupujícím, které kromě jiného zahrnují též platební a dodací podmínky.

Výše uvedený nákupní postup zahrnuje projev svobodné vůle kupujícího i jeho schopnost vybrat si ze zboží nabízeného v e-shopu to, které sám požaduje, aniž by k výběru zboží na internetu použil asistenci, pomoc či doporučení poskytnuté prodávajícím.

Chatbot jako nákupní pomocník

Vývoj algoritmů hlubokého učení přinesl v éře chytrých mobilních zařízení (telefonů, tabletů) z pohledu uživatelů převratný vývoj v roce 2011. Byl to rok, v němž se inteligentní hlasová asistentka Siri stala poprvé součástí telefonu iPhone 4s od společnosti Apple.¹²

Postupně byli do internetových obchodů zavedeni chatovací roboti (chatboti) a virtuální asistenti řízení umělou inteligencí. Ti mohou simulovat lidskou konverzaci s uživateli v reálném čase, čtyřicet hodin denně, sedm dní v týdnu. Tyto systémy zvládnou celou řadu úkolů, od odpovědí na často kladené otázky až po vedení zákazníka složitým nákupním procesem. Pokročilé zpracování přirozeného jazyka umožňuje těmto botům porozumět kontextu, sentimentu výpovědi, a dokonce zpracovat více témat v jednom konverzačním vlákně. Dochází k dynamickému vývoji nejen díky rozmachu nových technologií, ale především kvůli ceně lidské práce.¹³

Z pohledu právního je chatovací robot (chatbot), dle Nařízení Evropského Parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024 – aktu o umělé inteligenci (dále jen „Akt o umělé inteligenci“) systémem umělé inteligence. Jedná se o software, který používá algoritmy umělé inteligence ke komunikaci s uživateli (fyzickými osobami) prostřednictvím textu (například v chatovacím okně) nebo hlasu (například prostřednictvím hlasových asistentů) a je navržen tak, aby simuloval lidskou konverzaci prostřednictvím automatizovaných odpovědí. Cílem chatbota je poskytovat informace, odpovídat na dotazy, pomáhat s řešením úkolů nebo simulovat konverzaci v různých kontextech. Podle Aktu o umělé inteligenci musí být

¹¹ Srov. TLOUŠŤOVÁ, Pavla: Jaká práva má spotřebitel dle českého práva při nákupu padělků na internetu? In: Obchodní právo, Ročník 34, číslo 8/2025, s. 5

¹² KNIHOVÁ, Ladislava: AI Marketing Playbook. Praha : Grada, 2024, s. 44

¹³ KNIHOVÁ, Ladislava: AI Marketing Playbook. Praha : Grada, 2024, s. 53

uživatel při interakci s chatbotem jasně informován, že komunikuje s umělou inteligencí, nikoliv s člověkem.

V rámci konkurenčního boje panujícího v České republice v prodeji zboží v e-shopech nyní prodávající často zdarma nabízejí zákazníkovi službu chatbota. Kupující zákazník chatbotu zadává své pokyny či otázky ke zboží nabízenému prodávajícím podnikatelem v e-shopu či ke zboží, které kupující poptává a má zájem koupit a chatbot mu poskytuje doporučení a rady, tedy informace.

Již z definice podnikatele dle ustanovení § 420 odst. 1 občanského zákoníku vyplývá, že cílem jím samostatně vykonávané činnosti na vlastní účet a odpovědnost, se záměrem tak činit soustavně, je zisk. Proto i zavedení služeb chatbota má podnikateli – provozovateli e-shopu – pomoci maximalizovat zisk v podnikání prostřednictvím stabilních či rostoucích tržeb získaných prodejem zboží v jeho e-shopu.

Škoda způsobená prodávajícím informacemi poskytnutými chatbotem kupujícím

Problém, který analyzuje tento příspěvek je situace, kdy chatbot dlouhodobě a opakovaně v komunikaci s kupujícími doporučuje kupovat pouze levnější nabízené zboží v dané kategorii. Kontrolou komunikace mezi kupujícími a chatbotem je prodávající podnikatel schopen zjistit a prokázat vznik a postupné zvyšování materiální újmy na jmění (škody) v podobě ušlých tržeb.

Právní nároky prodávajícího ve vztahu ke způsobené škodě

K posouzení právních nároků prodávajícího na náhradu škody způsobené informacemi dlouhodobě poskytovanými chatbotem kupujícím k tíži prodávajícího je třeba vzít v úvahu jakým způsobem byl chatbot, jakožto software s prvky umělé inteligence, prodávajícím pro provoz e-shopu dodán.

Software s prvky umělé inteligence je v praxi zpravidla vyvíjen softwarovou vývojářskou společností, jakožto zhotovitelem a podnikatelem provozujícím e-shop jako objednatel na základě smlouvy o dílo dle ustanovení § 2586 a násl. občanského zákoníku, pokud by byl takový smluvní vztah uzavřen podle českého práva. Společně s touto smlouvou strany uzavírají tzv. Service level agreement (SLA)¹⁴ jako „servisní“ smlouvu obsahující závazná ujednání o dostupnosti, údržbě a kvalitě služby, tj. vyvinutého softwaru s prvky umělé inteligence (chatbotu) po jeho úspěšném vývoji a předání podnikateli provozujícím e-shop na základě podepsaného akceptačního protokolu dle smlouvy o vývoji software. Druhou variantou z pohledu provozovatele e-shopu je nabytí software s prvky umělé inteligence jako hotového,

¹⁴ K tomu též JANSÁ L., OTEVŘEL P., ŠTEVKA M.: Softwarové právo, Brno : Computer Press, 3. vydání, 2018, s. 256

vyvinutého produktu na základě licenční smlouvy dle ustanovení § 2358 a násl. občanského zákoníku, byl-li by takový smluvní vztah uzavřen podle českého práva. V obou těchto případech se tedy z pohledu odpovědnosti za vadné plnění (vady) softwaru – chatbotu – jedná o smluvní odpovědnost dle českého právního řádu.

V praxi však nejčastěji dochází k tomu, že smlouva o vývoji software s prvky umělé inteligence, Service level agreement (SLA) či licenční smlouva na užívání hotového software nebývá uzavřena podle českého práva, ale typicky podle práva jiného státu, např. práva státu New York, Kalifornie či Delaware. Tato volba cizího práva souvisí zejména s hlavním místem podnikání dané softwarové vývojářské společnosti, což je zpravidla území Spojených států amerických, a znalostí výkladu a aplikace zvoleného amerického práva, na rozdíl od minoritního práva českého. Akcionáři takové zahraniční vývojářské společnosti chtějí mít pod kontrolou potenciální právní nároky, které by proti jejich portfoliové společnosti mohli vznést třetí osoby podle práva, kterým se řídí smlouvy s obchodními partnery (zde zejména zákazníky). Proto je pro tyto akcionáře zásadní, jakým právem se smlouvy o vývoji software společnosti, v nichž drží akcie, řídí a jaká je právní interpretace ujednání takové smlouvy. Zhotovitel software tak ve smlouvě o jeho vývoji software uzavřené podle zahraničního práva typicky vyžaduje, aby jeho jakákoliv odpovědnost za újmu (materiální i nemateriální) způsobenou objednateli byla vyloučena tím, že se objednatel práva na náhradu škody v písemné smlouvě vzdá, případně je toto právo objednatele smlouvou výrazně omezeno.¹⁵ Oproti tomu ujednání v servisní smlouvě – Service level agreement (SLA) - bývají pro objednatele, tj. prodávajícího v e-shopu, možností sjednat v ní alespoň smluvní pokutu za každou zjištěnou nedostupnost software a jeho chybovost, a to ve formě paušalizované náhrady škody.

Pokud by z teoretického hlediska smlouva uzavřená podle českého práva mezi společnostmi vyvíjející software s prvky umělé inteligence a prodávajícím v e-shopu ujednání o vyloučení či limitaci odpovědnosti za škody neobsahovala a ponechala tak otázku odpovědnosti za vadné plnění na zákonné normě jakožto delikt ní odpovědnosti dle ustanovení § 2910 občanského zákoníku, mohl by provozovatel e-shopu zvážit uplatnění nároku na náhradu škody (újmy na jmění) za předpokladu, že zhotovitel software (škůdce) (a) porušil zákonnou povinnost, (b) existuje újma a (c) prokáže se příčinná souvislost mezi jednáním škůdce a vznikem škody poškozeného. Uplatnění nároku na náhradu škody (újmy na jmění) by bylo možné z právních důvodů uvedených níže, jakkoliv by se pro poškozeného jednalo o komplikované dokazování.

- (i) Software s prvky umělé inteligence i robota lze považovat za věc v právní smyslu podle ustanovení § 489 občanského zákoníku. Je jí vše, co je

¹⁵ Srov. KOLAŘÍKOVÁ, L., HORÁK, F. Umělá inteligence & právo. Praha : Wolters Kluwer ČR, 2020, s. 138

rozdílné od osoby a slouží potřebě lidí, což bezpochyby software i robot splňují. Z toho vyplývá, že by podnikající provozovatel e-shopu mohl újmu způsobenou chatbotem nárokovat po společnosti vyvíjející software (škůdci) dle ustanovení o újmě způsobené věcí dle ustanovení § 2936 a násl. občanského zákoníku. Podle ustanovení § 2937 odst. 1 občanského zákoníku má škůdce možnost zprostit se povinnosti k náhradě, pokud prokáže, že nezanedbal náležitý dohled na věci, tj. softwarem s prvky AI pro provoz chatbotu. Škůdce tedy má možnost liberace, což odpovídá objektivní odpovědnosti.¹⁶

- (ii) Nárok provozovatele e-shopu by mohl být též uplatněn jako škoda z provozní činnosti podle ustanovení § 2924 občanského zákoníku. Ten, kdo provozuje závod nebo jiné zařízení sloužící k výdělečné činnosti, nahradí škodu vzniklou z provozu, ať již byla způsobena vlastní provozní činností, věcí při ní použitou nebo vlivem činnosti na okolí. Pojem provozu je třeba vykládat jako činnost související s předmětem činnosti (zpravidla podnikatelské, obchodní), kterou subjekt vyvíjí zpravidla opakovaně za použití určitých organizačních opatření, někdy s využitím různých technologií či postupů, včetně věcí, jimiž je místo činnosti (provozovna) vybavena. Do rámce provozu tak patří i činnosti, které bezprostředně, objektivně a fakticky předcházejí či navazují na činnost hlavní.¹⁷ Zde by chatbot byl považován za tzv. jiné zařízení sloužící k výdělečné činnosti, škoda by vznikla činností – informacemi poskytovanými chatbotem zákazníkům e-shopu a prokázána by musela být příčinná souvislost mezi jednáním chatbota a vznikem škody. Odpovědnosti by se společnost vyvíjející software s prvky umělé inteligence zprostila, pokud by prokázala, že vynaložila veškerou péči, kterou lze rozumně požadovat, aby ke škodě nedošlo.¹⁸
- (iii) Pokud by škodu způsobil software pro provoz chatbotu v e-shopu jako vadný výrobek, pak by dle ustanovení § 2939 občanského zákoníku škodu hradil ten, kdo výrobek vyrobil, případně na trh dovezl či dodal¹⁹. Škodu hradí uvedené osoby solidárně, a to v částce převyšující 500 EUR. Jakkoliv se očekává transpozice Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ze dne 23. října 2024 o odpovědnosti za vadné výrobky, do českého právního řádu, nebylo by možné její ustanovení aplikovat na

¹⁶ K tomu např. rozsudek Nejvyššího soudu ČR ze dne 29.7.2022, sp. zn. 25 Cdo 2342/2021

¹⁷ HULMÁK, M. a kol. Občanský zákoník VI. Závazkové právo. Zvláštní část (§2055 – 3014). Komentář. 1. vydání. Praha : C. H. Beck, 2014, s. 1601

¹⁸ K otázce neodvratitelné události nemající původ v provozu srov. Rozhodnutí Nejvyššího soudu ČR z 29.1.2008, sp. zn. 25 Cdo 529/2006

¹⁹ Ustanovení § 2940 zákona č. 89/2012 Sb., občanský zákoník, v platném znění

případ náhrady škody pro provozovatele e-shopu za škodu způsobenou informacemi poskytovanými chatbotem. Tato Směrnice sice v článku 4 v bodě 1) napevno stanovila, že software je výrobkem, ale škodu za porušení právní povinnosti mimo smluvní vztah budou moci vymáhat ve vztahu k výrobkům uvedeným na trh nebo do provozu po 9. prosinci 2026 pouze spotřebitelé či jiné fyzické osoby, a nikoliv osoby právnické. Podle směrnice nebude možné vymáhat škodu čistě ekonomickou²⁰, ani škodu za poškození či zničení majetku používaného výhradně pro profesní účely.²¹

Návrh evropské směrnice o odpovědnosti za umělou inteligenci zveřejněný Evropskou komisí dne 28. září 2022²² obsahující pravidla pro občanskoprávní uplatňování nároků na náhradu škody způsobené systémy umělé inteligence, nebyla přijata. S ohledem na přijatou Směrnici o odpovědnosti za vadné výrobky, se přijetí směrnice o odpovědnosti za umělou inteligenci neočekává.

Právo de lege ferenda

Podle mého názoru nelze aktuálně očekávat, že by byla přijata další evropská norma zohledňující možné nároky spojené s využíváním software s prvky umělé inteligence. Smluvní strany musí v praxi klást důraz na vyvážené obchodní smlouvy, které vzájemně uzavírají i na aspekt jisté předvídatelnosti ve fungování software s prvky umělé inteligence v provozech společností, včetně internetových obchodů. Domnívám se, že tak jak tomu bylo u vývoje každého předchozího software, nastane i u software s prvky umělé inteligence v budoucnu okamžik, kdy obavy z výstupů generovaných umělou inteligencí v podnikání korporací ustoupí stabilnímu provozu.

Závěr

Ve svém příspěvku jsem dospěla k názoru, že uplatňování nároku na náhradu škody způsobené informací poskytnutou (a opakovaně poskytovanou) chatovacím robotem kupujícím při nákupu zboží online bude v praxi problematické, ať již by se ze strany poskytovatele software jednalo o porušení smluvní nebo zákonné povinnosti. Přesto však očekávám, že také implementace software s prvky umělé inteligence jako určitého software sui generis a nástroje pro podnikání nebude běžně způsobovat

²⁰ Bod (24) Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ze dne 23. října 2024 o odpovědnosti za vadné výrobky [cit. 2025-09-27]

²¹ Článek 6 odst. 1 Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ze dne 23. října 2024 o odpovědnosti za vadné výrobky [cit. 2025-09-27]

²² Návrh směrnice o odpovědnosti za umělou inteligenci. Online. Dostupné na: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52022PC0496> [cit. 2025-09-27]

zásadní škodní události, tak jako tomu bylo s vývojem dosavadních typů software. Ostatně již nyní tento typ software korporace běžně v marketingu a prodeji jejich zboží a služeb používají. Podnikatelé, kteří na sebe při každodenní podnikatelské činnosti berou nespočet rizik, se mohou výše popsaná rizika pokusit zohlednit např. v pojistných smlouvách, které pro jejich podnikání uzavírají.

Seznam použité literatury

1. HULMÁK, M. a kol. Občanský zákoník VI. Závazkové právo. Zvláštní část (§2055 – 3014). Komentář. 1. vydání. Praha : C. H. Beck, 2014, 2072 s.
2. JANSÁ L., OTEVŘEL P., ŠTEVKO M.: Softwarové právo, Brno : Computer Press, 3. vydání, 2018, 488 s. ISBN 978-80-251-4914-0
3. KNIHOVÁ, Ladislava: AI Marketing Playbook. Praha : Grada, 2024, 232 s. ISBN 978-80-271-5226-1.
4. KOLAŘÍKOVÁ, L., HORÁK, F. Umělá inteligence & právo. Praha : Wolters Kluwer ČR, 2020, 216 s.
5. ŠTĚDRŮŇ, B. a kol. Právo a umělá inteligence. Plzeň: Aleš Čeněk, 2020. 201 s. ISBN 978-80-7380-803-7.
6. MCCARTHY, John; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C.E.A. Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. In Stanford University. 31.8.1955. Online. Dostupné na: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>
7. MCCARTHY, John: What is Artificial Intelligence? Článek. Revidováno 12. listopadu 2007. Online. Dostupné z: <https://www-formal.stanford.edu/jmc/whatisai.pdf>
8. MIKEŠ, Stanislav. Právo ve věku inteligentních strojů. In: Bulletin advokacie. Online. 2018. Dostupné na: <http://www.bulletin-advokacie.cz/pravo-ve-veku-inteligentnich-stroju>
9. POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. In. Bulletin advokacie. Online. 2018. Dostupné z: <http://www.bulletin-advokacie.cz/odpovednost-umele-inteligence-a-informacni-utvary-bez-pravni-osobnosti>
10. SHERER, Matthew U., Regulating Artificial Systems: Risks, Challenges, Competencies, and strategies. In: Harvard Journal of Law & Technology. Online 2016. Dostupné z: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>
11. TOMÍŠEK, Jan. Jaký je ideální model odpovědnosti za autonomní systém? In. Revue pro právo a technologie. Online. 2018. Dostupné z: <https://journals.muni.cz/revue/article/view/10452/pdf>

12. TURING, Alan M.: Computing Machinery and Intelligence. In: Mind. 1950. Ročník LIX, Číslo 236, Online. Dostupné z: <http://dx.doi.org/10.1093/mind/lix.236.433>
13. TLOUŠŤOVÁ, Pavla: Jaká práva má spotřebitel dle českého práva při nákupu padělků na internetu? In: Obchodní právo, Ročník 34, číslo 8/2025, s. 2 - 8.

Kontaktní údaje

JUDr. Pavla Tloušťová, MBA, Ph.D.
pavla.tloustova@simplylegal.eu
Západočeská univerzita v Plzni
Fakulta právnická

AI V SLUŽBÁCH ŠTATUTÁRNEHO ORGÁNU: DIGITÁLNY ASISTENT PRE ROZHODOVANIE

AI IN THE SERVICE OF THE STATUTORY BODY: A DIGITAL ASSISTANT FOR DECISION-MAKING

Richard Laura¹

Abstrakt: Štatutárne orgány nesú zodpovednosť za riadne a informované rozhodovanie, pričom jedným z liberačných dôvodov ich zodpovednosti je povinnosť zaobstarat' si a zohľadniť všetky dostupné informácie týkajúce sa predmetu rozhodnutia. V ére technológií môže umelá inteligencia (AI) zohrávať kľúčovú úlohu ako podporný nástroj pri plnení tejto povinnosti. AI dokáže v krátkom čase spracovať veľké množstvo dát, identifikovať súvislosti a ponúknuť odporúčania, ktoré by inak mohli zostať skryté. To môže významne prispieť k lepšej informovanosti štatutárneho orgánu a k minimalizácii rizika rozhodnutia prijatého na základe neúplných či nesprávnych podkladov. Práca ma za účel skúmať možnosti využitia AI ako digitálneho asistenta pre rozhodovanie, jeho prínos k naplneniu zákonnej povinnosti konať s odbornou starostlivosťou, ako aj potenciálne limity a riziká, ktoré si vyžadujú zodpovedný prístup k jej využívaniu.

Kľúčové slová: riziká a limity AI, rozhodovací proces, odborná starostlivosť, liberačný dôvod.

Abstract: Statutory bodies bear the responsibility for making proper and well-informed decisions, and one of the exonerating grounds for their liability is the duty to obtain and consider all available information relevant to the matter at hand. In the era of technology, artificial intelligence (AI) can play a key role as a supportive tool in fulfilling this duty. AI is capable of processing large volumes of data in a short period, identifying patterns, and providing recommendations that might otherwise remain undiscovered. This can significantly enhance the statutory body's level of information and help minimize the risk of decisions being made on the basis of incomplete or incorrect information. The purpose of this work is to examine the possibilities of using AI as a digital decision-making assistant, its contribution to fulfilling the statutory body's duty of

¹ Univerzita Komenského v Bratislave, Právnická fakulta, externý doktorand na katedre Obchodného práva a hospodárskeho práva.

acting with duty of care, as well as its potential limitations and risks, which require a responsible approach to its use.

Key words: and limitations of AI, decision-making process, duty of care, exculpatory reason.

Úvod

Umelá inteligencia prechádza dynamickým rozvojom a výrazne zasahuje do rôznych oblastí, vrátane podnikania. V podnikateľskom prostredí je však dôležité vnímať aj riziká, ktoré vyplývajú najmä z konania štatutárnych orgánov pri jej využívaní.²

Podľa Obchodného zákonníka³ sú štatutárne orgány povinné vykonávať svoju činnosť s odbornou starostlivosťou a lojálne, pričom zodpovedajú za škodu, ktorá môže vzniknúť spoločnosti alebo jej veriteľom v dôsledku porušenia týchto povinností.⁴ Zákon síce stanovuje viaceré povinnosti štatutárnych orgánov, avšak v súčasnom znení nevyžaduje špecifické kvalifikačné či odborné predpoklady (napr. úroveň dosiahnutého vzdelania). S ohľadom na vysokú mieru zodpovednosti vyvstáva otázka, aké kvalifikačné kritériá by mali členovia štatutárnych orgánov spĺňať, prípadne do akej miery je možné ich odborné znalosti či skúsenosti doplniť alebo outsourcovať, aby bol výkon ich funkcie riadny a v súlade s právnymi predpismi. V tejto súvislosti je preto namieste skúmať, do akej miery môže vyššia úroveň vzdelania členov štatutárnych orgánov prispieť k eliminácii rizika úpadku obchodných spoločností a k zníženiu škôd spôsobených spoločnosti a jej veriteľom. Súčasne je potrebné otvoriť aj otázku, či a v akom rozsahu možno absentujúce odborné znalosti či schopnosti štatutárnych orgánov, ktoré by inak zabezpečovalo vzdelanie, nahradiť prostredníctvom využitia umelej inteligencie.

Tieto otázky je nutné posúdiť najmä skrz zodpovednosť štatutárnych orgánov, primárne ustanovenia § 135a a § 194 Obchodného zákonníka.

² MÖSLEIN, Florian: Robots in the Boardroom: Artificial Intelligence and Corporate Law. In: WOODROW BARFIELD a UGO PAGALLO (eds.). Research Handbook on the Law of Artificial Intelligence. 1. vyd. Cheltenham: Edward Elgar Publishing, 2018, s. 649–670. DOI: 10.4337/9781786439055.00039

³ Zákon č. 513/1991 Zb. Obchodný zákonník (ďalej len „Obchodný zákonník“).

⁴ DURAČINSKÁ, Jana: Povinnosť starostlivosti riadneho hospodára alebo povinnosť odbornej starostlivosti z hľadiska právnej komparatistiky. In: Dny práva 2012 – „Bermudský trojuholník obchodného práva II“. Brno: Masarykova univerzita, 2013, [online]. Dostupné z: https://www.law.muni.cz/sborniky/dny_prava_2012/files/Bermudskytrojuhelnik/DuracinskaJana.pdf

Vplyv kvalifikácie štatutárnych orgánov na finančnú stabilitu a úverovú dôveryhodnosť obchodných spoločností

Viaceré empirické štúdie poukazujú na to, že úroveň vzdelania štatutárnych orgánov sama osebe nemá zásadný vplyv na dosahované finančné výsledky obchodných spoločností. Tento záver vyplýva najmä z článku „*Does Entrepreneurial Education Matter for the Performance of Medium-Sized Venture Entrepreneurs?*“ podľa ktorého hospodárske ukazovatele spoločností závisia skôr od externých trhových faktorov, štruktúry odvetvia alebo interných strategických rozhodnutí než od samotnej úrovne formálneho vzdelania štatutárnych orgánov.⁵

Podnikateľské vzdelávanie a tréning (MBA), často prezentované ako prostriedok na prekonanie hlavných prekážok podnikania, sa podľa štúdií neukazuje ako rozhodujúci faktor.⁶ Úzko špecializované kurzy a rady zamerané na zvládanie kríz môžu byť príliš neflexibilné a nedokážu sa plne prispôbiť špecifickým podmienkam podnikania. Výskum naznačuje, že absolventi týchto programov dosahujú v zlepšení podnikateľských schopností len zanedbateľné alebo takmer žiadne rozdiely v porovnaní s tými, ktorí tieto kurzy neabsolvovali. Pri zvládaní mimoriadnych situácií, ako bola pandémia, sa dokonca ukázali ako menej efektívni než ich kolegovia bez formálneho podnikateľského vzdelania.⁷

Podobné závery prináša aj štúdia, ktorá kladie dôraz na osobnostné vlastnosti jednotlivých členov štatutárnych orgánov a ich význam nad samotným vzdelaním. Podľa nej schopnosť efektívne zvládať krízové situácie nie je determinovaná iba akademickým či odborným vzdelaním, ale skôr komplexnou charakteristikou osoby, jej rozhodovacími schopnosťami, osobnostnými predpokladmi a rozsahom moci,⁸ ktorú má k dispozícii na riadiacej pozícii.⁹

⁵ AREND, Richard – UNAL, Ali – BILODEAU Richard: Does Entrepreneurial Education Matter for the Performance of Medium-Sized Venture Entrepreneurs? Administrative Sciences. 2025, roč. 15, č. 3, článok č. 75. Dostupné na: <https://doi.org/10.3390/admsci15030075>.

⁶ AREND, Richard – UNAL, Ali – BILODEAU Richard: Does Entrepreneurial Education Matter for the Performance of Medium-Sized Venture Entrepreneurs? Administrative Sciences. 2025, roč. 15, č. 3, článok č. 75. Dostupné na: <https://doi.org/10.3390/admsci15030075>.

⁷ AREND, Richard – UNAL, Ali – BILODEAU Richard: Does Entrepreneurial Education Matter for the Performance of Medium-Sized Venture Entrepreneurs? Administrative Sciences. 2025, roč. 15, č. 3, článok č. 75. Dostupné na: <https://doi.org/10.3390/admsci15030075>.

⁸ V prípade limitácie kompetencií internými predpismi dochádza k zníženiu reakčných schopností štatutárneho orgánu, zo štúdie: KLYVER, Kim – STEFFENS, Paul – NIELSEN, Suna Løwe: Crisis response efficacy: Perceived ability to respond entrepreneurially to crises. Journal of Business Venturing Insights. 2023, roč. 20, článok e00429. Dostupné na: <https://doi.org/10.1016/j.jbvi.2023.e00429>

⁹ KLYVER, Kim – STEFFENS, Paul – NIELSEN, Suna Løwe: Crisis response efficacy: Perceived ability to respond entrepreneurially to crises. Journal of Business Venturing Insights. 2023, roč. 20, článok e00429. Dostupné na: <https://doi.org/10.1016/j.jbvi.2023.e00429>.

V súvislosti s kompetenciami pritom iná štúdia ukazuje, že vyššia koncentrácia rozhodovacej moci medzi vedúcimi predstaviteľmi organizácie¹⁰ môže významne zlepšiť schopnosť obchodných spoločností rýchlo a účinne reagovať na krízové situácie.¹¹ To naznačuje, že schopnosť členov štatutárnych orgánov kombinovať osobné vlastnosti, autoritu a kompetencie je kľúčovým faktorom pre úspešné zvládanie kríz, pričom samotné vzdelanie predstavuje iba jeden z mnohých determinantov efektívneho vedenia.

Hoci vzdelanie samo osebe neposkytuje zásadne rýchlejší postup pri riešení problémov či napredovaní spoločnosti, osobná skúsenosť má v tomto smere omnoho väčší význam. V článku „*Do bank CEOs learn from crisis experiences?*“ sa ukázalo, že skúsenosti riadiacich orgánov s prekonávaním problémov významne prispievajú k tomu, ako dokážu spoločnosti zvládať ďalšie krízové situácie. Výskum potvrdil, že po prekonaní krízy dokázali tieto spoločnosti riešiť následné problémy efektívnejšie, a to najmä vďaka opatrnejšiemu prístupu, ktorý vychádzal zo skúseností z predchádzajúcej krízy.¹² Zároveň sa ukázalo, že takýto rezervovaný prístup spoločnosti nijako neznevýhodňoval v porovnaní s obchodnými spoločnosťami, ktoré preferovali rizikovejšie stratégie. Na základe toho možno konštatovať, že praktické skúsenosti členov štatutárnych orgánov majú väčší prínos pre zvládanie kríz než samotné akademické vzdelanie alebo podnikateľské kurzy.¹³

Posledná zo štúdií, z ktorej vychádza tento článok však preukazuje pozitívny a merateľný vplyv vzdelania členov štatutárnych orgánov s doktorátom (PhD) na

¹⁰ Predmetná štúdia sa nezameriavala výlučne na činnosť štatutárnych orgánov, ale aj na osoby pôsobiace v riadiacich pozíciách na rôznych úrovniach a stupňoch riadenia v rôznych typoch korporácií. Získané výsledky naznačili, že nižšia miera obmedzenia kompetencií najvyšších orgánov prispieva k efektívnejšiemu manažmentu organizácie. Keďže štúdia, z ktorej vychádzame, sa nezaoberá iba štatutárnymi orgánmi, považujeme za vhodné v tomto prípade nahradiť pojem „štatutárny orgán“ pojmom „vedúci predstaviteľ organizácie“.

¹¹ SAMREEN, Mahmood – MEHMOOD, Chadhar – SELENA Firmin: Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, 2024, roč. 32, č. 1, článok č. e12549. Dostupné z: <https://doi.org/10.1111/1468-5973.12549>.

¹² Toto tvrdenie platí za podmienky zachovania týchto osôb na pozícií. Vyplýva z YU, Yang. *Do bank CEOs learn from crisis experiences?* Singapore: Singapore Management University, 4-2025. Institutional Knowledge at Singapore Management University, Research Collection, Lee Kong Chian School of Business. [online]. Dostupné z: https://ink.library.smu.edu.sg/lkcsb_research/xxx.

¹³ YU, Yang: *Do bank CEOs learn from crisis experiences?* Singapore: Singapore Management University, 4-2025. Institutional Knowledge at Singapore Management University, Research Collection, Lee Kong Chian School of Business. [online]. Dostupné z: https://ink.library.smu.edu.sg/lkcsb_research/xxx.

výkonnosť obchodných spoločností, ktoré riadia.¹⁴ Faktorová analýza naznačuje, že jedna štandardná odchýlka v PhD vzdelaní je spojená s nárastom ROA upraveného o odvetvie o 1,20 %.¹⁵

Analýza ukázala, že:

- štatutárny orgán so vzdelaním s PhD zvyšuje výkonnosť obchodných spoločností o 3,03 %.
- štatutárny orgán so vzdelaním s PhD z top 100 univerzít zlepšuje výkon ešte výraznejšie, až o 4,65 %, čo poukazuje na pridanú hodnotu prestížnej vzdelávacej inštitúcie.

Preukázané zlepšenia činnosti štatutárnych orgánov s PhD vzdelaním sú:

- Efektívnejšie riadenie nákladov,
- lepší manažment cash flow.

Posledným zistením analýzy je zrejme zlepšenie širšieho spektra kognitívnych schopností a soft skills, ktoré si absolventi doktorandských programov osvojili. Medzi tieto schopnosti patrí vytrvalosť, analytické myslenie, schopnosť riešiť komplexné problémy a strategické uvažovanie.¹⁶

Posledným aspektom vplyvu vzdelania štatutárnych orgánov na riadenie obchodných spoločností je korelácia medzi dosiahnutou úrovňou vzdelania člena štatutárneho orgánu a kreditným skóre spoločnosti. Viaceré analýzy naznačujú, že vzdelanie týchto osôb môže mať nepriamy, avšak významný dopad na postavenie spoločnosti na trhu, predovšetkým prostredníctvom jej kreditného hodnotenia.¹⁷ Vyššia úroveň vzdelania členov štatutárnych orgánov môže zvýšiť dôveryhodnosť spoločnosti vo vzťahu k finančným inštitúciám, a tým jej umožniť získať priaznivejšie podmienky financovania. **V praxi to znamená, že spoločnosť je schopná flexibilnejšie reagovať na prechodné finančné ťažkosti a zabezpečiť si dostatočné zdroje na pokračovanie v podnikateľskej činnosti.** Takto môže vzdelanie štatutárnych orgánov prispieť k zníženiu rizika úpadku a k zvýšeniu stability obchodnej spoločnosti.

¹⁴ SIDKI, Marcus – BOERGER, Lara – BOLL, David: The effect of board members' education and experience on the financial performance of German state-owned enterprises. [online] 2023. Volume 28, pp. 445–482. Available at: [link if available] [Accessed 28 Sep. 2025].

¹⁵ URQUHART, Andrew – ZHANG, Hanxiong: PhD CEOs and firm performance. [online]. First published 11 May 2021. European Financial Management. Dostupné z: <https://doi.org/10.1111/eufm.12316>.

¹⁶ URQUHART, Andrew – ZHANG, Hanxiong: PhD CEOs and firm performance. [online]. First published 11 May 2021. European Financial Management. Dostupné z: <https://doi.org/10.1111/eufm.12316>.

¹⁷ PAPADIMITRI, Panagiota – PASIOURAS, Fotios – TASIOU, Menelaos – VENTOURI, Alexia: The Effects of Board of Directors' Education on Firms' Credit Ratings. Portsmouth Business School, University of Portsmouth, UK; Montpellier Business School, Montpellier, France; King's Business School, King's College London, UK.

Z predložených štúdií vyplýva, že dosiahnuté vzdelanie členov štatutárnych orgánov môže ovplyvniť schopnosť spoločnosti predchádzať hroziacemu úpadku. Po prvé, so zvyšujúcou sa úrovňou dosiahnutého vzdelania členov jej štatutárneho orgánu rastie aj kreditné skóre spoločnosti, vďaka čomu si dokáže zabezpečiť výhodnejšie financovanie. Po druhé, od určitého stupňa vzdelania (podľa štúdií PhD.) je možné pozorovať aj zlepšenie v riadení finančných tokov spoločnosti, jej manažmente a celkovej výkonnosti.

Dosiahnuté vzdelanie členov štatutárnych orgánov by však nemalo byť rozhodujúcim kritériom pri výkone ich funkcie, keďže na to, aby sa vzdelanie stalo reálnou konkurenčnou výhodou, muselo by dosahovať takú úroveň, ktorú by vzhľadom na náročnosť jeho dosiahnutia nebolo primerané štandardne vyžadovať.

Za kľúčové preto možno považovať rozvoj kognitívnych schopností, ktoré napomáhajú flexibilitu členov štatutárnych orgánov a podporujú ich efektívne rozhodovanie. Naopak, mechanické osvojovanie si teoretických poznatkov alebo memorovanie informácií má pri riadení spoločnosti iba obmedzený praktický prínos.

Outsourcované vzdelanie štatutárnych orgánov

V súčasnej diskusii o podnikaní a vedení obchodných spoločností rezonuje otázka, či je v ére rýchlo sa rozvíjajúcej umelej inteligencie stále potrebné a vhodné klasické vzdelanie ako i otázka či AI nenahradí osoby v ich zamestnaní alebo vykonávaní jednotlivých funkcií v obchodnom vzťahu.¹⁸ Táto úvaha vychádza z predložených štúdií a má skôr načrtnúť otvorenie otázok, ktoré si zasluhujú ďalšie skúmanie, než poskytnúť definitívne odpovede.

Z dostupných štúdií vyplýva, že samotná znalosť problematiky často nepostačuje na prijímanie optimálnych rozhodnutí zo strany štatutárnych orgánov. S pokrokom v oblasti umelej inteligencie a rastúcou úrovňou jej schopností však možno očakávať čoraz širšie uplatňovanie AI pri ich rozhodovaní.¹⁹ Externé získavanie informácií, vrátane využitia umelej inteligencie, môže rozhodovanie zlepšiť, avšak ak sú otázky nesprávne položené alebo kontext zle definovaný, výsledky poskytnuté systémom AI môžu spoločnosti skôr uškodiť než pomôcť.

V tomto kontexte je pravdepodobné, že rozdiely medzi vysoko vzdelanými členmi štatutárnych orgánov (najmä tými s titulom PhD), a tými s nižším vzdelaním sa budú postupne zväčšovať. Tento rozdiel sa môže prejaviť najmä v schopnosti efektívne a

¹⁸ MÖSLEIN, Florian: Robots in the Boardroom: Artificial Intelligence and Corporate Law. In: BARFIELD, W. a PAGALLO, U. (eds.). Research Handbook on the Law of Artificial Intelligence. Cheltenham : Edward Elgar Publishing, 2018, s. 649–670. DOI: 10.4337/9781786439055.00039.

¹⁹ MÖSLEIN, Florian: Robots in the Boardroom: Artificial Intelligence and Corporate Law. In: BARFIELD, W. a PAGALLO, U. (eds.). Research Handbook on the Law of Artificial Intelligence. Cheltenham : Edward Elgar Publishing, 2018, s. 649–670. DOI: 10.4337/9781786439055.00039.

správne využiť nástroje umelej inteligencie a interpretovať ich výstupy v komplexnom podnikateľskom prostredí.²⁰

Je dôležité zdôrazniť, že umelá inteligencia sama o sebe nie je riešením problémov. Ide o nástroj, ktorý môže významne zvýšiť efektivitu a kvalitu rozhodovania, ak je používaný správnymi rukami a na základe dobre položených otázok. Schopnosť strategicky kombinovať vlastné skúsenosti, kritické myslenie a výstupy AI sa preto stávajú kľúčovým predpokladom k úspechu v modernej podnikateľskej praxi.

Umelá inteligencia tak za určitých okolností môže byť efektívny asistent štatutárnych orgánov.

Právne aspekty využitia umelej inteligencie

Z právneho hľadiska je pre štatutárne orgány kľúčová otázka predchádzania hroziacemu úpadku a zodpovednosti za škodu spôsobenú spoločnosti a jej veriteľom. Obe oblasti majú spoločný základ v rozhodnutiach štatutárneho orgánu. Bez ohľadu na to, či sú tieto rozhodnutia správne alebo chybné, spoločnosť môže skončiť v úpadku alebo jej môže vzniknúť škoda. Preto je nevyhnutné klásť dôraz na schopnosti štatutárnych orgánov predchádzať týmto rizikám.

Následky spoločnosti v krízovej situácii môžu byť závažné, vrátane ohrozenia existencie spoločnosti a finančných záväzkov voči veriteľom. Následky vyvodenia zodpovednosti voči štatutárnym orgánom obchodných spoločností zahŕňajú možnosť siahnuť na osobný majetok člena štatutárneho orgánu. Súčasná právna úprava tak prenáša veľkú časť rizika práve na osoby zastávajúce funkciu štatutárneho orgánu, pričom tieto osoby nemusia disponovať dostatočnými znalosťami ani skúsenosťami, aby plne pochopili dôsledky svojho konania.

Jednou z možností, ako vyjadriť koreláciu medzi postavením člena štatutárneho orgánu a jeho zodpovednosťou, by bolo zavedením minimálneho požadovaného stupňa vzdelania. Avšak podľa dostupných štúdií by vzdelanie, ktoré by skutočne ovplyvnilo jeho schopnosti, muselo byť na úrovni PhD, čo nie je v praxi realizovateľné ani primerané vzhľadom na zistenia predložených štúdií.

Alternatívou preto môže byť využitie umelej inteligencie pri každodennom rozhodovaní. AI by mohla štatutárnemu orgánu pomôcť analyzovať informácie a generovať odporúčania, čím by sa zvýšila kvalita rozhodnutí.

²⁰ LI, Ning – DENG, Wenming – CHEN, Jiatan: From G-Factor to A-Factor: Establishing a Psychometric Framework for AI Literacy [online]. 2025 [cit. 2025-11-26]. Dostupné z: <https://arxiv.org/abs/2503.16517>

Štatutárne orgány si však musia byť vedomé, že AI je už dnes výrazne zaťažená predsudkami.²¹ AI nie je za každých okolností objektívna a jej naučené vzorce správania ju môžu viesť k určitým skresleniam. Tento nedostatok by však do budúcnosti mohla odstrániť regulácia, ktorá bude podporovať vývoj a tréning umelej inteligencie nediskriminačne.²² Otázkou preto zostáva, či a za akých podmienok možno odporúčanie AI považovať za liberačný dôvod a či sú citlivé informácie (vrátane obchodných tajomstiev alebo postupov) vložené do systému dostatočne chránené.

Odporúčania AI ako liberačný dôvod

Otázkou je, či možno odporúčania umelej inteligencie považovať za liberačný dôvod pri posudzovaní zodpovednosti štatutárnych orgánov, napríklad konateľov, za škodu spôsobenú spoločnosti. Podľa § 135a ods. 3 Obchodného zákonníka konateľ nenesie zodpovednosť za škodu, ak preukáže, že pri výkone svojej pôsobnosti konal s odbornou starostlivosťou a v dobrej viere, že sleduje záujem spoločnosti.

V kontexte tohto ustanovenia môže AI zohrávať dôležitú úlohu pri podpornom rozhodovaní. Používanie algoritmických odporúčaní môže konateľovi (štatutárnemu orgánu) pomôcť analyzovať komplexné situácie, predvídať riziká a navrhnúť optimálne riešenia, čím sa zvyšuje pravdepodobnosť, že jeho rozhodnutia budú v súlade s požiadavkami, ktoré vyžaduje súčasná právna úprava.²³ Teoreticky by teda mohlo ísť o faktor, ktorý podporuje presvedčenie konateľa, že koná v dobrej viere a v záujme spoločnosti, čo predstavuje kľúčový predpoklad pre uplatnenie § 135a Obchodného zákonníka.

Zastávame názor, že AI sama o sebe nikdy nemôže byť považovaná za liberačný dôvod. Ide vždy len o nástroj na získavanie informácií, ktorý môže štatutárnemu orgánu pomôcť pri rozhodovaní. Skutočný liberačný dôvod spočíva v tom, že štatutárny orgán na základe týchto informácií a ďalších relevantných zdrojov môže preukázať, že rozhodnutie bolo prijaté s odbornou starostlivosťou a v dobrej viere, že koná v záujme spoločnosti a všetkých jej spoločníkov, pričom riziko vzniku škodnej situácie bolo zrejme nízke alebo zanedbateľné. **Inými slovami, AI poskytuje podporu pri získavaní dát, ich analýze a rozhodnutí, ale zodpovednosť za správnosť rozhodnutia a posúdenie rizík zostáva výlučne na štatutárnom orgáne.** K rovnakému názoru dospel vo svojej publikácii i Sokol, keď uvádza, že „člen

²¹ ECCLES, Robert G. a Miriam Vogel. Board Responsibility for Artificial Intelligence Oversight. In: Harvard Law School Forum on Corporate Governance, 5. január 2022. DOI / URL: <https://corpgov.law.harvard.edu/2022/01/05/board-responsibility-for-artificial-intelligence-oversight/>.

²² PINTÉROVÁ, Dominika: Právna regulácia umelej inteligencie (perspektívy a výzvy). Právny obzor, 107, 2024, č. 4, s. 361 – 383. <https://doi.org/10.31577/pravnyobzor.2024.4.02>.

²³ Podľa ust. § 135a ods. 1 Obchodného zákonníka.

štatutárneho orgánu bude musieť pri využívaní umelej inteligencie dodržiavať aj povinnosť postupovať s odbornou starostlivosťou (ale aj povinnosťou lojality).“²⁴

Štatutárne orgány by zároveň pri využívaní AI mali na dosahovanie obchodných cieľov uplatňovať systematický rámec riadenia rizík, ktorý zahŕňa dohľad a riadenie, mapovanie rizík, ich meranie a kontrolu a ktorý umožňuje zavádzať technológie AI bezpečne a zodpovedne.²⁵

Ochrana poskytnutých údajov a informácií

Nový právny predpis na úrovni Európskej únie - Akt o umelej inteligencii²⁶ sa zaoberá aj otázkou ochrany osobných údajov a informácií nahrávaných do AI systémov. Aby mohla umelá inteligencia plniť úlohu efektívneho asistenta pri rozhodovaní členov štatutárnych orgánov, je nevyhnutné zabezpečiť prísnu dôvernosť spracúvaných údajov. Jej absencia by mohla viesť k negatívnym dôsledkom, napríklad k zodpovednosti štatutárneho orgánu podľa § 135a Obchodného zákonníka alebo k ohrozeniu obchodného tajomstva. Akt o umelej inteligencii však neposkytuje používateľom systémov umelej inteligencie automatickú ochranu údajov, ktoré majú povahu obchodného tajomstva alebo predstavujú iné informácie s hodnotou v obchodnom styku. Túto skutočnosť sú štatutárne orgány povinné zohľadniť v prípade využitia AI v rozhodovacích procesoch.

Zodpovednosť poskytovateľov AI systémov a asistentov

Poslednou a okrajovou otázkou je i možnosť prenosu zodpovednosti za nesprávne informácie poskytnuté systémom AI na jej poskytovateľov. Tu sa však stretávame s black box efektom. Black box efekt je fenoménom, ktorý označuje situáciu, kedy je ťažké alebo nemožné pochopiť, ako a prečo sa systém rozhodol alebo vykonal konkrétnu akciu.²⁷ Tento fenomén je obzvlášť dôležitý z hľadiska zodpovednosti za škodu, pretože poskytovatelia **AI nemôžu predvídať všetky**

²⁴ SOKOL, Michal: Digitalizácia a umelá inteligencia v obchodných spoločnostiach. Bratislava: C.H. Beck SK, 2024, s. 87. ISBN 978-80-8232-050-6.

²⁵ GREGORY, Holly J.: AI and the Role of the Board of Directors. In: Harvard Law School Forum on Corporate Governance, 07. október 2023. DOI / URL: <https://corpgov.law.harvard.edu/2023/10/07/ai-and-the-role-of-the-board-of-directors/>.

²⁶ NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (ďalej len „Akt o umelej inteligencii“).

²⁷ PLAZA, Juraj: Eliminácia pracovných úrazov pomocou umelej inteligencie. In: KNOLL, Vilém a Jakub HABLOVIČ (eds.). Naděje právní vědy 2023: právní věda v praxi. 1. vyd. Plzeň: Západočeská univerzita v Plzni, 2024, s. 550–559. ISBN 978-80-261-1258-7. DOI: 10.24132/ZCU.NADEJE.2023.550-559.

možné budúce akcie a rozhodnutia AI, a tým pádom ani škodu, ktorá by mohla vzniknúť druhej zmluvnej strane v dôsledku týchto rozhodnutí.²⁸

Z vyššie uvedeného vyplýva, že ak si štatutárny orgán zvolí ako poradcu systém umelej inteligencie namiesto kvalifikovaného poskytovateľa služby (napríklad advokáta zapísaného v advokátskej komore alebo účtovníka), stráca možnosť uplatnenia regresu za škody spôsobené chybou či nesprávnymi odporúčaniami takéhoto asistenta.²⁹

Na záver uvádzame, že sa objavujú názory, podľa ktorých by v budúcnosti bolo možné nedostatok zodpovednosti za škodu riešiť prostredníctvom poistenia AI a trhu s AI asistentmi alebo dokonca AI štatutárnymi orgánmi, pričom poskytovatelia týchto služieb by na seba aktívne preberali povinnosť nahradiť vzniknuté škody.³⁰

Záver

Z predloženej analýzy článkov a štúdií vyplýva, že v súčasnej podnikateľskej praxi nezáleží len na formálnom vzdelaní štatutárnych orgánov, ale najmä na ich osobných skúsenostiach, kognitívnych schopnostiach a schopnosti strategicky riadiť spoločnosť. **Ako bolo jednotlivými štúdiami preukázané, tak vzdelanie nie je nutne faktorom výkonnosti spoločnosti, pokiaľ nie je aspoň na úrovni PhD.** Dosiahnuté vzdelanie má pritom priamy vplyv na kreditné skóre spoločnosti. So zvyšujúcou sa úrovňou vzdelania, ako aj s prestížou vzdelávacej inštitúcie, kreditné skóre spravidla rastie.

Ako bolo uvedené, štatutárne orgány môžu umelú inteligenciu využiť ako nástroj, ktorý podporí ich rozhodovanie, umožní analyzovať komplexné situácie a predvídať riziká, čím môže do určitej miery nahrádzať formálne vzdelanie. AI však nikdy nemôže predstavovať automatický liberačný dôvod, pričom zodpovednosť za prijaté rozhodnutia a ich následky zostáva vždy výlučne na štatutárnom orgáne. Liberačný dôvod spočíva v tom, že štatutárny orgán sa rozhoduje na základe overených a relevantných informácií, pričom riziko vzniku škody je minimálne alebo zanedbateľné.

Z toho vyplýva, že využitie umelej inteligencie ako digitálneho asistenta pre rozhodovanie môže predstavovať významnú podporu pre štatutárne orgány,

²⁸ Domnievame sa, že efekt „black box“ môže naraziť na ustanovenie § 379 Obchodného zákonníka, pretože nie je možné určiť rozsah škôd, ktoré by boli pre vývojárov alebo poskytovateľov AI systémov predvídateľné.

²⁹ ÚSTAVNÝ SÚD SLOVENSKEJ REPUBLIKY. Uznesenie sp. zn. II. ÚS 678/2015 z 22. 10. 2015 Dostupné na: https://www.ustavnysud.sk/docDownload/9880b993-2ac5-4e6f-82ac-218bdca03517/%C4%8D.%2070%20-%20II.%20%C3%9AS%20678_2015.pdf

³⁰ DAEENABI, Imahn Milani: Beyond Human Oversight: Corporate Law and the Case for AI Directors. In: UC Hastings Law Journal, 1. vyd. Vol. 76, Issue 4, 2025, s. 1271–1306. Accessible at: UC Law SF L.J. https://repository.uclawsf.edu/hastings_law_journal/vol76/iss4/7/?utm_source=chatgpt.com.

avšak len za prísnych podmienok. Konateľ či iný štatutárny orgán musí vždy niesť plnú zodpovednosť za svoje rozhodnutia a **AI vnímať výlučne ako pomocný nástroj**, nie ako prostriedok automatického oslobodenia od zodpovednosti.

Zároveň je nevyhnutné zabezpečiť najvyšší štandard ochrany a dôvernosti spracovávaných údajov, keďže akékoľvek porušenie tejto povinnosti by mohlo viesť k závažným právnym aj ekonomickým dôsledkom spoločnosti. **Len pri splnení týchto predpokladov možno považovať umelú inteligenciu za legitímneho a efektívneho partnera štatutárnych orgánov v rozhodovacom procese.**

Zoznam použitej literatúry

1. AREND, Richard – UNAL, Ali – BILODEAU Richard: Does Entrepreneurial Education Matter for the Performance of Medium-Sized Venture Entrepreneurs? *Administrative Sciences*, 2025, roč. 15, č. 3, článok č. 75. <https://doi.org/10.3390/admsci15030075>
2. KLYVER, Kim – STEFFENS, Paul – NIELSEN, Suna Løwe: Crisis response efficacy: Perceived ability to respond entrepreneurially to crises. *Journal of Business Venturing Insights*, 2023, roč. 20, článok e00429. <https://doi.org/10.1016/j.jbvi.2023.e00429>
3. MAHMOOD, Samreen – CHADHAR, Mehmood – FIRMIN, Selena: Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, 2024, roč. 32, č. 1, článok e12549. <https://doi.org/10.1111/1468-5973.12549>
4. YU, Yang: Do bank CEOs learn from crisis experiences? *Journal of Financial Economics*, 2025, roč. 166, s. 1–21. Available at Institutional Knowledge, Singapore Management University: https://ink.library.smu.edu.sg/lkcsb_research/7684
5. URQUHART, Andrew – ZHANG, Hanxiong: PhD CEOs and firm performance. *European Financial Management*, 2021. <https://doi.org/10.1111/eufm.12316>
6. PAPADIMITRI, Panagiota – PASIOURAS, Fotios – TASIOU, Menelaos – VENTOURI, Alexia: The effects of board of directors' education on firms' credit ratings. *Journal of Business Research*, 2020, roč. 116, s. 294–313. <https://doi.org/10.1016/j.jbusres.2020.04.059>
7. SIDKI, Marcus – BOERGER, Lara – BOLL, David: The effect of board members' education and experience on the financial performance of German state-owned enterprises. 2023, vol. 28, s. 445–482. [ak URL/dostupnosť chýba — odporúčam doplniť presný názov časopisu + DOI]
8. PINTÉROVÁ, Dominika: Právna regulácia umelej inteligencie (perspektívy a výzvy). *Právny obzor*, 107, 2024, č. 4, s. 361–383. <https://doi.org/10.31577/pravnyobzor.2024.4.02>

9. PLAZA, Juraj: Eliminácia pracovných úrazov pomocou umelej inteligencie. In: KNOLL, Vilém – HABLOVIČ, Jakub (eds.). *Naděje právní vědy 2023: právní věda v praxi*. Plzeň: Západočeská univerzita v Plzni, 2024, s. 550–559. ISBN 978-80-261-1258-7. DOI: 10.24132/ZCU.NADEJE.2023.550-559
10. DAEENABI, Imahn Milani: Beyond Human Oversight: Corporate Law and the Case for AI Directors. *UC Hastings Law Journal*, 2025, vol. 76, č. 4, s. 1271–1306. Dostupné z: https://repository.uclawsf.edu/hastings_law_journal/vol76/iss4/7/
11. GREGORY, Holly J.: AI and the Role of the Board of Directors. *Harvard Law School Forum on Corporate Governance*, 07. október 2023. <https://corpgov.law.harvard.edu/2023/10/07/ai-and-the-role-of-the-board-of-directors/>
12. ECCLES, Robert G. – VOGEL, Miriam. Board Responsibility for Artificial Intelligence Oversight. *Harvard Law School Forum on Corporate Governance*, 05. január 2022. <https://corpgov.law.harvard.edu/2022/01/05/board-responsibility-for-artificial-intelligence-oversight/>
13. MÖSLEIN, Florian: Robots in the Boardroom: Artificial Intelligence and Corporate Law. In: BARFIELD, Woodrow – PAGALLO, Ugo (eds.). *Research Handbook on the Law of Artificial Intelligence*. Cheltenham: Edward Elgar Publishing, 2018, s. 649–670. DOI: 10.4337/9781786439055.00039
14. LI, Ning – DENG, Wenming – CHEN, Jiatan: From G-Factor to A-Factor: Establishing a Psychometric Framework for AI Literacy [online]. 2025. Dostupné z: <https://arxiv.org/abs/2503.16517>
15. DURAČINSKÁ, Jana: Povinnosť starostlivosti riadneho hospodára alebo povinnosť odbornej starostlivosti z hľadiska právnej komparatistiky. In: *Dny práva 2012 – „Bermudský trojuholník obchodného práva II“*. Brno: Masarykova univerzita, 2013. [online]. Dostupné z: https://www.law.muni.cz/sborniky/dny_prava_2012/files/Bermudskytrojuhelnik/DuracinskaJana.pdf
16. SOKOL, Michal: *Digitalizácia a umelá inteligencia v obchodných spoločnostiach*. Bratislava: C. H. Beck SK, 2024. 1. vyd. ISBN 978-80-8232-050-6.
17. ÚSTAVNÝ SÚD SLOVENSKEJ REPUBLIKY. Uznesenie sp. zn. II. ÚS 678/2015 z 22. 10. 2015 Dostupné na: https://www.ustavnysud.sk/docDownload/9880b993-2ac5-4e6f-82ac-218bdca03517/%C4%8D.%2070%20-%20II.%20%C3%9A%20678_2015.pdf
18. Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.
19. NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) **2024/1689** z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii).

Kontaktné údaje

Mgr. Richard Laura

laura2@uniba.sk

Univerzita Komenského v Bratislave, Katedra obchodného práva a hospodárskeho práva

IT GOVERNANCE: MONETIZÁCIA ÚDAJOV A JEJ VÝZVY PRI RIADENÍ OBCHODNÝCH SPOLOČNOSTÍ

IT GOVERNANCE: DATA MONETIZATION AND ITS CHALLENGES IN BUSINESS MANAGEMENT

Ľubica Kubíková¹

Abstrakt: V podnikateľskom prostredí obchodné spoločnosti čoraz častejšie prechádzajú digitálnou transformáciou s cieľom zefektívniť a účinne rozvíjať svoj podnikateľský zámer. Mnohé spoločnosti tak prechádzajú z tradičných metód na flexibilnejšie metódy. Jedným z prostriedkov, akým môže obchodná spoločnosť rozvíjať svoj podnikateľský zámer, je monetizácia údajov. Údaje sa stali súčasťou podnikania v rýchlo sa rozvíjajúcej digitalizácii podnikateľského prostredia. Niektoré zákaznícke segmenty – ako napríklad maloobchod, financie, marketing a komunikácia – pretransformovali z dát aktívum a používajú ich ako kľúčový pilier svojej obchodnej stratégie. Zavádzanie takýchto stratégií predstavuje výzvu pre obchodné spoločnosti zvládnuť riziká, ktoré prináša toto aktívum. Príspevok sa zameriava na riziká spojené s implementovaním novej digitálnej infraštruktúry, ktorá má zabezpečiť zbieranie, spracovanie, ukladanie a následnú monetizáciu údajov s ohľadom aj na často sa meniacu a pribúdajúcu právnu reguláciu. V rámci článku autorka identifikovala neustále sa meniacu a len čiastočnú právnu úpravu, ktorá nedostatočným spôsobom odpovedá na otázky súvisiace s limitmi využívania získaných dát na ďalší predaj. Zároveň v súčasnosti nejestvuje nadnárodná, ani v rámci EÚ, úprava regulujúca vlastnícke právo k získaným a následne predaným dátam a s tým súvisiacu zodpovednosť za spracovanie, predaj a následné využitie týchto dát (údajov vrátane osobných údajov) tretími osobami.

Kľúčové slová: monetizácia údajov, riadenie obchodných spoločností, riadenie informačných technológií

Abstract: In the business environment, commercial companies are increasingly undergoing digital transformation in order to streamline and effectively develop their business plans. Many companies are thus moving from traditional methods to more flexible ones. Data monetization is becoming one

¹ Interná doktorandka na Ústave štátu a práva SAV, v. v. i., Klemensova 19, 813 64 Bratislava

of the ways in which companies can develop their business plans. Data has become part of commerce in the rapidly developing digitalization of the business environment. Some customer segments – such as retail, finance, marketing and communications – have transformed data into an asset and use it as a key pillar of their business strategy. The implementation of such strategies presents a challenge for companies to manage the risks associated with this asset. This article focuses on the risks associated with implementing new digital infrastructure to collect, process, store, and monetize data, considering the frequently changing and growing legal regulations. In the article, the author identified constantly changing and only partial legal regulations that inadequately address issues related to the limits of using acquired data for resale. At the same time, there is currently no supranational regulation, even within the EU, governing ownership rights to acquired and subsequently sold data and the related responsibility for the processing, sale, and subsequent use of such data by third parties.

Key words: data monetization, corporate governance, IT governance

Úvod

Dáta sa stávajú jedným z najcennejších aktív v modernej ekonomike, ktoré možno v porovnaní s ropou niekoľkokrát replikovať a zhodnocovať bez toho, aby došlo k ich vyčerpaniu.² Hoci môže byť toto tvrdenie považované za klišé, nepopierateľná zostáva skutočnosť, že údaje, ktoré obchodná spoločnosť zbiera, spracováva a ukladá majú, obrovskú peňažnú hodnotu.³ Obchodné spoločnosti tak čoraz častejšie pristupujú k zavádzaniu nových digitálnych technológií, ktoré im umožnia efektívne využiť získané dáta na inováciu, optimalizáciu procesov, zlepšenie produktov, ale aj napr. na personalizáciu zákazníckych služieb.⁴ Tá pre obchodné spoločnosti však prináša mnohé výzvy súvisiace s efektívnym riadením obchodnej spoločnosti a predchádzaním rizík, ktoré so sebou prinášajú stále sa vyvíjajúce moderné technológie zamerané na spracovanie a analýzu veľkého množstva údajov, vrátane spracovávaní osobných údajov, monetizáciu týchto údajov, ktoré musia byť v súlade

² ADAMS, Nathan-Ross: Data monetisation: How to do so while avoiding legal trouble. 22/02/2025. Dostupné na internete: < <https://itlawco.com/data-monetisation-how-to-do-so-while-avoiding-legal-trouble/> >. [2025-08-04].

³ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 63.

⁴ MIRBAGHERI Fatemeh: To Sell or Not to Sell? Drivers and Barriers to Direct Data Monetization in Incumbents. In: Proceedings of the 58th Hawaii International Conference on System Sciences, 2025, s. 4034.

s vnútroštátnymi právnymi predpismi ale aj nadnárodnými reguláciami, s ohľadom na zabezpečenie bezpečného spracovania týchto údajov.⁵ Metodologicky príspevok vychádza z analýzy súčasnej právnej regulácie spracovávania údajov vrátane osobných údajov na regionálnej úrovni Európskej únie, s cieľom poukázať na právny stav, ktorý nereflektuje súčasné trendy pri spracovávaní (osobných) údajov, čo v konečnom dôsledku spôsobuje právnu neistotu na úkor (najmä) spotrebiteľa resp. dotknutej osoby/používateľa a zároveň prináša právne riziko pre obchodné spoločnosti, ktoré sa rozhodnú benefitovať z takýchto aktív.

IT Governance obchodnej spoločnosti pri monetizácii údajov

Riadenie informačných technológií (z ang. *IT governance* ďalej len „IT governance“) možno definovať ako systém práv a povinností, ktoré majú zabezpečiť želaný spôsob využívania informačných technológií v danej spoločnosti.⁶ Predstavuje podkategóriu riadenia obchodných spoločností, ktorá sa sústreďuje na riadenie a používanie informačných technológií s cieľom dosiahnuť želaný výsledok v obchodnej spoločnosti.⁷

Monetizácia údajov môže zabezpečiť konkurenčnú výhodu na trhu obchodnej spoločnosti, ktorá zabezpečuje efektívne zvýšenie spokojnosti a vernosti zákazníkov a zároveň umožňuje znížiť náklady vzniknuté v dôsledku neefektívnosti prevádzky.⁸ V súčasnosti nejestvuje jednotná legálna definícia monetizácie údajov.⁹ Monetizáciu údajov však podľa Gartner môžeme definovať ako proces získavania peňažnej hodnoty z **dát, ich analýz, využívania umelej inteligencie (AI), priamo alebo nepriamo vyjadrenej vo finančnej alebo peňažnej hodnote.**¹⁰ Inak povedané, monetizácia údajov predstavuje proces **využívania údajov na získanie kvantifikovateľného ekonomického prínosu.**¹¹ Obchodné spoločnosti môžu monetizovať dáta niekoľkými spôsobmi: (a.) predajom alebo licencovaním

⁵ INGALE, Ashish: IT Governance: Navigating the Figital Transformation era. 2024. Dostupné na internete: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5028361>. [2025-07-30].

⁶ WEILL, Peter – ROSS, Jeanne W.: IT Governance on One Page. CISR Working Paper. 2004, str. 1. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=664612 [2025-08-12].

⁷ Tamže, str. 1.

⁸ OFULUE Joan – BENYOUCEF, Morad: Data monetization: insights from a technology-enabled literature review and research agenda. In: Management Review Quarterly, Roč. 72, č. 2 (2024), s. 525.

⁹ MIRBAGHERIMARVILI, Sahar, GHANBARI, Hadi, ROSSI Matti: Data monetization challenges in established organizations: A systematic literature review. In: *Scandinavian Conference on Information Systems 2022 Aug 9*. It-universitetet i København. (2022), s. 2

¹⁰ Definícia dostupná na interenete: <<https://www.gartner.com/en/information-technology/glossary/data-monetization>> . [2025-08-27].

¹¹ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 65.

spracovaných údajov. Údaje predstavujú aktívum obchodnej spoločnosti, ktoré je ponúkané ako produkt alebo služba za peňažný zisk (tzv. priama monetizácia z ang. „*direct monetization*“), (b.) využitím už získaných údajov na zlepšenie prevádzky, personalizáciou služieb, a to konkrétnymi odporúčaniami alebo cieľenými reklamami, alebo zlepšovaním podnikateľského rozhodovania (tzv. nepriama monetizácia z ang. „*indirect monetization*“),¹² (c.) integráciou získaných poznatkov z dát do konkrétnych produktov resp. služieb (z ang. „*embedded monetization*“).¹³ Výber medzi jednotlivými metódami závisí od typu dát, konkurenčného prostredia a samotnej stratégie podniku.

Pri priamej metóde monetizácie údajov existujú štyri prístupy pri získavaní finančnej hodnoty z údajov obchodnej spoločnosti od tretích osôb:

(i.) predaj tzv. surových dát, kedy kupujúci získava nespracované dáta bez štatistík alebo analýz, od ktorých si následne sám vyhodnocuje relevantné informácie (z ang. „*Data as a Service*“ (DaaS)).¹⁴ Ide o najjednoduchšiu a najpriamejšiu metódu. Nevýhodou tejto metódy je najmä otázka súkromia, pričom kupujúci môže nadobudnúť vlastnícke právo k získaným dátam.¹⁵

(ii.) v druhom prístupe kupujúci získava poznatky z analýzy získaných údajov, zároveň však kupujúci nemá prístup k pôvodným údajom, čím je zabezpečená vyššia miera ochrany súkromia (z ang. „*Insights as Service*“).¹⁶ Nevýhodou tohto prístupu je samotné obmedzenie spôsobu využitia jednotlivých dát v porovnaní s prvým prístupom.

(iii.) tretí prístup je jeden s najflexibilnejších spôsobov zhodnocovania údajov, pri ktorom sa implementuje platforma poskytujúca univerzálnu analýzu údajov (z ang. „*Analytics-Enabled Platform Service*“).¹⁷

(iv.) posledný prístup je najpokročilejším spôsobom monetizácie údajov, pri ktorej dochádza k zhodnocovaniu údajov integrovanou analýzou (z ang. „*Embedded Analytics*“). Predstavuje začlenenie analytických funkcií priamo už v poskytovanom

¹² MIRBAGHERIMARVILI, Sahar, GHANBARI, Hadi, ROSSI Matti: Data monetization challenges in established organizations: A systematic literature review. In: *Scandinavian Conference on Information Systems 2022 Aug 9*. It-universitetet i København. (2022), s. 2.

¹³ ADAMS, Nathan-Ross: Data monetisation: How to do so while avoiding legal trouble. 22/02/2025. Dostupné na internete: <<https://itlawco.com/data-monetisation-how-to-do-so-while-avoiding-legal-trouble/>>. [2025-08-04].

¹⁴ MIRBAGHERIMARVILI, Sahar, GHANBARI, Hadi, ROSSI Matti: Data monetization challenges in established organizations: A systematic literature review. In: *Scandinavian Conference on Information Systems 2022 Aug 9*. It-universitetet i København. (2022), s. 2.

¹⁵ Tamže, s. 2.

¹⁶ Tamže, s. 2.

¹⁷ ADAMS, Nathan-Ross: Data monetisation: How to do so while avoiding legal trouble. 22/02/2025. Dostupné na internete: <<https://itlawco.com/data-monetisation-how-to-do-so-while-avoiding-legal-trouble/>>. [2025-08-04].

produkte alebo službe.¹⁸ Integrovaná analytika zahŕňa pridávanie funkcií spojených so softvérom pre tzv. *business intelligence*, ako sú analytické nástroje, reportovanie prostredníctvom *dashboards* a vizualizácie údajov, do existujúcich aplikácií. Výhoda spočíva v tom, že analytické rozhrania sa nachádzajú v jednej aplikácii a kupujúci platí za prístup k danej aplikácii alebo za sprístupnenie informácií.¹⁹

Monetizácia údajov tak zahŕňa nie len speňaženie získaných dát z predaja alebo zdieľania (externá monetizácia), ale aj vytváraním nových hodnôt, prípadne znižovaním nákladov alebo zlepšovaním podnikateľského rozhodovania (interná monetizácia).²⁰ Akonáhle začali obchodné spoločnosti vnímať údaje ako aktívum, koncepcia ich zhodnocovania sa stala spoločným cieľom.²¹ V dôsledku toho obchodné spoločnosti čoraz častejšie skúmajú možnosti, akými tieto dáta využijú na ich speňaženie.²² Získavanie, spracovávanie a následná monetizácia údajov vytvára niekoľko výziev pri jej právnej regulácii, ktorým sa príspevok venuje v nasledujúcej časti.

Výzvy právnej regulácie pri monetizácii údajov

Otázke monetizácie údajov sa dotýkajú viaceré právne poriadky na národnej úrovni.²³ Nejestvuje však jednotný štandardizovaný postup monetizácie údajov na medzinárodnej resp. nadnárodnej úrovni. V rámci EÚ právnu úpravu monetizácie údajov čiastočne regulujú dve nariadenia a to všeobecné Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „nariadenie GDPR“) a Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2854 z 13. decembra 2023 o harmonizovaných pravidlách týkajúcich sa spravodlivého prístupu k údajom a ich používania, ktorým sa mení nariadenie (EÚ) 2017/2394 a smernica (EÚ) 2020/1828 (Data Act) (ďalej len „nariadenie o údajov“).

¹⁸ Tamže.

¹⁹ Tamže.

²⁰ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 65.

²¹ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. s. 63.

²² Tamže, s. 63.

²³ California Consumer Privacy Act (CCPA), Protection of Personal Information Act (POPI Act), Personal Information Protection Law (PIPL). ADAMS, Nathan-Ross: Data monetisation: How to do so while avoiding legal trouble. 22/02/2025. Dostupné na internete: <<https://itlawco.com/data-monetisation-how-to-do-so-while-avoiding-legal-trouble/>>. [2025-08-04].

Výzvou právnej regulácie zostáva cezhraničné obchodovanie s údajmi, ktoré môže zahŕňať viacero jurisdikcií vzhľadom na skutočnosť, že nejednotný štandardizovaný regulačný rámec. Obchodovanie mimo Európskej únie napríklad s USA tak komplikuje uplatňovanie rôznych právnych noriem, v rôznych právnych odvetviach naprieč jednotlivými štátmi, kde jednotný regulačný rámec týkajúci sa bezpečnosti spracovávanía osobných údajov stále abscentuje.²⁴ Zároveň USA právny systém je založený na ochrane spotrebiteľa, pri ktorej balansuje ochranu súkromia s ochranou podnikania, s osobitným dôrazom na ochranu bezpečnosti údajov.²⁵

Monetizácia osobných údajov

Charta základných práv Európskej únie v čl. 8 vymedzuje transparentnosť a spravodlivosť pri spracovávaní osobných údajov, podľa ktorého v ods. 2: *„údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.“* Toto právo na ochranu osobných údajov bolo následne premietnuté aj do čl. 5 GDPR. Obchodná spoločnosť, ktorá sa rozhodne monetizovať údaje, je tak povinná zistiť, či tento údaj možno subsumovať pod osobný údaj²⁶ podľa všeobecného nariadenia.²⁷ V takomto prípade má obchodná spoločnosť možnosť anonymizovať osobné údaje tak, aby fyzická osoba nebola identifikovaná alebo identifikovateľná,²⁸ čím obchodná spoločnosť unikne spod pôsobnosti nariadenia GDPR, alebo ak to nie je možné, musí obchodná spoločnosť dôkladne informovať dotknuté osoby o tom, ako budú ich údaje použité, a aké dopady to bude mať na ich súkromie. Na takéto spracovávanie osobných údajov je potrebný právny základ, ktorý by bol v tomto prípade zvyčajne

²⁴ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 67.

²⁵ THOMAS, Llewellyn D. W.: 'Big data commercialization'. In: IEEE Engineering Management Review, Roč. 44, č. 2 (2016), s. 21.

²⁶ Čl. 4 ods 1 Nariadenia (EÚ) 2016/679 všeobecného nariadenia „osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

²⁷ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 67.

²⁸ Recitál 26 všeobecného nariadenia priamo vymedzuje kedy môže byť osoba na základe údajov identifikovaná alebo identifikovateľná.

založený na súhlase²⁹ dotknutých osôb³⁰ a zároveň je potrebné stanovenie presného cieľa využitia osobných údajov. Mnohokrát obchodné spoločnosti, v prípade že spracovávané údaje možno subsumovať pod osobné údaje, sa rozhodnú nemonetizovať tieto osobné údaje a to najmä v oblasti telekomunikácie, nakoľko by mohli stratiť dôveru svojich zákazníkov.³¹ Osobitne rizikové je v tomto prípade spracovávanie a zhodnocovanie údajov najmä o zdravotnej starostlivosti³², ktorých spracovanie môže zahŕňať okrem iného spracúvanie citlivých údajov, analýzu veľkého množstva údajov, používanie automatizovaných nástrojov a/alebo profilovanie, v ktorých môže mať dotknutá osoba obmedzené informácie a/alebo kontrolu nad svojimi osobnými údajmi.³³

V prípade, že by došlo k porušeniu nariadenia GDPR pri spracovávaní osobných údajov, je obchodná spoločnosť povinná oznámiť túto skutočnosť dozornému orgánu, ktorým je v podmienkach Slovenskej republiky Úrad pre ochranu osobných údajov ako i dotknutej osobe.³⁴ Následne je právna ochrana osobných údajov zabezpečená vyodením administratívnoprávnej zodpovednosti, kedy Úrad pre ochranu hospodárskej súťaže môže udeliť pokutu až do výšky do 10 000 000 eur, alebo ak ide o podnik do 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia,³⁵ pričom nie je dotknutá možnosť podania civilnej žaloby dotknutou osobou voči obchodnej spoločnosti.³⁶

²⁹ Všeobecné nariadenie v čl. 6 vymedzuje možnosť spracovania osobných údajov na viacerých základoch: a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely; b) spracúvanie je nevyhnutné na plnenie zmluvy, [...]; c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa; d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby; e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi; f) spracúvanie je nevyhnutné na účely oprávnených záujmov, [...], najmä ak je dotknutou osobou dieťa. Zastávame názor, že sa v tomto prípade bude vo všeobecnosti aplikovať čl. 6 ods. 1 písm. a všeobecného nariadenia.

³⁰ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 67.

³¹ THOMAS, Llewellyn D. W.: 'Big data commercialization'. In: IEEE Engineering Management Review, Roč. 44, č. 2 (2016), s. 24.

³² Čl. 9 ods. 1 všeobecného nariadenia.

³³ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 67.

³⁴ § 80 a nasl. Zákona č. 18/2018 Z.z. - o ochrane osobných údajov a o zmene a doplnení niektorých zákonov úplné a aktuálne znenie. (ďalej len „zákon o ochrane osobných údajov“)

³⁵ § 104 zákona o ochrane osobných údajov.

³⁶ Čl. 78 všeobecného nariadenia.

Monetizácia iných ako osobných údajov

V prípade druhého už spomenutého nariadenia o údajoch, ktoré Európsky parlament prijal v roku 2023, je cieľom regulovať a „*uľahčiť presun medzi službami spracúvania údajov a posilniť interoperabilitu údajov, ako aj mechanizmy a služby ich zdieľania v Únii*.“³⁷ Toto nariadenie o údajoch priamo neadresuje možnosť zhodnocovania údajov, ale naopak „*zabezpečuje spravodlivosť pri rozdeľovaní hodnoty údajov medzi subjekty dátového hospodárstva, pričom objasňuje, kto môže použiť aké údaje a za akých podmienok*.“³⁸ Nariadenie o údajoch stanovuje priamo povinnosť zdieľania údajov medzi podnikmi používateľov pripojených produktov v rámci internetu vecí³⁹ (z ang. *Internet of things* IoT),⁴⁰ väčšiu kontrolu nad údajmi, zavádza opatrenia na zvýšenie spravodlivosti a hospodárskej súťaže na európskom trhu a ochranu pred nespravodlivými podmienkami týkajúcimi sa zdieľania údajov, ktoré ukladajú silnejšie subjekty na trhu.⁴¹ Zároveň však neudeľuje akékoľvek právo držiteľom týchto údajov možnosť automatického použitia údajov. Takéto zdieľanie musí byť na zmluvnom základe, v ktorom sa vymedzujú práva týkajúce sa prístupu, cieľu využitia údajov, používania a zdieľania údajov, ktoré vytvára pripojený produkt alebo súvisiaca služba.⁴² Pri akomkoľvek ďalšom použití dát držiteľom dát alebo treťou stranou je tak nevyhnutne potrebná zmluva s povolením používateľa. Držiteľ dát má tak povinnosť sprístupniť údaje príjemcovi založenom na zmluvnom základe transparentne za spravodlivých, primeraných a nediskriminačných podmienok.⁴³ Rovnako ako v prípade nariadenia GDPR, aj podľa nariadenia o údajoch je v prípade porušenia možné udeliť pokutu,⁴⁴ ako aj možnosť fyzických a právnických osôb ako používateľov podať sťažnosť, pričom nie je dotknutá možnosť uplatnenia svojho práva na súde.⁴⁵

Toto nariadenie nadobudlo priamy účinok 12 septembra 2025⁴⁶ a má byť doplňujúcim podporným nariadením k nariadeniu GDPR a Nariadeniu Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018, o ochrane fyzických osôb pri

³⁷ Čl. 1 ods. 5 spolu s recitálom 5 nariadenia o údajoch.

³⁸ Dostupné na internete: < <https://digital-strategy.ec.europa.eu/sk/factpages/data-act-explained>>. [2025-09-15].

³⁹ Kapitola II nariadenie o údajoch.

⁴⁰ Pripojené zariadenia k internetu ako napríklad pripojené automobily, smart hodinky, domáce spotrebiče ale aj pripojené stroje v priemyselnom, výrobnom alebo poľnohospodárskom sektore. Pozri: KERBER, Wolfgang: EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation? IN: Journal of Antitrust Enforcement, č. 12 (2024), 234.

⁴¹ Recitál 14 a 20 nariadenia o údajoch.

⁴² Čl. 40 spolu s čl. 83 nariadenia o údajoch.

⁴³ FRAND podmienky podľa čl. 8 a 9 nariadenia o údajoch.

⁴⁴ Čl. 37 nariadenia o údajoch.

⁴⁵ Recitál 31 a čl. 38 a 39 nariadenia o údajoch.

⁴⁶ Čl. 50 nariadenia o údajoch.

spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES. V prípade „konfliktu medzi týmto nariadením a právom Únie o ochrane osobných údajov alebo súkromia alebo vnútroštátnym právnym predpisom prijatým v súlade s takýmto právom Únie má prednosť príslušné právo Únie alebo vnútroštátne právo o ochrane osobných údajov alebo súkromia.“⁴⁷ Inak povedané, ak údaj možno subsumovať pod osobný údaj podľa nariadenia GDPR, primárne musí obchodná spoločnosť naplňať reguláciu tohto nariadenia.⁴⁸ V prípade, že dáta obsahujú kombináciu osobných a iných ako osobných údajov, musí obchodná spoločnosť spĺňať podmienky GDPR ako aj nariadenia o údajoch. Nariadenie GDPR sa vzťahuje na osobné údaje a nariadenie o údajoch sa vzťahuje na všetky ostatné údaje⁴⁹ s výnimkou tzv. odvodených údajov, čím je naďalej možné zhodnocovať takéto odvodené údaje obchodnými spoločnosťami.⁵⁰ V takomto prípade je však viac než vhodné uzavrieť na takýto predaj odvodených údajov zmluvu v písomnej forme, v ktorej je priamo uvedený cieľ zhodnocovania údajov ako aj samotný aspekt zodpovednosti za ďalšie použitie týchto údajov, nakoľko nejestvuje žiadna právna regulácia takéhoto zhodnocovania, čo môže vytvárať právnu neistotu v zmluvných vzťahoch.

Myšlienka toho, že spracovanie veľkého množstva údajov podporuje rozhodovacie procesy, a tak v konečnom dôsledku predstavuje výhody pre toho kto vlastní tieto údaje, však môže byť ohrozená potenciálnym zneužitím resp. skompromitovaním

⁴⁷ Čl. 1 ods. 5 nariadenia o údajoch.

⁴⁸ ZOBOLI, Laura: Players and Interests at Stake in Data Sharing. In: ZOBOLI, Laura – BERNATT Maciej (editors) : Data Sharing Regulation in Europe. Taylor & Francis, 2025. Dostupné na internete: https://books.google.sk/books?hl=en&lr=&id=qXVeEQAAQBAJ&oi=fnd&pg=PA4&dq=data+monetisation+and+regulation+2020/1828+&ots=8g8Np8nt3x&sig=JUll-VtIhYdC2cC_qjObKWdEjll&redir_esc=y#v=onepage&q&f=false. [2025-09-01].

⁴⁹ Čl. 1 ods. 1 „údaje sú všetky digitálne formy aktov, skutočností alebo informácií a všetky kompilácie takých aktov, skutočností alebo informácií, a to aj v podobe zvukových, vizuálnych alebo audiovizuálnych nahrávok; “.

⁵⁰ Recitál 14 nariadenia o údajoch: „[...] Naopak, informácie získané alebo odvodené z takýchto údajov, ktoré sú výsledkom dodatočných investícií do získavania hodnôt alebo poznatkov z údajov, najmä prostredníctvom chránených, komplexných algoritmov vrátane tých, ktoré sú súčasťou proprietárneho softvéru, by sa nemali považovať za patriace do rozsahu pôsobnosti tohto nariadenia, a preto by sa na ne nemala vzťahovať povinnosť držiteľa údajov sprístupniť ich používateľovi alebo príjemcovi údajov, pokiaľ sa používateľ a držiteľ údajov nedohodnú inak. Takéto údaje by mohli zahŕňať najmä informácie získané prostredníctvom fúzie senzorov, pri ktorej sa údaje dedukujú alebo sa vyvodzujú z viacerých senzorov a zhromažďujú sa v pripojenom produkte použitím komplexných, proprietárnych algoritmov, a ktoré by mohli byť predmetom práv duševného vlastníctva.“

týchto údajov v rámci obchodovania.⁵¹ To môže priniesť radu otázok, kto je skutočným vlastníkom údajov, a kto nesie zodpovednosť za ich spracovanie, zneužitie a skompromitovanie, nakoľko pôvodný vlastník, ktorý tieto údaje zozbieral v konečnom dôsledku nemôže vedieť, akým spôsobom budú tieto údaje využité treťou osobou.⁵² Nariadenie GDPR a ani nariadenie o údajoch však priamo otázku zodpovednosti neupravuje. Je preto otázka zodpovednosti spracovania osobných údajov a údajov po jej monetizácii ponechaná na zmluvnej dohode strán, o tom kto zodpovedá, pričom do úvahy prichádzajú tieto alternatívy: držiteľ, poskytovateľ vedľajšej služby alebo tretia osoba.⁵³

Aktuálne tendencie monetizácie (osobných) údajov medzi B2C

Osobné údaje tak sú chráneným právom jednotlivcov úniijným právom, zatiaľ čo tzv. ostatné údaje generované na internete vecí nie sú *de iure* právom jednotlivca.⁵⁴ Obchodné spoločnosti tak mohli navrhnúť zariadenia tak, aby mali výlučné vlastníctvo nad údajmi získanými používaním týchto zariadení, čo v závere limitovalo samotných používateľov i sprostredkovateľom vedľajšej služby.⁵⁵ Tieto údaje podľa nariadenia o údajoch tak musia byť sprístupnené sprostredkovateľom vedľajšej služby, ale môžu byť používateľmi sprístupnené tretím stranám aj za účelom ďalšej monetizácie, avšak na zmluvnom základe s používateľom, držiteľom a treťou osobou.⁵⁶ To vytvára otázku efektívnosti úpravy, s ohľadom na už existujúcu problematickú aplikáciu právneho základu a súhlasu so spracovávaním osobných údajov podľa GDPR.⁵⁷ Rovnaká obava prichádza pri B2C kontraktoch podľa nariadenia o údajoch, pri ktorých si používateľ nebude čítať siahodlhé zmluvy resp. zmluvné podmienky a jednoducho bude súhlasiť s celým obsahom zmluvy, kedy môže vopred súhlasiť s možnosťou zhodnocovania a ďalšieho predaja týchto údajov

⁵¹ GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Cham: Springer Nature Switzerland, (2024), s. 63.

⁵² Tamže, s. 63.

⁵³ V súčasnosti tak koexistuje požiadavka na ochranu údajov vedľa ktorej jestvuje požiadavka na voľný prístup. DREXL, Josef: Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy (October 31, 2018). A. De Franceschi, R. Schulze (eds.), Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice, München, Beck, 2019, s. 21.

⁵⁴ KERBER, Wolfgang: EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation? IN: Journal of Antitrust Enforcement, č. 12 (2024), s. 241.

⁵⁵ Tamže, 235.

⁵⁶ KERBER, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives. In: GRUR International, Roč. 72, č. 2 (2023), s. 132 – 133.

⁵⁷ KERBER, Wolfgang: EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation? IN: Journal of Antitrust Enforcement, č. 12 (2024), s. 237.

na neobmedzené časové obdobie.⁵⁸ Naopak pri B2B kontraktach je očakávaná spravodlivá negociácia medzi používateľom zariadenia internetu vecí, držiteľom údajov a treťou osobou.⁵⁹ Odlišné závery však možno pozorovať a prípade Hoda vs. Google, na ktorom má autorka za cieľ demonštrovať silné postavenie držiteľov údajov s slabšie postavenie tak používateľa (spotrebiteľa) ako aj sprostredkovateľa vedľajšej služby či tretiu osobu (právnickú osobu – obchodnú spoločnosť).

Hoda/Google prípad

Úrad pre hospodársku súťaž (v Taliansku) začal 5. júla 2022 konanie voči spoločnosti Google z iniciatívy spoločnosti Hoda.⁶⁰ Obchodná spoločnosť Hoda je start-upovou spoločnosťou, ktorá vytvorila aplikáciu *Weople*. Jedná sa o aplikáciu, v ktorej používatelia delegujú na spoločnosť zbieranie údajov používateľov, ktoré majú vo vlastníctve resp. v držbe spoločnosti na iných platformách. Zároveň táto aplikácia ponúkala vedľajší produkt zameraný na zhodnocovanie spracovaných údajov na trhu používateľov.⁶¹ Spoločnosť Google neposkytla možnosť spoločnosti Hoda vytvoriť protokol interoperability, s cieľom vzájomnej výmeny údajov medzi obchodnou spoločnosťou Google a obchodnou spoločnosťou Hoda. Okrem toho Google vlastní obdobnú aplikáciu *Takeout*, na základe čoho obchodná spoločnosť Hoda považovala takéto konanie za zneužitie svojho dominantného postavenia na trhu.⁶² Voči obchodnej spoločnosti Google bolo následne vedené konanie Úradom pre hospodársku súťaž za porušenie pravidiel hospodárskej súťaže podľa čl. 102 ZFEÚ spolu s čl. 20 nariadenia GDPR. Vo februári 2023 bolo vyšetrovanie uzatvorené, pričom bolo obchodnej spoločnosti Google uložená povinnosť vyvinúť nástroje, ktoré používateľom umožnia stiahnuť a exportovať svoje údaje do aplikácií tretích strán.⁶³ Záverom tohto prípadu vyplýva, že počiatočná potreba regulácie narastajúceho získavania a spracovávaného množstva (osobných) údajov, sa posunula z prílišného protekcionizmu a potreby prísnej regulácie, na možnosť fyzických osôb, ktorých údaje sú spracovávané, predáť svoje údaje obchodným spoločnostiam, o čom svedčí

⁵⁸ Obmedzenia monetizácie sú obsiahnuté v čl. 4 až čl. 5 nariadenia o údajoch. KERBER, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives. In: GRUR International, Roč. 72, č. 2 (2023), s. 132 – 133.

⁵⁹ Tamže, s. 132 – 133.

⁶⁰ CORRENTI, Antonella: the monetisation of Personal Data in EU Strategies: The Hoda/Google Case. In: Studia Europejskie – Studies in European Affairs, Roč. 28, č. 2 (2024), s. 205.

⁶¹ CORRENTI, Antonella: the monetisation of Personal Data in EU Strategies: The Hoda/Google Case. In: Studia Europejskie – Studies in European Affairs, Roč. 28, č. 2 (2024), s. 205 – 206.

⁶² Tamže, s. 205 – 206.

⁶³ Tamže, s. 205 – 206.

aj nariadenie o údajoch.⁶⁴ Z práva chráneného unijným právom sa tak stáva majetok, ktorý je obvyčajným predmetom predaja.⁶⁵ Túto skutočnosť využili aj niektoré obchodné spoločnosti zavádzaním modelu "*consent or pay*";⁶⁶ pri ktorom obchodné spoločnosti zavádzajú predplatené aplikácie s možnosťou využívania bez ďalších poplatkov v prípade, že fyzické osoby poskytnú súhlas na spracovávanie a ďalšie zhodnocovanie údajov. Podľa Európskej komisie užívatelia, ktorí neudelia súhlas na spracovávanie údajov za účelom ďalšieho predaja resp. zhodnocovania, tak aj v takomto prípade by mali mať aj naďalej prístup k rovnocennej službe, ktorá využíva menej ich osobných údajov.⁶⁷ Súčasná právna regulácia, najmä nariadenie o údajoch, tak nenapĺňa ciele a nezabezpečuje dostatočné riešenie najmä pri B2C kontraktach, kde je práve predpoklad, že odmena bude patriť držiteľovi dát a len malá čiastka bude určená pre používateľov zariadenia resp. dotknutej osobe.⁶⁸ Túto skutočnosť potvrdzuje aj vyššie analyzované rozhodnutie, nakoľko súčasná právna regulácia nedokázala poskytnúť ochranu konečnému spotrebiteľovi, v situácii kedy spoločnosť Google nedodržiavala podmienky vzájomnej výmeny údajov, ale bola zabezpečená konkurentom spoločnosťou Hoda, prostredníctvom mechanizmom súťažného práva.

Záver

Napriek neustále sa meniacej a pribúdajúcej právnej regulácii nejestvuje jednotný ucelený právny rámec, ktorý by komplexne adresoval otázku získavania, spracovávania a monetizácie (osobných) údajov.⁶⁹ V príspevku autorka identifikovala niekoľko výziev, ktoré prináša monetizácia (osobných) údajov obchodnými spoločnosťami, ktorými sú: (i) limity využitia získaných dát, (ii) vlastnícke právo k monetizovaným údajom a následná zodpovednosť konkrétneho

⁶⁴ CORRENTI, Antonella: the monetisation of Personal Data in EU Strategies: The Hoda/Google Case. In: *Studia Europejskie – Studies in European Affairs*, Roč. 28, č. 2 (2024), s. 211 – 212.

⁶⁵ Tamže, s. 211 – 212.

⁶⁶ V Súčasnej právnej úprave takýto biznis plán je v súlade s reguláciou EÚ. Pozri odlišné závery v prípade spoločnosti Meta, v ktorej bola posudzovaná najmä neprimeraná výška, ktorá de facto nútila jednotlivcov s udelením súhlasu: Európska komisia, Komisia zaslala spoločnosti Meta predbežné zistenia týkajúce sa jej modelu „zaplať alebo súhlas“ za porušenie zákona o digitálnych trhoch, tlačová správa. [2025.11.10] https://digital-markets-act.ec.europa.eu/commission-sends-preliminary-findings-meta-over-its-pay-or-consent-model-breach-digital-markets-act-2024-07-01_en

a porovnaj: BACHELET, Vitttorio: Pay or Consent Models in Europe: Already Outdated or an Overlooked Crisis in Freely Given Consent?. In: *European Review of Private Law*, Roč. 32, č. 5 (2024) pp. 773 – 802.

⁶⁷

⁶⁸ KERBER, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives. In: *GRUR International*, Roč. 72, č. 2 (2023), s. 134.

⁶⁹ THOMAS, Llewellyn D. W.: 'Big data commercialization'. In: *IEEE Engineering Management Review*, Roč. 44, č. 2 (2016), s. 24.

subjektu za ich monetizáciu, (iii) otázka rozhodného práva pri cezhraničnej výmene údajov, s ktorou úzko súvisí aj štandardizácia obchodovania, nakoľko mimo EÚ ako napríklad v USA nejestvuje jednotná právna úprava. Nedávne tendencie dokonca ukazujú, že regulácia na úrovni EÚ sa posunula z ochrany osobných údajov, ako práva hodného ochrany zakotveného v Charte, ktoré nie je na predaj, na majetok, ktorý je predmetom obchodovania. Okrem toho súčasná právna regulácia nie je schopná reagovať na súčasné trendy v oblasti monetizácie osobných údajov, kedy jediným korekčným mechanizmom je podnet konkurujúcej obchodnej spoločnosti mechanizmami súťažného práva.

Zoznam použitej literatúry

1. ADAMS, Nathan-Ross: Data monetisation: How to do so while avoiding legal trouble. 22/02/2025. Dostupné na internete: < <https://itlawco.com/data-monetisation-how-to-do-so-while-avoiding-legal-trouble/>>. [2025-08-04].
2. BACHELET, Vittrorio: Pay or Consent Models in Europe: Already Outdated or an Overlooked Crisis in Freely Given Consent?. In: *European Review of Private Law*, Roč. 32, č. 5 (2024) pp. 773 – 802.
3. CORRENTI, Antonella: the monetisation of Personal Data in EU Strategies: The Hoda/Google Case. In: *Studia Europejskie – Studies in European Affairs*, Roč. 28, č. 2 (2024), s. 203 – 216.
4. DREXL, Josef: Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy (October 31, 2018). A. De Franceschi, , R. Schulze (eds.), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice*, München, Beck, 2019, s. 19 – 41.
5. GIZELIS, Christos A., et al. "Data monetization opportunities and challenges: the European landscape by Datamite." . In: *IFIP International Conference on Artificial Intelligence Applications and Innovations*. Cham: Springer Nature Switzerland, (2024), s. 62 – 79.
6. INGALE, Ashish: IT Governance: Navigating the Figital Transformation era. 2024. Dostupné na internete: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5028361>. [2025-07-30]
7. KERBER, Wolfgang: EU Data Act: Will new user acess and sharing rights on IoT data hepl competition and inovation? IN: *Journal of Antitrust Enforcement*, č. 12 (2024), 234 – 240.
8. KERBER, Wolfgang: Governance of IoT Data: Why the EU Data Act will not fulfill its objectives. In: *GRUR International*, Roč. 72, č. 2 (2023), s. 120 – 135.
9. KERBER, Wolfgang – ZOLNA K. Kasrten: Beyond the EU Data Act: Value of IoT Data, Market Failures, and Consumer Choice in the B2C Sector. Dostupné na

internete: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5130593>. [2025-11-10].

10. MIRBAGHERI Fatemeh: To Sell or Not to Sell? Drivers and Barriers to Direct Data Monetization in Incumbents. In: Proceedings of the 58th Hawaii International Conference on System Sciences, 2025, s. 4034 – 4043.
11. MIRBAGHERIMARVILI, Sahar – GHANBARI, Hadi – ROSSI Matti: Data monetization challenges in established organizations: A systematic literature review. In: Scandinavian Conference on Information Systems 2022 Aug 9. It-universitetet i København. (2022), s. 1 - 15.
12. OFULUE Joan – BENYOUCEF, Morad: Data monetization: insights from a technology-enabled literature review and research agenda. In: Management Review Quarterly, Roč. 72, č. 2 (2024), s. 521 – 565.
13. THOMAS, Llewellyn D. W.: 'Big data commercialization'. In: IEEE Engineering Management Review, Roč. 44, č. 2 (2016), s. 1 – 39.
14. WEILL, Peter – ROSS, Jeanne W.: IT Governance on One Page. CISR Working Paper. s. 349. Dostupné na internete: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=664612 [2025-08-12].
15. ZOBOLI, Laura – BERNATT Maciej: Data Sharing Regulation in Europe. Taylor & Francis, 2025. Dostupné na internete: https://books.google.sk/books?hl=en&lr=&id=gXVeEQAAQBAJ&oi=fnd&pg=PA4&dq=data+monetisation+and+regulation+2020/1828+&ots=8g8Np8nt3x&sig=JUll-VtihYdC2cC_qjObKWdEjll&redir_esc=y#v=onepage&q&f=false. [2025-09-01].
16. <<https://www.gartner.com/en/information-technology/glossary/data-monetization>>. [2025-08-27].

Kontaktné údaje

Mgr. Ľubica Kubíková

kubikova.lubica@savba.sk

Ústav štátu a práva SAV, v. v. i.

**Sekcia pracovného práva a práva sociálneho
zabezpečenia**

Rovnaké zaobchádzanie v ére digitalizácie: Výzvy
a príležitosti pre trh práce

ANALÝZA RODOVÝCH A ETNICKÝCH NEROVNOSTÍ V ALGORITMICKOM NÁBOROVOM PROCESE NA SLOVENSKU¹

ANALYSIS OF GENDER AND ETHNIC INEQUALITIES IN THE ALGORITHMIC RECRUITMENT PROCESS IN SLOVAKIA

Juraj Hamulák²

Abstrakt: Príspevok sa zaoberá problematikou algoritmickeho náboru zamestnancov s dôrazom na riziká vzniku rodových a etnických nerovností v podmienkach Slovenskej republiky. Cieľom je identifikovať mechanizmy, prostredníctvom ktorých umelá inteligencia môže reprodukovat' alebo zhoršovať existujúce nerovnosti, analyzovať relevantný právny rámec na úrovni Európskej únie a Slovenska a navrhnúť opatrenia na ochranu pred diskrimináciou a podporu spravodlivého prístupu k zamestnaniu. Autor analyzuje relevantnú literatúru, právne predpisy a judikatúru a využíva komparatívny prístup pri hodnotení skúseností zo zahraničia. Dôraz sa kladie na kľúčové oblasti náborového procesu, ako sú tvorba inzerátov, skrining uchádzačov a využívanie video-interview nástrojov. Autor poukazuje na potrebu povinných auditov algoritmov, zlepšenia transparentnosti a práva uchádzačov na zrozumiteľné vysvetlenie automatizovaných rozhodnutí. Záverom autor formuluje odporúčania de lege ferenda, ktoré zahŕňajú legislatívne ukotvenie ľudského dohľadu, zavedenie certifikácie HR-AI systémov a rozvoj odborných kapacít na ich audit. Príspevok prináša vedecký prínos v rozšírení teoretickej a právnej diskusie o algoritmickej spravodlivosti a praktický prínos pre tvorcov politík, zamestnávateľov a odbornú verejnosť pri nastavovaní transparentných náborových procesov.

Kľúčové slová: Rovnaké zaobchádzanie, algoritmy, umelá inteligencia, trh práce, diverzita.

Abstract: The paper deals with the issue of algorithmic recruitment of employees with an emphasis on the risks of gender and ethnic inequalities in Slovakia. The aim is to identify the mechanisms through which artificial

¹ Príspevok bol spracovaný pod záštitou projektu VEGA č. 1/0677/24 s názvom „Ženy v kríze“.

² Univerzita Komenského v Bratislave, Právnická fakulta, Katedra pracovného práva a práva sociálneho zabezpečenia

intelligence can reproduce or exacerbate existing inequalities, analyze the relevant legal framework at the level of the European Union and Slovakia, and propose measures to protect against discrimination and promote fair access to employment. The author analyzes relevant literature, legislation, and case law and uses a comparative approach to evaluate experiences from abroad. Emphasis is placed on key areas of the recruitment process, such as ad creation, applicant screening, and the use of video interview tools. The author points to the need for mandatory algorithm audits, improved transparency, and the right of applicants to a comprehensible explanation of automated decisions. In conclusion, the author formulates recommendations *de lege ferenda*, which include the legislative anchoring of human oversight, the introduction of certification of HR-AI systems, and the development of professional capacities for their audit. The article makes a scientific contribution by expanding the theoretical and legal discussion on algorithmic fairness and provides practical benefits for policymakers, employers, and the professional public in setting up transparent recruitment processes.

Key words: Equal treatment, algorithms, artificial intelligence, labor market, diversity.

Úvod

Rozmach umelej inteligencie zásadne mení nielen spôsob, akým pracujeme, ale aj procesy súvisiace s náborom a výberom zamestnancov. To, čo sa kedysi považovalo za prevažne administratívnu úlohu, sa dnes transformuje na komplexný, viacvrstvový systém, do ktorého umelá inteligencia zasahuje vo všetkých kľúčových fázach -- od formulácie pracovných ponúk, cez skríning uchádzačov, až po finálne rozhodnutie o výbere kandidáta. Táto technologická zmena so sebou prináša potenciál podporiť inklúziu a rovnosť príležitostí, avšak zároveň otvára aj zásadné otázky o rizikách diskriminácie na základe pohlavia či etnicity. Rozšírené používanie umelej inteligencie v procese náboru mení spôsob, akým zamestnávateľia oslovujú, triedia a vyberajú kandidátov. Tam, kde ľudský personalista pracoval s desiatkami žiadostí, dnes algoritmy hodnotia stovky až tisíce profilov za krátky čas. Nárast efektívnosti prináša zároveň riziko reprodukcie historických predsudkov. Nástroje AI sú nasadzované v každom kroku náboru: pri tvorbe a zverejňovaní pracovných inzerátov, pri predvýbere a bodovaní uchádzačov, pri organizácii pohovorov a v niektorých prípadoch aj pri konečnom rozhodovaní o prijatí. Takáto technologická zmena sľubuje väčšiu efektívnosť, no zároveň prináša nové riziká (predovšetkým

reprodukcii historických predsudkov, ktoré môžu viesť k diskriminácii na základe pohlavia alebo etnicity).³

V podmienkach Slovenskej republiky, kde existujú pretrvávajúce rodové nerovnosti (napr. rozdiely v zamestnanosti a mzdách) a výrazné výzvy týkajúce sa možnosti zamestnať sa (napr. v prípade rómskych komunit)⁴, je potrebné preskúmať, či a ako algoritmy môžu prispieť k prehľbovaniu týchto disproporcií.

Cieľom tohto príspevku je identifikovať mechanizmy vzniku rodových a etnických nerovností v algoritmickom náboře, analyzovať právne nástroje použiteľné v podmienkach EÚ a na Slovensku, ktoré riešia automatizované rozhodovanie a formulovať návrhy de lege ferenda, ktoré sa budú týkať konkrétnych právnych, prípadne organizačných opatrení v podmienkach Slovenskej republiky.

Metodologické východiská a vymedzenie

Príspevok vychádza z kvalitatívnej právnej a interdisciplinárnej analýzy, ktorá kombinuje doktrínálny výklad právnych predpisov Európskej únie a Slovenskej republiky s poznatkami z oblasti etiky umelej inteligencie a sociológie práce, ako aj z empirických poznatkov autora z jeho priamych skúseností z aplikačnej praxe. Primárne sa opiera o analýzu relevantnej domácej a zahraničnej literatúry, právnych predpisov a judikatúry v oblasti algoritmickej spravodlivosti a antidiskriminačného práva.

Pojem algoritmický nábor označuje využívanie systémov založených na umelej inteligencii alebo automatizovanom spracúvaní dát v jednotlivých fázach výberového procesu — od tvorby a distribúcie pracovných ponúk, cez predvýber uchádzačov (screening, scoring), až po podporu rozhodovania pri finálnom výbere. Súčasťou tejto kategórie sú aj nástroje tzv. Applicant Tracking Systems (ATS) a HR softvérové riešenia s implementovanými funkciami strojového učenia.

V slovenskom prostredí absentuje systematická evidencia používania algoritmických HR nástrojov. Verejne dostupné informácie vychádzajú prevažne z trhových reportov poradenských spoločností a sekundárnych analýz (napr. ManpowerGroup, 2023; Slovenská aliancia pre inovatívnu ekonomiku – SAPIE, 2024). Limity výskumu predstavuje aj nedostupnosť údajov o interných algoritmických moduloch nadnárodných platforiem, ktoré slovenskí zamestnávateľia používajú bez lokálnej adaptácie či auditu. Analýza je preto čiastočne hypotetická, postavená na

³ „Umelá inteligencia v náborovom procese“, [cit. 5.9.2025] Dostupné online: <https://www.manpower.sk/magazin/umela-inteligencia-v-naborovom-procese>

⁴ VAŠEČKA, M. (2022). Rómovia na Slovensku: Sociálna exklúzia a diskriminácia. In: Sociológia, roč. 54, č. 3, s. 215; HAMULÁK, J. [et al.]. (2022). Zamestnávanie osôb so zdravotným postihnutím a služby zamestnanosti. In: Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia [elektronický dokument]. 1. vyd. Bratislava: Právnická fakulta UK, ISBN 978-80-7160-659-8; s. 18.

medzinárodných skúsenostiach a aplikácii existujúceho právneho rámca na špecifické slovenské socio-ekonomické nerovnosti (napr. rómske komunity, rodové rozdiely).

Algoritmická spravodlivosť v kontexte náborovania

Algoritmická spravodlivosť skúma, do akej miery modely a systémy strojového učenia produkujú výsledky, ktoré sú rovné alebo neutrálne voči chráneným skupinám. V kontexte náborovania sa táto problematika stáva obzvlášť akútnou, keďže rozhodnutia o prijatí do zamestnania majú priamy dopad na životné príležitosti jednotlivcov.

AI a diverzita v náborových procesoch

Moderné náborové platformy dokážu optimalizovať jazyk pracovných inzerátov tak, aby nepôsobil odrádzajúco na určité skupiny uchádzačov. Odstraňovanie stereotypných výrazov zvyšuje šancu, že sa o pracovnú pozíciu uchádzajú aj ženy, príslušníci etnických menšín alebo osoby vo vyššom veku. Ďalším pozitívnym prvkom je rozšírenie okruhu uchádzačov: algoritmy dokážu cielene vyhľadávať vhodných kandidátov aj na profesionálnych sieťach a databázach, čím znižujú závislosť od osobných kontaktov.

Pri predvýbere AI často prideluje kandidátom skóre podľa objektívnych kritérií, ako sú kvalifikácia, prax alebo jazykové znalosti. Tým sa očakáva redukcia subjektívnych predsudkov personalistov a urýchlenie procesu.⁵ Tieto predpoklady však nie vždy zodpovedajú realite.

Algoritmus je len tak spravodlivý, ako sú spravodlivé dáta, na ktorých sa učí. Ak historické údaje o úspešných kandidátoch odrážajú skôr mužské, majoritné alebo bezdetné profily, AI má tendenciu reprodukovать tieto preferencie. Klasickým príkladom je medializovaný prípad spoločnosti Amazon, kde interný náborový algoritmus znevýhodňoval ženy pri prijímaní do technických pozícií, pretože bol trénovaný na dátach zo životopisov prevažne mužských uchádzačov.⁶

Fázy náborového procesu a ich špecifiká

Inzeráty a vyhľadávanie kandidátov: V úvodných štádiách náboru zohráva AI úlohu pri optimalizácii pracovných inzerátov, čím dokáže eliminovať stereotypné

⁵ LÄSSIG, N., OPPOLD, S. a HERSCHEL, M. (2022) Metrics and Algorithms for Locally Fair and Accurate Classifications using Ensembles. In: Datenbank Spektrum, roč. 23, s. 4, [cit. 2025-09-05]. Dostupné na: <https://doi.org/10.1007/s13222-021-00401-y>

⁶ The guardian. Amazon ditched AI recruiting tool that favored men for technical jobs, [cit. 5.9.2025] Dostupné na : <https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>

formulácie a osloviť širšie spektrum uchádzačov vrátane marginalizovaných skupín. Tým sa zvyšuje pravdepodobnosť, že o pozície budú žiadať aj ženy, etnické menšiny či starší pracovníci. Algoritmy zároveň vyhľadávajú potenciálnych kandidátov na online platformách, čím rozširujú diverzitu tzv. talent poolu.⁷ Automatizované generovanie textu môže byť optimalizované pre inkluzívnejší jazyk, avšak bez kontrolných mechanizmov môže vytvoriť skreslený tón, ktorý priťahuje skôr určité demografické skupiny. Algoritmické vyhľadávanie môže navyše preferovať kandidátov s oveľa viditeľnejšími online stopami, čo môže napr. znevýhodňovať marginalizované skupiny s obmedzeným prístupom na internet.

Skríning životopisov a bodovanie: V skríningovej fáze AI priraduje kandidátom skóre podľa objektívnych kritérií (jazykové znalosti, skúsenosti, kvalifikácia), čím sa predpokladá redukcia ľudských predsudkov. Okrem toho AI dokáže v krátkom čase spracovať obrovské množstvo údajov, čo zefektívňuje celý proces. Systémy, ktoré automaticky pridelujú skóre, často používajú meracie nástroje nastavené napr. na historických úspechoch. Ak sú historické úspechy zaujaté, skóre bude reprodukovat tento vzor; navyše uchádzači často nedostanú spätnú väzbu ani vysvetlenie pre svoje vylúčenie. To komplikuje možnosť právnej nápravy v zmysle článku 22 GDPR.

Video-interview a finálny výber: Aj keď je osobný pohovor naďalej kľúčovou časťou náborového procesu, umelá inteligencia ho výrazne mení. Hoci plne automatizované pohovory sú zatiaľ neobvyklé, AI pomáha pri formulovaní otázok alebo plánovaní termínov. Tzv. chatboty vedú v prvom kole pohovoru viesť konverzáciu a odpovedať uchádzačom na otázky, čo pomáha udržať ich záujem. Niektoré nástroje AI analyzujú reakcie uchádzačov, ich tón hlasu a výrazy tváre počas video-pohovorov. AI takisto zefektívňuje záverečnú fázu výberu, v ktorej pomáha určiť prínosy a riziká spojené s jednotlivými kandidátmi a predpovedať, ktorý z nich je najvhodnejší pre danú pozíciu.

Mechanizmy vzniku algoritmickej diskriminácie

Zdroje a riziká algoritmickej diskriminácie

Riziko algoritmickej diskriminácie má dve hlavné príčiny. Prvou je kvalita vstupných dát. Ak sú tzv. tréningové súbory nereprezentatívne alebo obsahujú historické predsudky, AI ich preberá ako „štandard“ a reprodukuje ich vo svojich rozhodnutiach. To vedie k systematickému znevýhodňovaniu určitých skupín, hoci formálne kritériá vyzerajú neutrálne.⁸

⁷ Pozn. Talent pool je databáza tzv. vopred identifikovaných a preverených kandidátov, interných aj externých, ktorí majú potenciál pre budúce pozície alebo projekty vo firme.

⁸ RUDŽIKOVÁ, D. (2024). Vplyv AI na pracovné právo. In: Inovatívne právo a inovácie v práve. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, ISBN 978-80-574-0346-3, s. 33.

Druhým zdrojom predsudkov sú chyby v samotnom návrhu algoritmu, tzv. bias by design. Už vo fáze vývoja rozhodujú programátori, ktoré atribúty budú hodnotené a akú váhu im algoritmus prideli. Ak sú preferované lineárne kariérne dráhy bez prestávok, môžu byť penalizovaní kandidáti, ktorí mali pauzy v zamestnaní napríklad z dôvodu starostlivosti o deti. Hoci sa tieto nastavenia nemusia javiť ako zámerne diskriminačné, výsledok môže byť nespravodlivý.

Empirické dôkazy diskriminácie

Problém algoritmickej nespravodlivosti je komplexný a má korene vo viacerých fázach vývoja a implementácie AI systémov. Najčastejší a najštudovanejší zdroj predsudkov pochádza z tzv. trénovacích dát. Ak dáta, na ktorých sa algoritmus učí, odrážajú historické alebo spoločenské nerovnosti, algoritmus sa ich naučí a nespravodlivosť automaticky replikuje.

Príkladom je štúdia ProPublica z roku 2016, ktorá ukázala, že softvér COMPAS, používaný na predikciu rizika recidívy v americkom súdnictve, predikoval s vyššou pravdepodobnosťou recidívu u Afroameričanov než u belochov, a to aj pri kontrole iných premenných.⁹ Podobne, ak systém na rozpoznávanie tváre dosahuje horšiu presnosť pre osoby s tmavšou pleťou, je to často dôsledok toho, že tzv. trénovacie dáta obsahovali prevahu tvárí svetlej pleti.¹⁰

Intersekcionalita a kumulatívne nevýhody

Diskriminácia sa často nevyskytuje iba na jednej osi identity; intersekcionalita poukazuje na to, že rod, etnicita, vek, zdravotný stav a sociálno-ekonomické faktory sa môžu navzájom prekrývať a vytvárať špecifické zraniteľné pozície.¹¹ Pre slovenské podmienky to napríklad znamená, že rómske ženy môžu čeliť kumulatívnej nevýhode, ktorá bude algoritmicke zosilnená, ak systém nerozpozna alebo nekompenzuje tieto širšie spoločenské súvislosti.

⁹ ANGWIN, J., LARSON, J., MATTU, S. a KIRCHNER, L. (2016). Machine Bias---There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks [online]. New York: ProPublica, s. 559 [cit. 2025-09-11]. Dostupné na: <https://www.scirp.org/reference/referencespapers?referenceid=3337609>.

¹⁰ BUOLAMWINI, J. a GEBRU, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of the 1st Conference on Fairness, Accountability, and Transparency, s. 2 [online] [cit. 2025-09-13]. Dostupné na: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

¹¹ CRENSHAW, K. (1989). Demarginalizing the Intersection of Race and Sex. In: University of Chicago Legal Forum [online], roč. 1989, č. 1, s. 151. [cit. 2025-09-11]. Dostupné na: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1052&context=uclf>.

Špecifické mechanizmy diskriminácie v náboře

AI systémy sa učia z historických dát, pričom ak sú tieto dáta ovplyvnené spoločenskými predsudkami (napr. historicky viac prijatých mužov na technické pozície), model ich dokáže reprodukovat' a legitimizovat'.¹² Odstránenie explicitných citlivých premenných (pohlavie, rasa) nemusí stačiť - množstvo neexplicitných premenných (PSČ, typ školy, jazykové konštrukcie) funguje ako proxy pre pohlavie, etnicitu alebo sociálny status a algoritmus ich môže použiť na diskrimináciu.¹³

Predvoľby tvoriace tzv. váhovanie kritérií, výber features, či penalizácia kariérnych prerušení sú príkladmi bias by design - konštruktérské rozhodnutia, ktoré môžu byť neúmyselne diskriminačné.¹⁴ Aj keď algoritmus poskytuje „skóre“, jeho interpretácia človekom môže viesť k ďalšej polarizácii. Ak napríklad HR pracovník slepo dôveruje skóre bez pochopenia jeho limitov, diskriminačné vzory sa ešte zosilnia.¹⁵

Algoritmy ovplyvňujú každú fázu náboru, od tvorby inzerátov, cez vyhľadávanie vhodných kandidátov, skríning životopisov, video-pohovory a finálny výber. V každej z týchto fáz sa objavujú špecifické riziká pre rodové a etnické skupiny, ako napr. jazyk inzerátu (odradzujúc mužov alebo ženy), modely penalizujúce „ženské“ slová, video-analýza s nižšou presnosťou pri tmavej pokožke a pod.¹⁶

Právny a etický rámec

Výzvy pre pracovné právo

S ohľadom na právny a etický rozmer používania AI v náborovom procese vznikajú pre pracovné právo tieto kľúčové výzvy:

Diskriminácia a predsudky: Z pohľadu pracovného práva je kľúčovou hrozbou algoritmická diskriminácia. Algoritmy môžu replikovat' alebo dokonca zosilňovat'

¹² BAROCAS, S., HARDT, M. a NARAYANAN, A. (2019). Fairness and Machine Learning [online], s. 210 [cit. 2025-09-12]. Dostupné na: <https://fairmlbook.org/pdf/fairmlbook.pdf>.

¹³ GORDON, F. (2019). Virginia Eubanks (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: Picador, St Martin's Press. In: Law, Technology and Humans [online], roč. 1, november, s. 162. [cit. 2025-09-12]. Dostupné na: <https://doi.org/10.5204/lthj.v1i0.1386>.

¹⁴ LUPETTI, M., MURRAY-RUST, D., CANGIANO, S. a MELA, A. (2025). Speculative AI Prototyping: From Measuring Bodies to Confronting Ideals. In: Interactions [online], roč. 32, č. 5, s. 11 [cit. 2025-09-12]. Dostupné na: <https://dl.acm.org/doi/pdf/10.1145/3757748>.

¹⁵ WACHTER, S., MITTELSTADT, B. a FLORIDI, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. In: International Data Privacy Law [online], roč. 7, č. 2, s. 2, [cit. 2025-09-12]. Dostupné na: <https://doi.org/10.1093/idpl/ixx005>.

¹⁶ BUOLAMWINI, J. a GEBRU, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of the 1st Conference on Fairness, Accountability, and Transparency [online], s. 2, [cit. 2025-09-13]. Dostupné na: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

historické predsudky, ktoré sa vyskytujú v spoločnosti. Ak je algoritmus na výber kandidátov trénovaný na historických dátach, v ktorých boli úspešnejší muži, môže v budúcnosti preferovať mužských uchádzačov, a to aj nevedomky a bez explicitného programovania. Tým by dochádzalo k nepriamej diskriminácii, ktorá je v zmysle antidiskriminačného zákona zakázaná.¹⁷

Transparentnosť a zdôvodnenie výberu: Pracovné právo sa opiera o zásadu, že zamestnávateľ musí byť schopný odôvodniť svoje rozhodnutia, najmä ak ide o negatívne rozhodnutie (napr. odmietnutie uchádzača, prepustenie). Ak je rozhodnutie urobené „čiernou skrinkou“ (black-box) AI, ktorá neponúka transparentné vysvetlenie, stáva sa tento princíp neudržateľným.¹⁸

Systémy by mali byť navrhnuté tak, aby dokázali vysvetliť svoje rozhodnutia. Zamestnávateľ by mal uchádzačom o prácu a zamestnancom poskytnúť jasné informácie o tom, ako AI systém vyhodnotil ich profil alebo výkon. Ak je uchádzač o prácu zamietnutý, mal by mať možnosť získať vysvetlenie, ktoré by bolo zrozumiteľné a umožnilo by mu pochopiť dôvody odmietnutia.¹⁹

Dôkazné bremeno a štatistické údaje: Pracovné právo vyžaduje preukázanie existencie diskriminácie. Pri nepriamej diskriminácii, ktorá je v kontexte algoritmického náboru najčastejšia, sa dôkazné bremeno v zmysle antidiskriminačného zákona presúva. Uchádzačovi stačí predložiť dôkazy, z ktorých možno domnievať sa, že bol diskriminovaný. Ak napríklad algoritmus opakovane vylučuje kandidátov určitej etnickej skupiny, je možné použiť štatistické dáta o rozdelení výsledkov (disparate impact) ako dôkaz diskriminačného vzorca. Zamestnávateľ (používateľ) potom musí preukázať, že dané kritériá sú objektívne odôvodnené legitímnym cieľom a sú na jeho dosiahnutie nevyhnutné. Tento princíp reflektuje aj judikatúra Súdneho dvora EÚ, napr. vec C-109/88 Danfoss a vec C-127/92 Enderby, ktoré uznali použitie štatistických údajov ako relevantného nepriameho dôkazu diskriminačného účinku určitej praxe, hoci bez preukázania úmyslu. V kontexte algoritmického náboru sa tento prístup prejavuje v potrebe umožniť uchádzačovi prístup k vysvetleniu spôsobu hodnotenia a k agregovaným údajom o

¹⁷ § 2a ods. 3) ADZ: „nepriama diskriminácia je navonok neutrálny predpis, rozhodnutie, pokyn alebo prax, ktoré znevýhodňujú alebo by mohli znevýhodňovať osobu v porovnaní s inou osobou; nepriama diskriminácia nie je, ak takéto predpis, rozhodnutie, pokyn alebo prax sú objektívne odôvodnené sledovaním oprávneného záujmu a sú primerané a nevyhnutné na dosiahnutie takého záujmu“

¹⁸ 1. DAŇKO, M., PORUBAN, A. (2024) Práva a povinnosti zamestnancov v Akte o umelej inteligencii, In. Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024 - Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie 14. - 15. novembra 2024, Trenčín, s. 11, ISBN 978-80-8295-044-4

¹⁹ Článok 22 GDPR hovorí, že „Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.“ Ak teda algoritmus odmietne kandidáta, má právo požadovať preskúmanie tohto rozhodnutia človekom.

výsledkoch rôznych skupín. Ak systém vykazuje štatisticky významné rozdiely v úspešnosti uchádzačov podľa pohlavia alebo etnicity, vzniká prima facie domnienka diskriminácie, ktorú musí zamestnávateľ vyvrátiť.²⁰

Otázky zodpovednosti (Zamestnávateľ vs. Poskytovateľ): Kritickou výzvou je stanovenie zodpovednosti za diskriminačné rozhodnutie. Hoci konečné rozhodnutie o prijatí robí spravidla zamestnávateľ (používateľ), chybu alebo bias (predsudok) môže spôsobiť poskytovateľ (dodávateľ) HR-AI systému, napr. nevhodným tréningovým súborom dát. V prípade zistenia diskriminácie je nutné legislatívne jasne stanoviť, že poskytovatelia systémov majú primárnu povinnosť zabezpečovať kvalitu používaných dát a vykonávať interné testy spravodlivosti. Máme za to, že v zmysle právneho stavu *de lege lata* nesie hlavnú zodpovednosť za dodržiavanie antidiskriminačného zákona a iný pracovnoprávných predpisov zamestnávateľ, pretože on systém nasadil a robí na jeho základe rozhodnutia. Zmluvy medzi nimi musia obsahovať záruky a mechanizmy nápravy.

Spravodlivosť a ľudský dohľad (Human in the Loop): Žiadne rozhodnutie, ktoré má zásadný dopad na zamestnanca (ako napríklad prijatie, prepustenie alebo kariérny postup), by nemalo byť výlučne automatizované. AI by mala slúžiť len ako nástroj na podporu rozhodovania. Konečné rozhodnutie by mal vždy urobiť kvalifikovaný človek, ktorý prehodnotí odporúčania algoritmu a zváži širší kontext.

Delegovanie kritických rozhodnutí na algoritmy bez ľudského dohľadu je z hľadiska pracovného práva rizikové. Algoritmy môžu byť účinné, ale nemajú schopnosť posúdiť kontext, pochopiť ľudské faktory alebo zohľadniť výnimky.²¹

Európsky a národný právny rámec

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 (tzv. AI Act) považuje používanie AI v procese náboru (vrátane hodnotenia, profilovania, videopohovorov a rozhodovania o kariérnom postupe) za systémy s vysokým rizikom. Tieto systémy budú podliehať prísnyim pravidlám, ktoré ukladajú povinnosti ako hodnotenie zhody, zavádzanie prísneho ľudského dohľadu a zabezpečenie transparentnosti. Povinnosti dopadajú primárne na poskytovateľov (napr. riadenie rizík, kvalita dát,

²⁰ C-109/88, Handels- og Kontorfunktionærernes Forbund i Danmark v. Dansk Arbejdsgiverforening (Danfoss), ECLI:EU:C:1989:383, [cit. 05.11.2025] Dostupné online: <https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX:61988CJ0109>; C-127/92, Enderby v. Frenchay Health Authority, ECLI:EU:C:1993:859, [cit. 05.11.2025] Dostupné online: <https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX:61992CJ0127>

²¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 (tzv. AI Act) považuje používanie AI v pracovných pohovoroch za systémy s vysokým rizikom, pričom budú podliehať prísnyim pravidlám, pričom zamestnávateľia budú povinné vykonávať hodnotenie zhody, zaviesť prísny ľudský dohľad a zabezpečiť transparentnosť rozhodovacích procesov.

transparentnosť) a na používateľov (zamestnávateľov), ktorí musia zabezpečiť ľudský dohľad a monitorovať fungovanie systému.

Článok 22 GDPR ustanovuje, že „Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú“. Ak teda algoritmus odmietne kandidáta, má právo požadovať preskúmanie tohto rozhodnutia človekom.²²

Výklad kritérií Čl. 22 GDPR: V kontexte náboru je kľúčové kritérium „výlučne automatizovaného“ rozhodnutia. Ak zamestnávateľ pri náboře používa algoritmus len na skríning a finálne rozhodnutie prehodnotí človek (human in the loop), uplatniteľnosť čl. 22 sa obmedzuje. To však neoslobodzuje zamestnávateľa od povinnosti transparentnosti a ľudského dohľadu. Druhým kľúčovým kritériom je „významný účinok“, ktorý odmietnutie uchádzača o prácu, prirodzene, spĺňa, keďže priamo ovplyvňuje jeho životné príležitosti. Vďaka neúplnej aplikovateľnosti čl. 22 GDPR pri systémoch s ľudským dohľadom je potrebné explicitné legislatívne ukotvenie práva na vysvetlenie.

Situácia na Slovensku - Analýza a hodnotenie

Aktuálny stav implementácie AI v náboře

Na Slovensku chýba systematický zber a zverejňovanie údajov o algoritmickej náboře. Na slovenskom trhu sa v náborových procesoch najčastejšie využívajú zahraničné ATS systémy ako Teamio, Datacruit, Recrutee, Grafton/Manpower, Talentlyft či HireVue (posledný s prvkami analýzy videorozhovorov). Väčšina týchto systémov bola vyvinutá mimo SR a využíva cloudové riešenia bez lokálnej certifikácie alebo auditu z hľadiska algoritmickej spravodlivosti. Niektoré väčšie spoločnosti (najmä v IT sektore) využívajú vlastné moduly na predvýber kandidátov prostredníctvom kľúčových slov a hodnotenia profilov na platformách ako LinkedIn. Rámcový prehľad praxe naznačuje, že slovenské firmy, najmä stredné a väčšie, využívajú lokálne i globálne HR platformy, ktoré majú integrované AI funkcie na:

Automatické triedenie (scoring): Pridelovanie skóre na základe kvalifikácie a skúseností.

Talent Matching: Párovanie zručností v životopise s požiadavkami na danú rolu.

Automatizáciu hiringu: Pomoc pri tvorbe pracovných ponúk a hromadnom nahrávaní životopisov. Tieto nástroje sú často používané bez nezávislého auditu a transparentných národných pokynov. Z právneho hľadiska síce platia európske, resp.

²² DAŇKO, M., PORUBAN, A. (2024) Práva a povinnosti zamestnancov v Akte o umelej inteligencii, In. Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024 - Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie 14. - 15. novembra 2024, Trenčín, s. 14, ISBN 978-80-8295-044-4

vnútroštátne pravidlá (GDPR, antidiskriminačný zákon, prípadne AI Act), avšak implementačné nástroje - nezávislé auditorské kapacity, certifikácia systémov, a národné pokyny - sú nedostatočné.

Ako ilustráciu môžeme uviesť príklad spoločnosti pôsobiacej v službách, ktorá využívala ATS s funkciou automatického skórovania životopisov podľa kontinuity pracovnej histórie. Kandidátky po materskej dovolenke, ktoré mali niekoľkoročnú pauzu v zamestnaní, získavali nižšie skóre, hoci iné kritériá (vzdelanie, prax) boli porovnateľné. Po internom prehodnotení sa ukázalo, že algoritmus priradzoval penalizáciu za „neaktívne obdobie“ bez zohľadnenia jeho dôvodu. Tento model predstavuje typický príklad nepriamej diskriminácie na základe pohlavia, ktorá môže mať aj právne dôsledky, ak sa preukáže kauzálny vzťah medzi algoritmickým skórovaním a vylúčením uchádzačky.

Identifikované riziká v slovenskom kontexte

Medzi riziká, ktoré môžu v podmienkach Slovenskej republiky pri používaní AI v náboře vyplynúť, možno zahrnúť:

- Znevýhodnenie rómskych uchádzačov v dôsledku používania umelo namodelovaných vstupných ukazovateľov (napr. nedostupnosť internetového pripojenia, rozdielne vzdelanostné možnosti)
- Diskriminácia matiek a otcov po rodičovskej dovolenke kvôli výpadkom v praxi, ktoré algoritmy môžu hodnotiť negatívne
- Jazykové bariéry pri hodnotení kandidátov s iným materinským jazykom, kde AI systémy môžu nesprávne interpretovať jazykové nuansy
- Geografická diskriminácia založená na poštových smerových číslach alebo adresách bydliska

Odporúčania a návrhy riešení

Odporúčania pre prax

Keďže v podmienkach Slovenskej republiky nie sú jasne definované pravidlá, spoločnosti a zamestnávateľia, ktorí používajú AI v náboře a chcú sa vyhnúť právnym problémom, by mali zvážiť nasledovné opatrenia:

Audit používaných algoritmov: Vykonávanie nezávislých auditov prostredníctvom tretích osôb; Testovanie algoritmov na prítomnosť predsudkov a diskriminácie; Pravidelné overovanie výsledkov podľa rôznych demografických skupín.

Transparentnosť a komunikácia: Jasné informovanie zamestnancov a uchádzačov o používaní automatizovaných systémov; Vysvetlenie fungovania systémov zrozumiteľnou formou; Poskytovanie možnosti získať dodatočné informácie o rozhodnutiach.

Vzdelávanie a kompetencie: Školenie zamestnancov používajúcich AI systémy o rizikách; Výcvik v správnej interpretácii výsledkov; Budovanie kapacít pre kritické hodnotenie algoritmických odporúčaní

Zodpovednosť a dohľad: Určenie zodpovednej osoby za konečné rozhodnutia; Zabezpečenie ľudského prvku v rozhodovacích procesoch; Vytvorenie mechanizmov pre odvolanie a sťažnosti

Odporúčania pre legislatívu a exekutívu

Povinné nezávislé audity a publikovanie výsledkov: Zaviesť povinnosť vykonávať nezávislé audity algoritmov používaných pri náboře najmenej raz ročne a zverejňovať súhrnné výsledky. Tieto audity by mali hodnotiť rozdelenie výsledkov podľa pohlavia, národnosti, veku, zdravotného stavu, resp. iných chránených dôvodov v zmysle antidiskriminačného zákona a identifikovať rozdielne dopady na uchádzačov.

Právo na zdôvodnenie/vysvetlenie a ľudský zásah: Zakotviť v slovenskom právnom poriadku explicitné právo uchádzača žiadať o zmysluplné vysvetlenie rozhodnutí vykonaných s významnou automatizačnou zložkou a právo na preskúmanie človekom (ako doplnok k čl. 22 GDPR). To zahŕňa povinnosť poskytnúť uchádzačovi stručný opis procesu rozhodovania a opis hlavných faktorov, ktoré viedli k jeho vyhodnoteniu.

Transparentnosť rozhodovania a právo na informácie: Povinnosť zamestnávateľa informovať uchádzačov/kandidátov pri náboře o použití AI nástrojov, vrátane charakteru hodnotenia (bodovanie, video-analýza a pod.), o dostupných možnostiach odvolania proti rozhodnutiu, ako aj o kontakte na príslušný orgán zodpovedný za prípadné sťažnosti.

Certifikácia a vzdelávanie odborníkov: Zriadiť orgán (napr. agentúru pre AI dohľad), resp. systém certifikácie pre AI nástroje používané v náborovom procese, prípadne zaviesť povinné školenia HR zamestnancov o pravidlách a rizikách používania AI.

Zodpovednosť poskytovateľov a transparentné zmluvné podmienky:

Legislatívne jasne stanoviť, že poskytovatelia tzv. HR-AI systémov majú primárnu povinnosť zabezpečovať kvalitu používaných dát a vykonávať interné testy spravodlivosti. Zároveň jednoznačne vymedziť zodpovednosť zamestnávateľov za konečné rozhodnutia, pričom zmluvy medzi zamestnávateľmi a dodávateľmi týchto systémov by mali obsahovať dojednania o zárukách, prípadných nápravách v prípade zistenia diskriminácie.

Vyváženie inovácií a ochrany práv: V tejto súvislosti je potrebné uviesť, že zavádzanie regulácie vždy prináša kompromisy medzi inováciou a ochranou práv. Zabezpečiť úplnú „bezchybnosť“ AI je nereálne. Preto cieľom regulácie by malo byť znížovanie rizika diskriminácie na prijateľnú úroveň a zabezpečenie mechanizmov nápravy. Kľúčové bude to, aby sa na jednej strane nenarušila možnosť

zamestnávateľov efektívne nájsť kvalifikovaných zamestnancov, a na strane druhej, aby bola čo v najväčšej miere zabezpečená ochrana práva jednotlivcov na rovnaké zaobchádzanie v prístupe k zamestnaniu.

Záver

Algoritmický nábor predstavuje dvojsečný meč: môže pomôcť pri zlepšení inklúzie, ale rovnako ľahko môže systematicky prehľbovať rodové a etnické nerovnosti, ak nie sú zavedené mechanizmy kontroly a zodpovednosti. Analýza ukázala, že riziká algoritmickej diskriminácie v náborovom procese na Slovensku sú reálne a vyžadujú si komplexný prístup k riešeniu. Historické predsudky obsiahnuté v tréningových dátach, nedostatočná transparentnosť rozhodovacích procesov a absentujúci ľudský dohľad vytvárajú podmienky pre systematické znevýhodňovanie určitých skupín uchádzačov.

Pre Slovensko odporúčame kombináciu právnych opatrení (právo na vysvetlenie, povinné audity), organizačných zmien (vzdelávanie HR, mechanizmy sťažností) a technických požiadaviek (certifikácia, monitoring), ktoré by spoločne znížili riziká diskriminácie a posilnili dôveru v automatizované rozhodovanie. Úspešná implementácia týchto opatrení bude vyžadovať koordinovaný prístup všetkých zainteresovaných strán – od zákonodarcov cez zamestnávateľov až po samotných uchádzačov o prácu. Len tak bude možné využiť potenciál umelej inteligencie v náborovom procese pri zachovaní základných princípov spravodlivosti a rovnosti príležitostí. Budúci výskum by sa mal zamerať na empirické testovanie navrhnutých opatrení v praxi, analýzu ich vplyvu na efektívnosť náborových procesov a dlhodobé sledovanie dopadov na diverzitu a inklúziu na slovenskom trhu práce.

Zoznam použitej literatúry

1. ANGWIN, J., LARSON, J., MATTU, S. a KIRCHNER, L. (2016). *Machine Bias - There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks* [online]. New York: ProPublica [cit. 2025-09-11]. Dostupné na: <https://www.scirp.org/reference/referencespapers?referenceid=3337609>.
2. BAROCAS, S., HARDT, M. a NARAYANAN, A. (2019). *Fairness and Machine Learning* [online], 284 s. [cit. 2025-09-12]. Dostupné na: <https://fairmlbook.org/pdf/fairmlbook.pdf>.
3. BUOLAMWINI, J. a GEBRU, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: *Proceedings of the 1st Conference on Fairness, Accountability, and Transparency* [online] [cit. 2025-09-13]. Dostupné na: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

4. CRENSHAW, K. (1989). Demarginalizing the Intersection of Race and Sex. *In: University of Chicago Legal Forum* [online], roč. 1989, č. 1, s. 139-167 [cit. 2025-09-11]. Dostupné na: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1052&context=uclf>.
5. DAŇKO, M., PORUBAN, A. (2024) Práva a povinnosti zamestnancov v Akte o umelej inteligencii, *In. Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024 - Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie 14. - 15. novembra 2024, Trenčín*, s. 10-19, ISBN 978-80-8295-044-4
6. GORDON, F. (2019). Virginia Eubanks (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: Picador, St Martin's Press. *In: Law, Technology and Humans* [online], roč. 1, november, s. 162-164 [cit. 2025-09-12]. Dostupné na: <https://doi.org/10.5204/lthj.v1i0.1386>.
7. HAMULÁK, J. [et al.]. (2022). Zamestnávanie osôb so zdravotným postihnutím a služby zamestnanosti. *In: Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia* [elektronický dokument]. 1. vyd. Bratislava: Právnická fakulta UK, s. 197-308. ISBN 978-80-7160-659-8.
8. LÄSSIG, N., OPPOLD, S. a HERSCHEL, M. (2022). Metrics and Algorithms for Locally Fair and Accurate Classifications using Ensembles. *In: Datenbank Spektrum* [online], roč. 22, s. 23-43 [cit. 2025-09-05]. Dostupné na: <https://doi.org/10.1007/s13222-021-00401-y>.
9. LUPETTI, M., MURRAY-RUST, D., CANGIANO, S. a MELA, A. (2025). Speculative AI Prototyping: From Measuring Bodies to Confronting Ideals. *In: Interactions* [online], roč. 32, č. 5, s. 10-12 [cit. 2025-09-12]. Dostupné na: <https://dl.acm.org/doi/pdf/10.1145/3757748>.
10. RUDŽIKOVÁ, D. (2024). Vplyv AI na pracovné právo. *In: Inovatívne právo a inovácie v práve*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 30-38. ISBN 978-80-574-0346-3.
11. VAŠEČKA, M. (2022). Rómovia na Slovensku: Sociálna exklúzia a diskriminácia. *In: Sociológia*, roč. 54, č. 3, s. 215-232.
12. WACHTER, S., MITTELSTADT, B. a FLORIDI, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. *In: International Data Privacy Law* [online], roč. 7, č. 2 [cit. 2025-09-12]. Dostupné na: <https://doi.org/10.1093/idpl/ixp005>.

Judikatúra:

1. C-109/88, Handels- og Kontorfunktionærernes Forbund i Danmark v. Dansk Arbejdsgiverforening (Danfoss), ECLI:EU:C:1989:383, [cit. 05.11.2025] Dostupné na: <https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX:61988CJ0109;>

2. C-127/92, Enderby v. Frenchay Health Authority, ECLI:EU:C:1993:859, [cit. 05.11.2025] Dostupné na: <https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX:61992CJ0127THE>

Sekundárne zdroje a periodiká:

1. GUARDIAN. (2018). Amazon ditched AI recruiting tool that favored men for technical jobs [online] [cit. 2025-09-05]. Dostupné na: <https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>.
2. MANPOWER. [s.a.]. Umelá inteligencia v náborovom procese [online] [cit. 2025-09-05]. Dostupné na: <https://www.manpower.sk/magazin/umela-inteligencia-v-naborovom-procese>.

Kontaktné údaje

prof. JUDr. Juraj Hamulák, PhD.
juraj.hamulak@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Katedra pracovného práva a práva sociálneho zabezpečenia

AI - NÁSTROJ NEROVNOSTI ALEBO GARANT INKLÚZIE?¹

AI – A TOOL OF INEQUALITY OR A GUARANTEE OF INCLUSION?

Marcel Dolobáč²

Abstrakt: Príspevok sa zameriava na analýzu umelej inteligencie (AI) v pracovnoprávnom a širšom právnom kontexte, a to z perspektívy jej ambivalentného pôsobenia ako zdroja diskriminácie, ale aj potenciálneho nástroja inklúzie. Cieľom je identifikovať hlavné riziká spojené so zavádzaním AI do spoločenských procesov, medzi ktoré patrí algoritmická diskriminácia, sociálna selekcia a zásah do súkromia, monopolizácia technológií a deformácia pracovného trhu. Metodologicky príspevok vychádza z komparácie vybraných prípadových štúdií a rozhodnutí súdov v Európe aj USA, doplnených o analýzu aktuálnych strategických dokumentov a správ medzinárodných organizácií. Záver práce poukazuje na to, že hoci AI prináša zásadné riziká reprodukcie historických predsudkov a prehlbovania nerovností, môže byť zároveň prostriedkom na zjednodušenie prístupu k informáciám, podporu personalizovaného vzdelávania a demokratizáciu technológií prostredníctvom participatívnych projektov. Vedeckým prínosom práce je systematizácia právnych otázok, ktoré AI vyvoláva v súvislosti so zákazom diskriminácie a ochranou základných práv. Praktický prínos spočíva v identifikácii možných regulačných nástrojov a politík, ktoré by mohli zabezpečiť, aby AI podporovala inkluzívne prostredie a slúžila verejnému záujmu.

Kľúčové slová: umelá inteligencia; diskriminácia; inklúzia; pracovné právo; algoritmická spravodlivosť

Abstract: The paper focuses on the analysis of artificial intelligence (AI) in the context of labour law and broader legal frameworks, examining its ambivalent role as both a source of discrimination and a potential tool of inclusion. The aim is to identify the main risks associated with the deployment of AI in societal processes, including algorithmic discrimination, social selection and privacy concerns, monopolisation of technologies, and labour market disruption. Methodologically, the paper builds on a comparative analysis of selected case studies and court decisions in Europe and the United States, complemented by

¹ Článok bol spracovaný v rámci riešenia grantového projektu VEGA č. 1/0291/23 „Legislatívne výzvy pre pracovné právo pri tvorbe diverzných a inkluzívnych pracovísk“.

² Právnická fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach

an examination of current strategic documents and reports of international organisations. The findings highlight that while AI entails significant risks of reproducing historical biases and deepening inequalities, it can also serve as an instrument to facilitate access to information, promote personalised education, and democratise technology through participatory projects. The scientific contribution of the paper lies in the systematisation of legal issues raised by AI in relation to the prohibition of discrimination and the protection of fundamental rights. The practical contribution is the identification of regulatory tools and policies that could ensure AI fosters an inclusive environment and serves the public interest.

Key words: artificial intelligence; discrimination; inclusion; labour law; algorithmic justice

Úvod

Dnes, pri plejáde vedeckých, odborných, laických či lifestylových príspevkov nikto nepochybuje, že rozvoj umelej inteligencie (ďalej len „AI“) patrí medzi najzásadnejšie technologické a spoločenské zmeny 21. storočia. Tento nový fenomén smelo môžeme považovať za zdroj novej technologickej revolúcie, obdobne ako Guttenbergovu kníhtlač, Wattov parný stroj, či relatívne nedávny nástup internetu. Rovnako, napokon rečou historickej skúsenosti - ako pri každej priemyselnej revolúcii, potenciál nových technologických zmien spojených s AI je ambivalentný: na jednej strane máme strach a obavy z nepoznaného, uvedomujeme si riziká straty kontroly nad rozhodovaním a zásadnú zmenu spoločenských vzťahov; na strane druhej umožňuje efektívnejšie poskytovanie služieb, prístupnosť pre široký okruh osôb a nečakané možnosti za pomerne nízku cenu.

Cieľom tohto príspevku je analyzovať právne, presnejšie azda pracovnoprávne riziká nástupu AI vo vzťahu k zásadu diskriminácie. Skúmame riziko reprodukovania spoločenských predsudkov, prehľbovania digitálnej priepasti a oslabovania individuálnych práv. Súčasne však sa príspevok zamýšľa na zlepšení postavenie osôb zdravotným postihnutím či efektívnejšie využívanie verejných zdrojov. Základná otázka preto znie: je AI nástrojom nerovnosti, alebo môže byť naopak garantom inklúzie?

AI ako nástroj nerovnosti

AI možno definovať ako systémy, ktoré vykazujú inteligentné správanie tým, že analyzujú prostredie a podnikajú kroky s istou mierou samostatnosti na dosiahnutie

cieľov.³ Môže ísť o softvérové riešenia (hlasoví asistenti, systémy rozpoznávania hlasu a obrazu, vyhľadávače) aj hardvérové zariadenia (autonómne vozidlá, roboty, drony, internet vecí). Vďaka hĺbkovému učeniu sa výkon v úlohách ako rozpoznávanie obrazu alebo reči zvýšil natolko, že v niektorých prípadoch prekračuje schopnosti človeka.⁴ Systémy AI sú pritom existenčne závislé od dát. Strojové učenie využíva veľké množstvá označených údajov na hľadanie vzorcov a ich aplikáciu na nové prípady. Tieto technické základy majú zásadné dôsledky pre pracovné právo, ochranu osobných údajov aj pre otázku rovnosti. AI prináša nový model spolupráce človeka a stroja, ktorý môže byť na jednej strane emancipujúci, no na druhej reprodukovat' alebo prehľbovať nerovnosti.⁵

Početnosť identifikovaných rizík spojených s nástupom AI do pracovného a bežného života a ich pomenovanie variuje. Z pohľadu autora (a pre účely ďalšieho zostročeného výkladu) ich vieme kategorizovať na nasledovné štyri:

- *algoritmická diskriminácia* – riziko prenesenia historických predsudkov ukrytých v dátach do rozhodovacej činnosti;
- *sociálna selekcia, prílišný dohľad a zásah do súkromia* - riziko diskriminácie spočíva vo vyhodnocovaní osobných údajov a informácií súkromnej povahy, ku ktorým sa taktiež môžu viazať predsudky;
- *monopolizácia technológií* – riziko náskoku veľkých nadnárodných korporácií, ktoré kontrolujú prístup k dátam a infraštruktúre, čo môže vytvárať digitálnu priepasť;
- *deformácia pracovného trhu* – riziko prekarizácie a znevýhodnenia menej kvalifikovaných.

Algoritmická diskriminácia

Podľa dostupných štatistík po pandémie COVID-19 využíva umelú inteligenciu v oblasti ľudských zdrojov až 88 % spoločností na celom svete, pričom 67 % personalistov je presvedčených, že jej aplikácia má pozitívny vplyv na proces náboru.⁶ Za hlavné prínosy sa považuje najmä urýchlenie výberového konania a zníženie nákladov zamestnávateľa. Využívanie AI v náborovom procese sa preto označuje aj

³ OECD (2019): *Recommendation of the Council on Artificial Intelligence*. OECD Legal Instruments, OECD/LEGAL/0449. Dostupné na <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>. Pozri analýzu YEUNG, K.: *Introductory Note to Recommendation of the Council on Artificial Intelligence*. In: *International Legal Materials*, Volume 59, Issue 1, February 2020, pp. 27 - 34

⁴ LeCUN, Y. - BENGIO, Y. – HINTON, G.: *Deep learning*. In: *Nature*, Vol. 521, 2015, pp. 436–444

⁵ Pozri V. DE STEFANO, "Negotiating the algorithm": Automation, artificial intelligence, and labor protection, in *Comparative Labor Law & Policy Journal*, Vol. 41, č. 1, 2019

⁶ PANTELAKIS, A. Top AI in Hiring statistics in 2024. In: Resource for employers [online]. Január 2024. Citované z RUDŽIKOVÁ, Denisa. Vplyv AI na pracovné právo. In: *Inovatívne právo a inovácie v práve*. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2024., s. 30-38.

ako „nová éra ľudských zdrojov“ – technológia preberá rutinné úlohy, čím umožňuje personalistom venovať viac času strategickému plánovaniu a mení tradičný model náboru. Za kľúčový prínos sa však vo väčšine prípadov považuje zvyšovanie kvality výberového procesu a mnohokrát redukcia nevedomých predsudkov, čo môže významne prispieť k podpore diverzity na pracovisku. Mnohí autori celkom správne však poukazujú na opak, a vysvetľujú tzv. algoritmickú diskrimináciu.⁷

Podstatu algoritmickej diskriminácie môžeme ilustrovať na niekoľkých prípadoch. Jeden z najviac pertraktovanou je kauza vo veci Amazon. Amazon vyvíjal interný náborový algoritmus (AI tool) s cieľom automatizovať triedenie životopisov a výber kandidátov. Tento systém sa však ukázal byť predpojatosťou voči ženám — algoritmus znižoval skóre kandidátkam alebo ich preferoval menej v technických pozíciách, lebo bol trénovaný na historických dátach prevažne mužských uchádzačov. Konkrétne, algoritmus bol trénovaný na historických životopisoch, ktoré odrážali fakt, že väčšinu technických pozícií v Amazon obsadzovali muži. Systém penalizoval slová ako „*women's*“ (napr. „women's chess club captain“) alebo životopisy zo škôl s vyšším podielom žien. Tím, ktorý testoval model, si všimol, že AI dáva **nižšie skóre kandidátkam** a posilňuje genderové stereotypy. Keď Amazon zistil tieto zaujatosti, projekt bol nakoniec odložený a algoritmus stiahnutý.⁸

Ak opustíme priestor pracovného práva, ale ostaneme v oblasti algoritmickej diskriminácie - v Spojených štátoch amerických sa širokej pozornosti dostal prípad **State v. Loomis (2016)**,⁹ v ktorom bol súdny orgán pri rozhodovaní o výške trestu ovplyvnený algoritmom COMPAS.¹⁰ Tento systém vychádzal z historických dát, ktoré obsahovali prvky rasovej a rodovej zaujatosti, čím sa vytváral reálny rizikový profil diskriminácie. Predmetom sporu bol obžalovaný Eric Loomis, ktorý čelil obvineniu za účasť na strelbe a následný útek pred políciou. Pri ukladaní trestu súd využil hodnotenie rizika recidívy generované algoritmom COMPAS, čo vyvolalo zásadné námietky zo strany obhajoby. Loomis tvrdil, že takýto postup porušuje jeho právo na spravodlivý proces (due process), a to z viacerých dôvodov: algoritmus bol proprietárny a jeho vnútorné fungovanie zostalo pre obhajobu neprístupné („black box“), zároveň sa poukazyvalo na možnú diskrimináciu na základe pohlavia a rasy a napokon aj na fakt, že sudca sa pri odôvodnení trestu výslovne odvolal na výstup algoritmu. Najvyšší súd štátu Wisconsin napokon rozhodol, že použitie COMPAS-u nie je protiústavné, avšak stanovil limity jeho aplikácie: algoritmické hodnotenie nesmie byť rozhodujúcim faktorom pri ukladaní trestu, ale môže pôsobiť len ako

⁷ RUDŽIKOVÁ, Denisa. Vplyv AI na pracovné právo. In: Inovatívne právo a inovácie v práve. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2024, s. 30-38

⁸ LANGEKAMP, M – COSTA, A. – CHEUNG, CH.: *Hiring Fairly in the Age of Algorithms*. Dostupné na <https://ssrn.com/abstract=3723046> or <http://dx.doi.org/10.2139/ssrn.3723046>

⁹ Dostupné na <https://harvardlawreview.org/print/vol-130/state-v-loomis/>

¹⁰ Correctional Offender Management Profiling for Alternative Sanctions

doplňkový informačný zdroj. Tento prípad je dnes často uvádzaný ako ilustrácia rizík algoritmického rozhodovania v trestnom práve, osobitne v súvislosti s otázkami transparentnosti, diskriminácie a ochrany práv obhajoby. V európskom právnom prostredí pritom rezonujú analogické diskusie týkajúce sa využívania tzv. risk assessment systémov v trestnej justícii.

Podobný jav bol zaznamenaný aj v Spojenom kráľovstve počas pandémie COVID-19 (*A-level scandal*, 2020). V roku 2020 boli vo Veľkej Británii zrušené tradičné písomné skúšky A-level a GCSE. Namiesto nich bol zavedený systém tzv. *calculated grades*, v rámci ktorého učitelia navrhli predpokladané známky (centre assessed grades, CAGs) a zaradili žiakov podľa poradia v danom predmete. Tieto návrhy však nepodliehali priamemu schváleniu, ale boli upravované prostredníctvom algoritmu vyvinutého regulačným úradom Ofqual.¹¹ Cieľom algoritmu bolo zabezpečiť, aby výsledné rozdelenie známok zodpovedalo historickým trendom a aby sa zabránilo inflácii hodnotení. Algoritmus pritom zohľadňoval historický výkon školy v jednotlivých predmetoch, predchádzajúce výsledky študentov (najmä GCSE) a tiež poradie žiakov určené učiteľmi. V praxi to znamenalo, že navrhované známky učiteľov boli často významne redukované. Až 40 % študentov zaznamenalo zníženie svojich očakávaných známok, čo malo zásadné dôsledky pre ich možnosti prijatia na univerzity a ďalšie vzdelávacie dráhy. Osobitne boli postihnutí študenti zo škôl s horším historickým výkonom alebo z menej prestížneho prostredia, keďže ich navrhované známky boli systematicky častejšie znižované. Naproti tomu žiaci prestížnych, často súkromných škôl mali vyššiu šancu zachovať alebo dokonca zlepšiť svoje hodnotenie. Tento postup bol preto široko vnímaný ako nespravodlivý a diskriminačný. Po rozsiahlej verejnej kritike, protestoch študentov a tlaku zo strany odbornej i politickej verejnosti vláda spolu s Ofqual od algoritmicky upravených známok ustúpili. Výsledkom bolo, že študenti nakoniec dostali známky pôvodne navrhnuté učiteľmi (CAGs).¹² Uvedená kauza sa používa ako *učebnicový príklad „bias in AI“* – algoritmus nebol neutrálne technický nástroj, ale reprodukoval existujúce štrukturálne nerovnosti v školskom systéme.

Z uvedených prípadov môžeme usúdiť záver, že algoritmickú diskrimináciu možno chápať ako kvalitatívne novú formu diskriminačného konania. Nejde o technické nedostatky alebo chyby v programovaní, musíme mať na pamäti, že AI sa učí sama a historické dáta vyhodnocuje iba na základe rámcových pokynov. Diskriminácia, je latentná a vzniká z komplexnej súhry modelových parametrov, historických dát a štatistických vzorcov. V dôsledku toho pôsobí nenápadne, je ťažko identifikovateľná a systematicky reprodukováaná. Závažným dôsledkom je práve jej neviditeľnosť.

¹¹ Office of Qualifications and Examinations Regulation

¹² Kelly, Anthony. "A tale of two algorithms: The appeal and repeal of calculated grades systems in England and Ireland in 2020." *British Educational Research Journal*, 47(3), 725–741, 2021.

Dotknuté osoby si často neuvedomujú, že boli hodnotené automatizovaným spôsobom, a nemajú prístup k informáciám o tom, aké faktory ovplyvnili výsledok. To oslabuje ich možnosti efektívnej obrany. Situáciu ešte zhoršuje spoločenská legitimizácia umelej inteligencie – jej výstupy sú vnímané ako objektívne a neutrálne, hoci v skutočnosti môžu maskovať a reprodukovать hlboko zakorenené štrukturálne skreslenia.

Sociálna selekcia, prílišný dohľad a zásah do súkromia

Riziko sociálnej selekcie a neúmerneho zásahu do súkromia AI môžeme opätovne ilustrovať na dvoch prípadových štúdiách. Prípad **SyRI v. Holandsko (2020)** predstavuje kľúčový moment v diskusii o hraniciach využívania algoritmickej systémov vo verejnej správe. Systém SyRI (*System Risk Indication*) bol navrhnutý holandskou vládou s cieľom odhaľovať sociálne podvody, ako sú neoprávnené čerpanie sociálnych dávok, nelegálne zamestnávanie či daňové úniky. Jeho fungovanie spočívalo v prepájaní a analýze rozsiahlych údajov z rôznych verejných databáz, vrátane údajov o sociálnom poistení, daňových záznamoch, bývaní či zdravotnej starostlivosti. Na základe týchto dát systém označoval jednotlivcov alebo skupiny ako „rizikové“.

Národný súd v Holandsku (Rechtbank Den Haag) konštatoval,¹³ že prevádzka SyRI porušuje článok 8 Európskeho dohovoru o ľudských právach, ktorý garantuje právo na rešpektovanie súkromného života. Argumentácia súdu sa opierala o viacero zásadných dôvodov. Po prvé, súd upozornil na **neprimeranosť** – rozsiahly zber a prepojovanie citlivých dát neboli dostatočne odôvodnené potrebami demokratickej spoločnosti. Po druhé, poukázal na **nedostatok transparentnosti**, keďže občania nemali možnosť získať informácie o tom, ako systém funguje a akými kritériami sa riadi, čo prakticky znemožňovalo akúkoľvek efektívnu kontrolu jeho zákonnosti. Po tretie, súd upozornil na vysoké **riziko diskriminácie**: hoci priamy diskriminačný účinok nebol preukázaný, existovala reálna obava, že systém bude viesť k systematickému profilovaniu chudobných a zraniteľných skupín obyvateľstva. Rozhodnutie v prípade SyRI tak nastavilo jasný rámec pre posudzovanie proporcionality, transparentnosti a potenciálnych diskriminačných účinkov pri zavádzaní algoritmickej nástrojov do verejného sektora.¹⁴

¹³ Spisové číslo: C-09-550982-HA / ZA 18-388

¹⁴ Pozri bližšie Naomi Appelman, Ronan Ó Fathaigh, and Joris van Hoboken, Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, 12 (2021) JIPITEC 257 para 1. Dostupné <https://www.jipitec.eu/jipitec/article/download/324/317/1610>.

Vo veci **C-203/22 CK proti Magistrat der Stadt Wien**¹⁵ sa Súdny dvor EÚ zaoberal otázkou rozsahu práva subjektu údajov na prístup k „významným informáciám o logike“ použitej pri automatizovanom rozhodovaní podľa článku 15 ods. 1 písm. h) GDPR. Spor vznikol po tom, čo rakúska spoločnosť Dun & Bradstreet odmietla poskytnúť CK úplné vysvetlenie algoritmu, ktorým bola hodnotená jej bonitná spôsobilosť pri uzatváraní zmluvy. Argumentovala pritom ochranou obchodného tajomstva. Okresný a federálny správny súd v Rakúsku konštatovali porušenie práva na prístup k informáciám, pričom otázka vyváženia medzi právom na transparentnosť a ochranou obchodného tajomstva bola predložená Súdnemu dvoru EÚ. Ten vo svojom rozsudku z 27. februára 2025 (ECLI:EU:C:2025:117) zdôraznil, že prevádzkovatelia musia poskytnúť dostatočne zrozumiteľné informácie umožňujúce jednotlivcovi pochopiť podstatu automatizovaného rozhodnutia, a to aj napriek tomu, že podrobnosti algoritmu môžu byť chránené ako obchodné tajomstvo.

Čo možno vyvodiť? Obe označené rozhodnutia spája dôraz na potrebu transparentnosti a proporcionality pri využívaní algoritmických systémov verejnými či súkromnými inštitúciami. V prípade SyRI holandský súd zdôraznil, že rozsiahle prepojenie dát zo strany štátu bez dostatočnej kontroly a prístupu občanov k informáciám o fungovaní systému je neprimerané a v rozpore s právom na súkromie podľa čl. 8 EDLP. V prípade CK proti Magistrat der Stadt Wien Súdny dvor EÚ potvrdil, že aj v súkromnoprávných vzťahoch musí byť zachované právo jednotlivca na zrozumiteľné informácie o logike algoritmického rozhodovania podľa čl. 15 GDPR, a to aj vtedy, keď sa prevádzkovatelia odvolávajú na ochranu obchodného tajomstva. Spoločným menovateľom oboch prípadov je teda napätie medzi efektivitou algoritmických nástrojov a základnými právami jednotlivcov. Súdne orgány v oboch rozhodnutiach zdôraznili, že technologická komplexnosť ani hospodárske či administratívne záujmy nemôžu odôvodniť úplnú netransparentnosť. Z oboch sporov možno vyvodiť záver, že algoritmické systémy musia byť konštruované a aplikované spôsobom, ktorý je nielen zákonne predvídateľný a kontrolovateľný, ale aj spravodlivý a prístupný dotknutým osobám. Tieto rozhodnutia tak posúvajú štandard ochrany základných práv v digitálnom prostredí a posilňujú požiadavku, aby umelá inteligencia a automatizované rozhodovanie slúžili verejnému záujmu bez diskriminačných či netransparentných efektov.

Monopolizácia technológií

V oblasti umelej inteligencie a dátových technológií sa čoraz intenzívnejšie objavujú pojmy ako **digitálna priepasť** a **data colonialism**, ktoré poukazujú na nerovnováhu v prístupe k zdrojom, moci a zisku. Digitálna priepasť sa netýka iba prístupu k hardvéru

¹⁵ Court of Justice of the European Union. (2025, February 27). *Case C-203/22, CK v. Magistrat der Stadt Wien*, ECLI:EU:C:2025:117.

a internetu — kým veľké technologické spoločnosti disponujú obrovskou výpočtovou silou, rozsiahlymi dátovými zbierkami a odborným know-how, mnohé menšie subjekty, chudobnejšie regióny či jednotlivci sú z tejto ekosystémovej hry vylúčení. Tí, čo majú kontrolu nad údajmi a výpočtovými kapacitami, môžu dominovať technologické procesy, rozhodovanie a inovácie, čím sa rozdiely medzi „veľkými hráčmi“ a okrajovými aktérmi ďalej prehlbujú. S konceptom **data colonialism** sa spája kritika, že technologické giganty „ťažia“ údaje z verejnosti — získavajú surové dáta zo sociálnych sietí, aplikácií, senzorov a infraštruktúr — zatiaľ čo hodnota, analýza a rozhodovacie mechanizmy zostávajú sústredené u nich. Tento vzťah podľa časti odborení a vedeckej spisby pripomína koloniálne vzorce, v ktorých bola kolonizovaná krajina vysávaná z prírodných zdrojov, no kontrolu, spracovanie a profit držala materská mocnosť. V digitálnom priestore to znamená, že krajiny alebo komunity poskytujú dáta — ale majú len veľmi obmedzený prístup k tomu, ako sa s nimi narába, rozhoduje sa a zneužíva sa ich potenciál.¹⁶

Deformácia pracovného trhu

Deformácie pracovného trhu sa dotkneme len v krátkosti, zmena je úplne nespochybniteľná. **Medzinárodný menový fond (IMF)** vo svojej správe z januára 2024 upozornil, že rozvoj AI môže ovplyvniť až **40 % pracovných miest na celom svete**, pričom v rozvinutých ekonomikách môže tento podiel dosiahnuť až **60 %**.¹⁷ Tieto údaje naznačujú, že dopad nebude rovnomerne rozdelený, ale bude silne závisieť od štruktúry jednotlivých ekonomík a podielu pracovných činností náchylných na automatizáciu. Podobné závery priniesla aj analýza spoločnosti **McKinsey & Company** z mája 2024, podľa ktorej bude do roku 2030 potrebných v Európe až **12 miliónov pracovných prechodov** vyvolaných automatizáciou a implementáciou AI. Táto predikcia zároveň poukazuje na to, že tempo zmien je približne **dvojnásobné v porovnaní s obdobím pred pandémiou COVID-19**, čo ilustruje, ako rýchlo sa transformácia trhu práce akceleruje. Na riziká spojené s technologickou zmenou upozorňuje aj **Organizácia pre hospodársku spoluprácu a rozvoj (OECD)**. Jej správa z júla 2023 uvádza, že v priemere až **27 % pracovných miest v členských krajinách je vysoko rizikových** z hľadiska automatizácie. Zvlášť zraniteľné sú pritom **východoeurópske štáty**, kde štruktúra hospodárstva obsahuje vyšší podiel rutinných a manuálnych činností.

¹⁶ Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford, CA: Stanford University Press.
<https://doi.org/10.1515/9781503609754>

¹⁷ Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A. J., Pizzinelli, C., Rockall, E. J., & Tavares, M. M. (2024). *Gen-AI: Artificial Intelligence and the Future of Work* (IMF Staff Discussion Note No. 24/001). International Monetary Fund. <https://doi.org/10.5089/9798400262548.006>

Tieto zistenia spoločne naznačujú, že automatizácia a AI nielenže zásadne menia povahu práce, ale zároveň prehlbujú regionálne a štrukturálne nerovnosti. Ich zvládnutie si bude vyžadovať aktívne politiky štátov zamerané na rekvalifikáciu, podporu mobility a spravodlivú transformáciu trhu práce.

AI ako nástroj inklúzie

Inklúzia sa v právnom diskurze spája najmä s rovnakým prístupom k právam a službám. Európsky súd pre ľudské práva¹⁸ zdôrazňuje, že právo na rovnosť nemožno chápať len negatívne (zákaz diskriminácie), ale aj pozitívne – ako povinnosť štátu vytvárať podmienky pre účinné uplatnenie práv. AI môže tieto pozitívne povinnosti posilniť, ak sa použije na odstraňovanie bariér.

Ak sme kategorizovali z nášho pohľadu najviac vypuklé riziká spojené s AI, pokúsime sa to urobiť obdobne aj pri pohľade AI ako nástroja inklúzie. Domnievame sa, že najväčšími pozitívami AI – aspoň v potenciálnej rovine je

- *zjednodušenie prístupu k informáciám* – AI už teraz umožňuje za nulové ceny preklady, prístupnosť pre nevidiacich/sluchovo postihnutých, automatizované nástroje a iné pomôcky, ktoré zásadne zlepšia postavenie osôb so zdravotným postihnutím na trhu práce;
- *personalizované vzdelávanie* – AI môže vyrovnávať šance v školstve, ak je správne nasadená;
- *participatívne projekty* – open-source modely, ktoré demokratizujú prístup k informáciám a napokon aj k pracovným možnostiam.

Umelá inteligencia môže pôsobiť ako **nástroj inklúzie**, ak sa jej potenciál využije na znižovanie bariér a podporu rovného prístupu. Najmä vo vzdelávaní môže AI podporovať **personalizované učebné prostredia**, ktoré zohľadňujú individuálne tempo a potreby študentov, čím sa otvára priestor na vyrovnávanie šancí aj pre tých, ktorí sú v tradičných systémoch znevýhodnení. Ak sú tieto riešenia správne navrhnuté, môžu zmierňovať existujúce nerovnosti a posilňovať inkluzívny charakter školstva. Ako sme uviedli, významný rozmer inklúzie prinášajú **participatívne projekty** založené na princípe open-source, ktoré umožňujú širšej verejnosti prístup k modelom a technológiám AI.

Európske akčné plány reflektujú tieto výzvy a zdôrazňujú potrebu inkluzívneho prístupu. „**Coordinated Plan on AI 2021**“ identifikuje tri kľúčové oblasti: pripraviť spoločnosť ako celok prostredníctvom rozvoja digitálnych zručností, pomôcť pracovníkom v profesiách ohrozených automatizáciou a vyškoliť viac odborníkov na

¹⁸ Rozsudok Európskeho súdu pre ľudské práva vo veci **D.H. a ostatní proti Českej republike** (č. 57325/00, rozsudok Veľkej komory z 13. novembra 2007. European Court of Human Rights. (2007, November 13). *D.H. and Others v. Czech Republic* (Application no. 57325/00). Strasbourg: Council of Europe

AI vrátane prilákania talentov do Európy (Európska komisia, 2021). Na túto stratégiu nadväzuje aj záväzok, že rozvoj AI musí zohľadňovať **diverzitu, rodovú rovnosť a zapojenie osôb so zdravotným postihnutím**, aby sa zabránilo reprodukcii existujúcich nerovností (Európska komisia, 2020).¹⁹

Napokon, právne a politické úvahy o inklúzii môžu zahŕňať aj **kvótové systémy** alebo regulačné opatrenia, ktoré zaručia, že AI bude rozvíjaná a implementovaná spôsobom, ktorý reflektuje potreby rôznorodých skupín. V takomto nastavení sa umelá inteligencia stáva nielen technologickým nástrojom, ale aj prostriedkom **sociálnej spravodlivosti a rovnosti príležitostí**.²⁰

Záver

Myšlienky vyslovené v tomto príspevku naznačujú, že AI je technológia s rôznym účinkom – nie je apriórne nástrojom nerovnosti, ale ani garanciou inklúzie. Spoločenský dopad AI sa formuje v závislosti od jej dizajnu, transparentnosti, možnosti kontroly a predovšetkým od právnej regulácie, ktorá určuje hranice jej nasadenia. Skúmané prípady zo súdnej praxe potvrdzujú, že v neprítomnosti primeraných garancií má AI tendenciu reprodukovать historické predsudky, zosilňovať nerovnosti a zasahovať do práv na súkromie či rovnaké zaobchádzanie. Naopak, ak sa systém nastaví s ohľadom na princípy rovnosti a prístupnosti, môže pôsobiť ako silný nástroj integrácie – či už pri zlepšovaní prístupu k informáciám, personalizovanom vzdelávaní alebo demokratizácii technológií prostredníctvom open-source riešení.

Európske právo jasne smeruje k tomu, aby AI bola regulovaná v prospech inkluzívneho spoločenského rámca. Kľúčovým dokumentom je pripravovaný **AI Act**, ktorý zavádza model kategorizácie rizík a osobitné požiadavky na vysokorizikové systémy. Tento prístup má zabezpečiť, aby algoritmické rozhodnutia boli transparentné, auditovateľné a kontrolovateľné zo strany verejných orgánov aj samotných užívateľov. Regulácia tým sleduje nielen prevenciu diskriminačných účinkov, ale aj posilnenie dôvery spoločnosti vo využívanie nových technológií.

Osobitnú oblasť predstavuje **Smernica Európskeho parlamentu a Rady (EÚ) 2024/2831 o zlepšení pracovných podmienok v oblasti práce pre platformy**. Jej Kapitola III sa sústreďuje výlučne na fenomén **algoritmického riadenia** a zavádza zásadné záruky pre ochranu zamestnancov. Patrí sem informačná povinnosť zamestnávateľa, povinnosť zverejniť jasné pravidlá fungovania algoritmov, zákaz spracovávať citlivé osobné údaje (napríklad biometrické ukazovatele alebo

¹⁹ KUNDRÁT, I.: K otázke súladu § 66 Zákonníka práce s právom Európskej únie. In Právny obzor, 2025, roč. 108, č. 4, s. 357–368. <https://doi.org/10.31577/pravnyobzor.2025.4.03>.

²⁰ RUDŽIKOVÁ, Denisa: Kvóty – búranie hraníc diskriminácie? In: Právo bez hraníc. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2023. ISBN 978-80-574-0243-5, s. 123-132

emocionálny stav) a tiež požiadavka ľudského dohľadu nad rozhodovaním. Zároveň sa ustanovuje právo pracovníkov odvolať sa voči algoritmickému rozhodnutiu. Tento rámec ilustruje, že Európska únia chápe ochranu pred zneužitím algoritmov ako nevyhnutný predpoklad sociálnej inklúzie.

Z vyššie uvedeného vyplýva, že budúcnosť AI nie je determinovaná samotnou technológiou, ale hodnotovými rozhodnutiami spoločnosti. Regulácia, ktorá sa opiera o zásady rovnosti, transparentnosti a ľudskej dôstojnosti, môže premeniť AI z potenciálneho zdroja nerovností na nástroj spoločného dobra. Úlohou právnej vedy preto nie je iba spätne reflektovať tieto procesy, ale aktívne navrhovať normatívne a politické riešenia, ktoré umožnia, aby AI napĺňala princíp rovnosti, spravodlivosti a participácie. Len tak môže byť technologický pokrok pretransformovaný do inkluzívneho rámca, v ktorom inovácie slúžia celej spoločnosti, nie úzkej skupine aktérov.

Zoznam použitej literatúry

1. APPELMAN, Naomi – Ó FATHAIGH, Ronan – VAN HOBOKEN, Joris: Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands. In: *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, Vol. 12, No. 3 (2021), s. 257–273. ISSN 2190-3387.
2. ARORA, Ananya: Risk and the future of AI: Algorithmic bias, data colonialism, and increasing marginalization. In: *Technology in Society*, Vol. 74 (2023), 102302. 1879-3274.
3. CAZZANIGA, M. – JAUMOTTE, F. – LI, L. – MELINA, G. – PANTON, A. J. – PIZZINELLI, C. – ROCKALL, E. J. – TAVARES, M. M.: *Gen-AI: Artificial Intelligence and the Future of Work*. IMF Staff Discussion Note No. 24/001. Washington, D.C.: International Monetary Fund, 2024. ISBN 979-8-4002-6254-8.
4. COULDRY, Nick – MEJIAS, Ulises A.: *The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019. 336 s. ISBN 978-1-5036-0974-7.
5. DE STEFANO, Valerio: "Negotiating the algorithm": Automation, artificial intelligence, and labor protection. In: *Comparative Labor Law & Policy Journal*, Vol. 41, No. 1 (2019), s. 1–34. ISSN 1095-6654.
6. KELLY, Anthony: A tale of two algorithms: The appeal and repeal of calculated grades systems in England and Ireland in 2020. In: *British Educational Research Journal*, Vol. 47, No. 3 (2021), s. 725–741. ISSN 0141-1926. <https://doi.org/10.1002/berj.3705>
7. KUNDRÁT, Ivan: K otázke súladu § 66 Zákonníka práce s právom Európskej únie. In: *Právny obzor*, Roč. 108, č. 4 (2025), s. 357–368. ISSN 0032-6984.

8. LANGEKAMP, M. – COSTA, A. – CHEUNG, Ch.: Hiring Fairly in the Age of Algorithms. In: *SSRN Electronic Journal* (2020). <https://ssrn.com/abstract=3723046> | <http://dx.doi.org/10.2139/ssrn.3723046>
9. LeCUN, Yann – BENGIO, Yoshua – HINTON, Geoffrey: Deep learning. In: *Nature*, Vol. 521 (2015), s. 436–444. ISSN 0028-0836.
10. MCKINSEY, C.: *The future of work in Europe: Navigating disruption*. McKinsey Global Institute, May 2024. ISBN 978-1-73395-621-8.
11. RACHOVITSA, Adamantia: Lessons Learned from the Dutch SyRI Case. In: *Human Rights Law Review*, Vol. 22, No. 2 (2022), s. 1–25. ISSN 1461-7781.
12. RUDŽIKOVÁ, Denisa: Kvóty – búranie hraníc diskriminácie? In: *Právo bez hraníc*. Košice: Univerzita Pavla Jozefa Šafárika, 2023, s. 123–132. ISBN 978-80-574-0243-5.
13. RUDŽIKOVÁ, Denisa: Vplyv AI na pracovné právo. In: *Inovatívne právo a inovácie v práve*. Košice: Univerzita Pavla Jozefa Šafárika, 2024, s. 30–38. ISBN 978-80-8152-0346-3.
14. SALAMI, Aishat O.: Artificial intelligence, digital colonialism, and the implications for Africa's future development. In: *Data & Policy*, Vol. 3 (2021), e10. ISSN 2632-3249
15. TIELEMAN, Merel: Fairness in tension: A socio-technical analysis of an algorithm used to grade students. In: *Cambridge Forum on AI: Law and Governance*, Vol. 1 (2025), e19. ISSN 2754-6924.
16. UK OFQUAL: *Report on the A-level grading algorithm controversy*. London: Office of Qualifications and Examinations Regulation, 2020. ISBN 978-1-83870-016-1.
17. YEUNG, Karen: Introductory Note to Recommendation of the Council on Artificial Intelligence. In: *International Legal Materials*, Vol. 59, No. 1 (2020), s. 27–34. ISSN 0020-7829.

Kontaktné údaje

doc. JUDr. Marcel Dolobáč, PhD.

marcel.dolobac@upjs.sk

Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta

NEUTRALITA ALGORITMOV A ROVNOSŤ PRÍLEŽITOSTÍ

ALGORITHMIC NEUTRALITY AND EQUAL OPPORTUNITIES

Denisa Rudžiková¹

Abstrakt: Nariadenie AI Act (EÚ 2024/1689) je prvým komplexným právnym rámcom Európskej únie pre reguláciu umelej inteligencie. V oblasti zamestnávania zaraďuje systémy automatizovaného rozhodovania medzi vysokorizikové a stanovuje požiadavky na kvalitu dát, transparentnosť, vysvetliteľnosť a ľudský dohľad. Tento prístup vychádza z koncepcie formálnej rovnosti, ktorá poskytuje ochranu pred priamou diskrimináciou, avšak nezaručuje materiálnu rovnosť príležitostí. Empirické skúsenosti ukazujú, že algoritmy, aj keď sú nastavené ako neutrálne, môžu reprodukovать historické nerovnosti obsiahnuté v dátach alebo sprostredkované prostredníctvom proxy premenných. Cieľom príspevku je analyzovať obmedzenia princípu neutrality v pracovnoprávných vzťahoch a predstaviť koncept inkluzívneho dizajnu (inclusion-by-design) ako možný prístup k eliminácii štrukturálnych nerovností. Inclusion-by-design predstavuje metodiku, ktorá systematicky integruje rozmanitosť a férovosť do procesu vývoja algoritmických systémov. V príspevku sa skúma, do akej miery môže tento prístup prispieť k vytvoreniu podmienok, v ktorých formálne rovnaké pravidlá vedú k porovnateľným výsledkom, a akým spôsobom môže právny a inštitucionálny rámec usmerniť digitalizáciu trhu práce s ohľadom na zásadu rovnosti príležitostí.

Kľúčové slová: AI Act, algoritmus, rovnosť príležitostí, pracovné právo

Abstract: The AI Act (EU 2024/1689) constitutes the first comprehensive legal framework of the European Union governing artificial intelligence. In the field of employment, it classifies automated decision-making systems as high-risk and introduces requirements relating to data quality, transparency, explainability, and human oversight. This approach builds on the concept of formal equality, which protects against direct discrimination but does not ensure substantive equality of opportunity. Empirical evidence demonstrates that algorithms, even when formally neutral, may reproduce historical inequalities embedded in data or indirectly transmitted through proxy variables. The paper aims to examine the limitations of the neutrality principle

¹ Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Katedra pracovného práva a práva sociálneho zabezpečenia

in employment relations and to introduce the concept of inclusion-by-design as a potential means of addressing structural inequalities. Inclusion-by-design denotes a methodology that systematically incorporates diversity and fairness into the design and development of algorithmic systems. The analysis focuses on the extent to which this approach can create conditions under which formally equal rules yield comparable outcomes, and on the role of legal and institutional frameworks in guiding the digitalization of the labor market in line with the principle of equality of opportunity.

Key words: AI Act, algorithm, equality of opportunity, labour law

Úvod

Uplatňovanie umelej inteligencie v pracovnoprávných vzťahoch sa stáva jedným z najvýraznejších trendov digitalizácie trhu práce.² Algoritmy sľubujú rýchlejšie a efektívnejšie rozhodovanie pri nábere, výbere či hodnotení zamestnancov, no zároveň prinášajú zásadné otázky spojené so zachovaním princípu rovnakého zaobchádzania. Skúsenosti ukazujú, že aj pri formálnom vylúčení chránených znakov môžu algoritmy generovať nepriamu diskrimináciu prostredníctvom tzv. proxy premenných, keďže pracujú s historickými dátami odrážajúcimi existujúce nerovnosti.³ Na tieto riziká reaguje nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 o umelej inteligencii (AI Act), účinné od augusta 2024. Zaradením HR technológií medzi vysokorizikové systémy zavádza osobitné povinnosti pre ich poskytovateľov a používateľov - dôraz na kvalitu a reprezentatívnosť dát, testovanie, transparentnosť či ľudský dohľad. Základom regulácie je koncept neutrality algoritmov, ktorý vychádza z tradície formálnej rovnosti v antidiskriminačnom práve.⁴ Neutralita však sama osebe nemusí viesť k reálnej rovnosti príležitostí, pretože štrukturálne nerovnosti môžu pretrvávať aj v „neutrálnych“ systémoch. Predkladaný príspevok preto analyzuje limity princípu neutrality a hľadá možnosti, ako princíp rovnakého zaobchádzania uchopiť v digitálnom prostredí prostredníctvom inkluzívneho dizajnu algoritmov.

² DOLOBÁČ, M., E. LACKOVÁ. Futurology of labour law. 1. vyd. Praha: Leges, 2022. 58, 60 - 61 s.

³ SHEARD, N. Algorithm-facilitated discrimination: a socio-legal study of the use by employers of artificial intelligence hiring systems. *Journal of Law and Society*. 2025; 52: s. 282 -283.

STRAND, V. B. Algorithms, artificial intelligence and discrimination: An analysis of the Norwegian Equality and Anti-Discrimination Act's possibilities and limitations. 1. vyd. Oslo: The Equality and Anti-Discrimination Ombud, 2025, s. 26 – 27.

⁴ K zásade rovnakého zaobchádzania v EÚ pozri, napr.: KUNDRÁT, I.: K otázke súladu § 66 Zákonníka práce s právom Európskej únie. In: *Právny obzor*, 2025, roč. 108, č. 4, s. 357–368.

Algoritmická diskriminácia

Algoritmické systémy sa v pracovnej oblasti často prezentujú ako nástroje, ktoré prinesú väčšiu efektivitu a objektivitu rozhodovania. Od ich nasadenia si zamestnávateľia sľubujú schopnosť spracovať rozsiahle množstvo prihlášok, rýchlejšie identifikovať najvhodnejších kandidátov a minimalizovať ľudské predsudky.⁵ Tento technologický príslub však naráža na zásadnú výzvu: aj keď algoritmy pôsobia neutrálne, ich výstupy môžu viesť k systematickému znevýhodňovaniu určitých skupín. S týmto problémom sa spája termín algoritmická diskriminácia, ktorý označuje situáciu, keď rozhodnutia generované systémami umelej inteligencie spôsobujú nerovné zaobchádzanie, hoci model formálne nepracuje s chránenými znakmi, ako je pohlavie, vek či etnicita.⁶ Mechanizmus diskriminácie je väčšinou nepriamy a prebieha prostredníctvom tzv. proxy premenných - atribútov, ktoré na prvý pohľad pôsobia neutrálne, ale v skutočnosti úzko súvisia s chránenými kategóriami.⁷ Typ školy, lokalita bydliska, jazykové špecifiká v životopise či dĺžka kariérnych prestávok sa môžu v modeloch objaviť ako prediktory úspechu, čím sa nepriamo reprodukujú štrukturálne nerovnosti zakorenené v spoločnosti.⁸ Klasickým príkladom je náborový nástroj spoločnosti Amazon, ktorý bol trénovaný na historických životopisoch úspešných kandidátov - prevažne mužov v technologických profesiách. Algoritmus sa naučil penalizovať ženské životopisy, nie priamo podľa pohlavia, ale prostredníctvom jazykových indícií, ako boli zmienky o ženských školách alebo aktivitách. Výsledok pôsobil navonok neutrálne, no v praxi systematicky znevýhodňoval ženy a bránil im v prístupe k pracovným príležitostiam.⁹ Ešte aktuálnejší rozmer problematiky ilustruje prebiehajúci spor Mobley vs. Workday pred federálnym súdom v Kalifornii, ktorý patrí medzi prvé veľké prípady namierené priamo proti poskytovateľovi HR technológií. Žalobca Derek Mobley, afroamerický muž starší ako štyridsať rokov so zdravotným znevýhodnením, tvrdí, že bol prostredníctvom softvéru Workday opakovane vyradený z viac než stovky výberových konaní, hoci splňal požiadavky na

⁵ BIGMAN, Y. E.: *Algorithmic Discrimination Causes Less Moral Outrage than Human Discrimination* [online]. Journal of Experimental Psychology: General, 2023, roč. 152, č. 1, s. 15.

⁶ WANG, X., WU, Y. C., JI, X., FU, H. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. In *Frontiers in Artificial Intelligence*. 7, 2024.

⁷ KAHN, L. a kol.: *AI Safety and Automation Bias* [online]. Center for Security and Emerging Technology, 2024.

⁸ TRAVERS, M. *Legal Issues in the Use of Artificial Intelligence in Recruitment* [online]. 2024, roč. 5, č. 1, s. 285.

⁹ The guardian. *Amazon ditched AI recruiting tool that favored men for technical jobs* [online] Dostupné na: <https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>

dané pozície. Podľa žaloby nešlo o úmyselné rozhodnutie konkrétneho zamestnávateľa, ale o vedľajší účinok algoritmického systému, ktorý systematicky znevýhodňoval uchádzačov určitého veku, etnického pôvodu či zdravotného stavu. Kľúčová otázka prípadu spočíva v tom, či možno za takéto diskriminačné účinky niesť zodpovednosť aj poskytovateľa HR technológie, a nielen samotných zamestnávateľov. Súd v roku 2024 odmietol návrh Workday na zamietnutie žaloby a umožnil, aby sa vec posudzovala ďalej. V roku 2025 navyše rozhodol, že žaloba sa môže rozšíriť na väčší okruh dotknutých osôb, čím sa otvorila cesta k potenciálne kolektívnej žalobe obrovského rozsahu. Rozsah prípadu je bezprecedentný. Podľa údajov Workday bolo v danom období prostredníctvom jeho softvéru odmietnutých viac než miliarda žiadostí o zamestnanie, čo naznačuje, že počet potenciálne dotknutých uchádzačov je enormný. Ak by sa preukázalo, že algoritmus mal systematický diskriminačný účinok, išlo by o významný precedens, ktorý by nielen ovplyvnil budúcnosť súdnych sporov v tejto oblasti, ale mohol by zásadne zmeniť aj chápanie zodpovednosti poskytovateľov AI nástrojov na trhu práce.¹⁰ Tieto prípady poukazujú na širší problém. Algoritmická diskriminácia nevzniká ako technická „chyba“ alebo izolované zlyhanie systému - anomália či glitch. Je dôsledkom samotnej logiky algoritmického učenia, ktoré vychádza z historických dát. Tie nikdy nie sú úplne neutrálne, pretože odrážajú minulé štrukturálne nerovnosti, ktoré sú v našej spoločnosti všade prítomné. Výsledkom sú diskriminačné efekty, ktoré sú často neviditeľné, ťažko preukázateľné a o to nebezpečnejšie, že pôsobia plošne a konzistentne na veľké množstvo uchádzačov súčasne.

AI Act a neutralita algoritmov

AI Act, ktorý nadobudol účinnosť v auguste 2024, predstavuje prvý komplexný právny rámec regulujúci vývoj a používanie umelej inteligencie v Európskej únii. Ide o legislatívny míľnik, ktorého význam sa obzvlášť prejavuje v oblasti pracovného práva. Systémy využívané pri nábere, výbere, hodnotení či riadení zamestnancov sú totiž výslovne zaradené medzi tzv. vysokorizikové oblasti. Tým európsky normotvorca jednoznačne priznal, že algoritmické rozhodovanie v oblasti prístupu k práci zasahuje do jadra základných práv a slobôd a vyžaduje osobitnú reguláciu. Regulácia zavádza celý rad povinností, ktoré majú slúžiť ako ochranné mechanizmy proti diskriminačným účinkom. Poskytovatelia a používatelia vysokorizikových systémov sú povinní zabezpečiť, aby boli tieto systémy trénované na kvalitných, reprezentatívnych a aktuálnych dátach, ktoré minimalizujú riziko systematických skreslení. Musia vykonávať pravidelné testovanie a validáciu s cieľom identifikovať neželané efekty, zaviesť procesy monitorovania počas celej životnosti systému, ako

¹⁰ WARNER, C.: *AI Hiring Discrimination: Lessons from Workday Lawsuit* [online]. HRMorning, 2025. Dostupné z: <https://www.hrmorning.com/news/ai-hiring-discrimination-workday/>

aj povinnosti spojené s transparentnosťou a vysvetliteľnosťou algoritmických rozhodnutí. Neoddeliteľnou súčasťou je tiež zabezpečenie účinného ľudského dohľadu, ktorý má umožniť včas odhaliť a napraviť prípadné zlyhania.¹¹ Spoločným menovateľom týchto opatrení je snaha priblížiť fungovanie algoritmov k ideálu neutrality. Neutralita je v AI Acte chápaná ako absencia priameho rozlišovania podľa zakázaných kritérií, akými sú pohlavie, vek, etnický pôvod či zdravotný stav, a ako uplatňovanie rovnakých pravidiel pre všetkých účastníkov výberového konania. Tento prístup nadväzuje na dlhodobo prítomný princíp formálnej rovnosti, ktorý je základným pilierom práva. Podľa tejto logiky je rovnosť zabezpečená vtedy, ak sa všetkým jednotlivcom poskytnú rovnaké podmienky a ak sa zakázané kritériá explicitne vylúčia z rozhodovania. Takto koncipovaná neutralita pôsobí konzistentne v niekoľkých rovinách. Politicky sa prezentuje ako vyvážené a „apolitické“ riešenie: nejde o preferovanie konkrétnych výsledkov, ale o garanciu rovnakého procesu pre všetkých. Právne sa opiera o tradíciu zákazu diskriminácie, ktorá je v európskom právnom poriadku zakotvená už desaťročia a tvorí jeho stabilnú súčasť. A technicky sa javí ako cieľ, ktorý je možné sledovať prostredníctvom odstraňovania rizikových premenných, nastavovania auditov a zavádzania kontrolných mechanizmov. Neutralita je preto v rámci AI Actu formulovaná ako regulatívny ideál, ku ktorému majú vysokorizikové systémy smerovať. Pri bližšom pohľade sa však ukazuje, že tento koncept naráža na významné limity. Opatrenia stanovené AI Actom majú prevažne reaktívny charakter. Testovanie, validácia a audity sú nastavené tak, aby odhaľovali diskriminačné účinky až v momente, keď sa prejavia v praxi. Transparentnosť a vysvetliteľnosť poskytujú rámec na rekonštrukciu rozhodnutí, no nevedú k tomu, aby bol systém od počiatku koncipovaný inkluzívne. Ľudský dohľad, ktorý má slúžiť ako poistka, sa v praxi často stáva formálnou povinnosťou s obmedzenou účinnosťou - najmä tam, kde ide o spracovanie tisícov životopisov alebo rozsiahle rozhodovacie procesy. Problém neutrality v algoritmických systémoch je hlbší, než by sa mohlo zdať na prvý pohľad. Neutralita je síce atraktívnym ideálom, no jej naplnenie je v praxi mimoriadne náročné. Tréningové dáta, na ktorých algoritmy fungujú, nikdy nie sú hodnotovo prázdne. Sú odrazom spoločenského vývoja a nesú v sebe stopy minulých nerovností, predsudkov a štrukturálnych znevýhodnení. Tieto vzorce nemožno jednoducho eliminovať tým, že sa z databáz odstránia chránené znaky ako pohlavie či vek. Diskriminačné účinky sa totiž často prenášajú nepriamo prostredníctvom zástupných indikátorov, napríklad miesta bydliska, typu absolvovanej školy alebo dĺžky kariérnych prestávok. Výsledkom je, že aj pri formálne neutrálnom nastavení môže algoritmus reprodukovat historické

¹¹ Najmä čl. 8 – 17 AI Actu

nerovnosti obsiahnuté v dátach.¹² Neutralita tak v prostredí umelej inteligencie nepredstavuje záruku spravodlivosti, ale skôr normatívny ideál, ku ktorému sa možno približovať, no ktorý nemožno nikdy úplne dosiahnuť. Zabezpečuje rámec formálnej rovnosti, teda rovnakých pravidiel pre všetkých, ale nedokáže zachytiť hlbšie štrukturálne nerovnosti prítomné v spoločnosti aj v dátach. Práve tu sa odhaľuje napätie medzi právnym chápaním rovnakého zaobchádzania a praktickou realitou algoritmických systémov: formálna rovnosť síce chráni pred otvorenou diskrimináciou, no sama osebe nestačí na zabránenie jemnejších a menej viditeľných foriem znevýhodňovania. AI Act preto predstavuje nepochybne významný krok, ktorý posilňuje minimálne štandardy férovosti a vytvára rámec ochrany pred najvýraznejšími prejavmi diskriminácie. Zároveň však ukazuje hranice prístupu založeného výlučne na neutralite. Ak má byť algoritmické rozhodovanie v pracovnom práve skutočne spravodlivé, bude potrebné posunúť diskusiu ďalej – smerom k prístupom, ktoré už v samotnom dizajne systémov počítajú s rozmanitosťou a snažia sa aktívne predchádzať diskriminačným efektom.

Inkluzívny dizajn ako digitálne pozitívne opatrenie

Pracovné právo dlhodobo vychádza z poznania, že rovnaké pravidlá nemusia viesť k rovnakým výsledkom. Ak určité skupiny zamestnancov alebo uchádzačov štartujú z nerovnakých pozícií, formálna rovnosť často len udržiava existujúce rozdiely. Aj preto sa postupne rozvinul koncept materiálnej rovnosti, ktorý smeruje k reálnemu vyrovnávaniu šancí.¹³ Nejde teda iba o zákaz diskriminácie, ale o aktívnu snahu vytvárať také prostredie, v ktorom budú mať jednotlivci skutočne porovnateľné príležitosti.¹⁴ Analógia s digitálnym prostredím je zrejmá. Neutralita algoritmov, na ktorej stojí AI Act, korešponduje s princípom formálnej rovnosti: algoritmus má síce ignorovať zakázané kritériá a hodnotiť všetkých podľa rovnakých pravidiel, v praxi však nedokáže prekonať existujúce rozdiely. Namiesto odstraňovania štrukturálnych nerovností tak často vytvára len zdanlivý obraz rovnosti, ktorý zakrýva pretrvávajúce disproporcie. V reakcii na tieto obmedzenia sa čoraz viac do popredia dostáva koncept inkluzívneho dizajnu (*inclusion-by-design*), ktorý možno považovať za

¹² BARREDO ARRIETA, A. a kol. *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges* [online]. Information Fusion, 2020, roč. 58, s. 94.

¹³ DOLOBÁČ, M. Kvóta systém v pracovnom práve. In: Jurčová, M., Olšovská, A., Štefanko, J. (eds.). *Diskriminácia v zmluvnom práve*. Bratislava: TYPI UNIVERSITATIS TYRNAVIENSIS, 2015. s. 249. [online].

¹⁴ KURIL, M. *Niekoľko filozofickoprávnych úvah k teoretickoprávnym základom antidiskriminačnej legislatívy* [online]. Bratislava: Akadémia Policajného zboru, 2022. Dostupné na: <https://www.akademiapz.sk/sites/default/files/2022-08/002%20%20KURIL%20%20Niekoľko%20filozofickopravných%20uváh%20k%20teoretickopravným%20základ.pdf>

digitálny ekvivalent pozitívnych opatrení. Jeho základnou ideou nie je dodatočná korekcia diskriminačných účinkov, ale preventívne zakotvenie inklúzie už do samotnej architektúry systému. Inclusion-by-design preto nepredstavuje len stratégiu minimalizácie rizík, ale aktívny prístup k vytváraniu prostredia, v ktorom sa rozmanitosť používateľov chápe ako kľúčový zdroj férovejších a reprezentatívnejších výsledkov. Z tohto hľadiska ide o zásadný posun od neutrality k skutočnej inklúzii. Kým AI Act stavia predovšetkým na mechanizmoch dohľadu, auditov a zákaze využívania chránených znakov, inclusion-by-design zdôrazňuje, že materiálnu rovnosť príležitostí možno dosiahnuť len vtedy, ak algoritmy už vo fáze návrhu zohľadňujú rôznorodosť a sú cielene koncipované tak, aby aktívne eliminovali štrukturálne nerovnosti.¹⁵

Inkluzívny dizajn v praxi

Ak chceme tento koncept uchopiť praktickejšie, je potrebné ukázať, čo inclusion-by-design znamená v samotnej praxi. Nejde o jediný nástroj, ale o súbor opatrení, ktoré prenikajú do viacerých rovín vývoja a používania algoritmov. Práve vďaka nim sa ukazuje, že inklúzia nie je abstraktnou ideou, ale môže byť konkrétnym princípom premietnutým do pravidiel, metodiky vývoja, technických riešení a napokon aj do kultúry organizácií, ktoré tieto systémy tvoria a využívajú. Metodika vývoja predstavuje základ inclusion-by-design, pretože zahŕňa celý životný cyklus systému od výberu dát až po hodnotenie jeho účinkov. Vývojári majú zabezpečiť, aby tréningové dáta reprezentovali rozmanitosť populácie vrátane menších a zraniteľných skupín, ktoré bývajú v tradičných datasetoch zanedbávané. Do samotného vývoja by sa mali zapájať nielen technickí odborníci, ale aj zástupcovia dotknutých komunít či experti na rovnosť príležitostí. Úlohou zamestnávateľov je následne overovať, či používaný algoritmus funguje spravodlivo aj voči špecifickým skupinám, napríklad ženám po rodičovskej dovolenke alebo starším uchádzačom. Významná je aj technologická dimenzia, ktorá sa sústreďuje na samotný dizajn systému. Vývojári musia implementovať metódy na zmierňovanie biasu, zavádzať priebežný monitoring výsledkov podľa rôznych demografických skupín a zabezpečiť vysvetliteľnosť modelu. V praxi to môže znamenať, že kreditný scoringový nástroj sa pravidelne testuje, či nedochádza k systematickému odmietaniu uchádzačov z určitej etnickej menšiny, pričom odhalené disproporcie si vyžadujú okamžité korekčné mechanizmy. Pre zamestnávateľov je rozhodujúce, aby mali prístup k týmto vysvetleniam a dokázali preukázať, že ich rozhodnutia nevychádzajú z diskriminačných vzorcov. Rozhodujúci význam má však kultúrny rámec, ktorý určuje,

¹⁵ SULASTRI, R., JANSSEN, M., VAN DE POEL, I., DING, A. Transforming towards inclusion-by-design: Information system design principles shaping data-driven financial inclusiveness. In *Government Information Quarterly*. 41, 4, 2024, s. 4 – 5.

či inclusion-by-design zostane iba formálnou požiadavkou, alebo sa pretaví do každodennej praxe. Bez organizačnej otvorenosti k diverzite a férovosti aj najlepšie technické či procesné opatrenia strácajú účinok. Pre vývojárov to znamená stavať na princípe rôznorodých tímov, kde sa spájajú odlišné perspektívy a skúsenosti. Takéto kolektívy dokážu včas identifikovať prekážky, ktoré by homogénne zloženie prehliadlo, napríklad problémy s prístupnosťou pre osoby so zdravotným znevýhodnením alebo nedostatok jazykovej prispôsobivosti pre migrantov. U zamestnávateľov sa kultúra premieňa do ochoty chápať digitálne nástroje nie ako neutrálne technológie, ale ako nástroje, ktoré je potrebné aktívne riadiť s dôrazom na rovnosť príležitostí a férový prístup k uchádzačom. Silnou stránkou inclusion-by-design je najmä jeho preventívny charakter. Nejde iba o odstraňovanie diskriminačných dôsledkov, keď sa už prejavia, ale o systematické vytváranie podmienok, ktoré reálne podporujú rovnosť príležitostí. Tento prístup môže zvýšiť dôveryhodnosť algoritmických systémov, posilniť legitimitu rozhodovacích procesov a prispieť k väčšej diverzite na pracovisku. Súčasne však nesie aj svoje úskalia - jeho implementácia je náročnejšia na zdroje, vyžaduje participáciu viacerých aktérov a priebežné monitorovanie. To zvyšuje náklady a kladie vyššie nároky na organizácie. Navyše, hranica medzi inkluzívnym prístupom a zásadou zákazu diskriminácie nemusí byť vždy jednoznačná a môže vyvolávať právne či etické dilemy. Rozdiel oproti neutralite je však zásadný. Neutralita predstavuje snahu zabezpečiť rovnaké procesy a chrániť pred diskrimináciou, inclusion-by-design však ide ďalej. Jeho cieľom je dosiahnuť reálnu rovnosť šancí tým, že férovosť a diverzita sú zabudované už do samotného návrhu systému. Z pohľadu pracovného práva možno tento prístup vnímať ako digitálny ekvivalent pozitívnych opatrení: nejde o vytváranie privilégií, ale o nastavenie takých podmienok, aby formálne rovnaké pravidlá viedli aj k materiálne spravodlivým výsledkom. Práve v tom možno vidieť cestu, ako predchádzať algoritmickej diskriminácii - nie až prostredníctvom dodatočných kontrol a auditov, ale už pri jej zdroji, v samotnom dizajne technológií.

Záver

AI Act je významným krokom, pretože stanovuje minimálne štandardy férovosti založené na neutralite algoritmov. Neutralita však zostáva regulatívnym ideálom, ktorý je v praxi ťažko dosiahnuteľný a ani pri jeho dodržaní nemožno garantovať skutočnú rovnosť príležitostí. Algoritmy vychádzajú z historických dát, ktoré nikdy nie sú úplne neutrálne, a preto sa diskriminačné účinky objavujú aj tam, kde sú formálne pravidlá nastavené rovnako. Preto je potrebné posunúť diskusiu ďalej k inkluzívnemu dizajnu. Ten možno chápať ako digitálny ekvivalent pozitívnych opatrení. Jeho cieľom nie je vytvárať privilégiá, ale systematicky odstraňovať bariéry a aktívne počítať s rozmanitosťou. Skutočnú diskrimináciu v algoritmoch

neodstránime neutralitou, ale až inkluzívnym dizajnom, ktorý dokáže nerovnosti eliminovať ešte predtým, než prerastú do nespravodlivých výsledkov. Výzvou pre pracovné právo a trh práce preto nie je len dohliadať na to, aby algoritmy neboli otvorene diskriminačné. Skutočným testom bude, či dokážeme vytvoriť právny a inštitucionálny rámec, ktorý nebude digitalizáciu len regulovať, ale ktorý ju usmerní tak, aby sa stala nástrojom aktívneho budovania rovnosti príležitostí. Práve v tom spočíva nielen výzva, ale aj príležitosť, ktorú digitalizácia prináša pre budúcnosť rovnakého zaobchádzania na trhu práce.

Zoznam použitej literatúry

1. BARREDO ARRIETA, A. a kol. *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges* [online]. Information Fusion, 2020, roč. 58, s. 90 - 97. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1566253519308103>
2. BIGMAN, Y. E.: *Algorithmic Discrimination Causes Less Moral Outrage than Human Discrimination* [online]. Journal of Experimental Psychology: General, 2023, roč. 152, č. 1, s. 4–27. Dostupné z: <https://pubmed.ncbi.nlm.nih.gov/35758989/>
3. DOLOBÁČ, M. Kvóta systém v pracovnom práve. In: Jurčová, M., Olšovská, A., Štefanko, J. (eds.). *Diskriminácia v zmluvnom práve*. Bratislava: TYPI UNIVERSITATIS TYRNAVIENSIS, 2015. 249 s. [online]. ISBN 978-80-8082-835-6. Dostupné na: <https://www.truni.sk/sites/default/files/uk/f000147.pdf>
4. DOLOBÁČ, M., E. LACKOVÁ. *Futurology of labour law*. 1. vyd. Praha: Leges, 2022. 180 s. ISBN 978-80-7502-662-0.
5. KAHN, L. a kol.: *AI Safety and Automation Bias* [online]. Center for Security and Emerging Technology, 2024. Dostupné z: <https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Safety-and-Automation-Bias.pdf>
6. KELLY-LYTH, A. Algorithmic discrimination at work. In *European Labour Law Journal*. 2023, 14, 2, s. 152–171. Dostupné na: <https://www.webofscience.com/wos/woscc/full-record/WOS:001006990700003>
7. KUNDRÁT, I.: K otázke súladu § 66 Zákonníka práce s právom Európskej únie. In *Právny obzor*, 2025, roč. 108, č. 4, s. 357–368. <https://doi.org/10.31577/pravnyobzor.2025.4.03>
8. KURIL, M. *Niekoľko filozofickoprávnych úvah k teoretickoprávnym základom antidiskriminačnej legislatívy* [online]. Bratislava: Akadémia Policajného zboru, 2022. Dostupné na: <https://www.akademiapz.sk/sites/default/files/2022-08/002%20%20KURIL%20%20Niekoľko%20filozofickopravných%20uváh%20k%20teoretickopravným%20zaklad.pdf>

9. SHEARD, N. Algorithm-facilitated discrimination: a socio-legal study of the use by employers of artificial intelligence hiring systems. *Journal of Law and Society*. 2025; 52: 269–291. <https://doi.org/10.1111/jols.12535>
10. STRAND, V. B. Algorithms, artificial intelligence and discrimination: An analysis of the Norwegian Equality and Anti-Discrimination Act's possibilities and limitations. 1. vyd. Oslo: The Equality and Anti-Discrimination Ombud, 2025. Dostupné na: <https://ldo.no/content/uploads/2025/05/Algorithms-artificial-intelligence-and-discrimination-report.pdf>
11. SULASTRI, R., JANSSEN, M., VAN DE POEL, I., DING, A. Transforming towards inclusion-by-design: Information system design principles shaping data-driven financial inclusiveness. In *Government Information Quarterly*. 41, 4, 2024. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S0740624X24000716>
12. TRAVERS, M. *Legal Issues in the Use of Artificial Intelligence in Recruitment* [online]. 2024, roč. 5, č. 1, s. 282–294. DOI: 10.3390/ai5010019. Dostupné z: <https://www.mdpi.com/2673-2688/5/1/19>
13. WANG, X., WU, Y. C., JI, X., FU, H. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. In *Frontiers in Artificial Intelligence*. 7 (2024). Dostupné na: <https://www.webofscience.com/wos/woscc/full-record/WOS:001237515300001>

Kontaktné údaje

Mgr. Denisa Rudžiková, PhD.

denisa.rudzikova@upjs.sk

Katedra pracovného práva a práva sociálneho zabezpečenia

Právnická fakulta, Univerzita Pavla Jozefa Šafárika v Košiciach

ALGORITMICKÁ DISKRIMINÁCIA A ROVNAKÉ ZAOBCHÁDZANIE NA DIGITÁLNOH TRHU PRÁCE: VÝZVY A PRÍLEŽITOSTI PRE ŽENY V ZRANITEĽNÝCH SITUÁCIÁCH¹

ALGORITHMIC DISCRIMINATION AND EQUAL TREATMENT IN THE DIGITAL LABOUR MARKET: CHALLENGES AND OPPORTUNITIES FOR WOMEN IN VULNERABLE SITUATIONS

Barbara Faktor Pavlíková²

Abstrakt: Digitalizácia trhu práce prináša nové príležitosti, ale aj riziká v oblasti rovnakého zaobchádzania. Automatizované náborové systémy a algoritmy umelej inteligencie sú čoraz častejšie využívané pri výbere uchádzačov o zamestnanie. Nevznikajú však vo vákuu – učia sa na historických dátach, ktoré odrážajú predsudky a nerovnosti v spoločnosti. Výsledkom môže byť algoritmická diskriminácia, pri ktorej sú ženy a najmä ženy v zraniteľných situáciách (po kariérnej prestávke, počas materstva či inej prechodnej fázy) systematicky znevýhodňované.

Príspevok sa zameria na právne a spoločenské aspekty tohto javu. Na príkladoch z praxe poukáže na konkrétne riziká spojené s algoritmizáciou náboru a následne predstaví európsky právny rámec – od zásad antidiskriminačného práva po nové pravidlá vyplývajúce z Nariadenia o umelej inteligencii (AI Act). Diskutované budú aj špecifiká slovenského trhu práce a bariéry, ktorým čelia ženy v zraniteľných situáciách.

Cieľom príspevku je ukázať, že digitalizácia sama osebe nie je hrozbou. Bez jasných pravidiel však môže reprodukovat' či prehĺbovat' nerovnosti. Ak je nastavená správne, môže priniesť flexibilnejšie zamestnanie, lepší prístup k vzdelávaniu a spravodlivejší trh práce.

Kľúčové slová: algoritmická diskriminácia; digitálny trh práce; ženy v zraniteľných situáciách; umelá inteligencia; antidiskriminačné právo;

¹ Príspevok bol spracovaný pod záštitou projektu VEGA č. 1/0677/24 s názvom „Ženy v kríze“.

² Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta Univerzity Komenského v Bratislave

Abstract: The digitalization of the labour market brings new opportunities but also risks in the field of equal treatment. Automated recruitment systems and artificial intelligence algorithms are increasingly used in hiring processes. However, they do not emerge in a vacuum – they are trained on historical data that often reflect existing social biases and inequalities. As a result, algorithmic discrimination may occur, where women, particularly those in vulnerable situations (after a career break, during motherhood, or in other transitional phases), are systematically disadvantaged.

The paper focuses on the legal and societal aspects of this phenomenon. Drawing on practical examples, it highlights specific risks linked to algorithmic recruitment and then turns to the European legal framework – from the principles of anti-discrimination law to the Artificial Intelligence Act (AI Act). The paper also discusses the particularities of the Slovak labour market and the barriers faced by women in vulnerable situations.

The aim is to demonstrate that digitalization is not inherently a threat. Without clear rules, however, it can reproduce or deepen inequalities. Properly regulated, it can instead create opportunities for more flexible employment, better access to education, and a fairer labour market.

Key words: algorithmic discrimination; digital labor market; women in vulnerable situations; artificial intelligence; anti-discrimination law;

Úvod

Digitalizácia a nástup umelej inteligencie zásadne menia charakter trhu práce. Využívanie algoritmov pri náboe a výbere zamestnancov je čoraz častejším javom – od automatizovaného triedenia životopisov až po hodnotenie uchádzačov na základe videoanalýzy či psychometrických testov. Tieto procesy sľubujú efektívnosť a úsporu nákladov, no zároveň vyvolávajú vážne otázky týkajúce sa rovnakého zaobchádzania a rizika diskriminácie. Algoritmy nevznikajú v sociálnom vákuu – učia sa na historických dátach, ktoré často obsahujú predsudky a štrukturálne nerovnosti prítomné v spoločnosti. Ak nie sú podrobené kontrole, hrozí, že ich budú reprodukovat' a dokonca prehlbovat'.³

Diskriminácia na trhu práce je dlhodobým problémom, ktorý právna úprava na úrovni Európskej únie i jednotlivých členských štátov rieši už celé desaťročia. Zavedenie smernice 2000/78/ES položilo základný rámec pre zákaz diskriminácie v zamestnaní a povolaniach, pričom sa opiera o princíp rovnakého zaobchádzania bez ohľadu na pohlavie, vek, zdravotné postihnutie, náboženstvo či sexuálnu orientáciu.⁴

³ Barocas – Selbst, *Big Data's Disparate Impact*, 2016, s. 672–674; 688–689.

⁴ Smernica 2000/78/ES, čl. 1–2.

Digitalizácia však prináša nové formy diskriminačných praktík, ktoré tradičné právne koncepty len ťažko postihujú. Ide najmä o tzv. algoritmicú diskrimináciu, pri ktorej zdanlivo neutrálne technické systémy vedú k systematickému znevýhodňovaniu určitých skupín.⁵ V kontexte trhu práce sú osobitne ohrozené ženy, a to predovšetkým tie, ktoré sa nachádzajú v zraniteľných situáciách – po návrate z rodičovskej dovolenky, počas materstva, v období prechodu na nový typ zamestnania alebo pri práci na atypických pracovných zmluvách.⁶

Právna veda stojí pred úlohou nielen identifikovať nové riziká, ale aj poskytnúť normatívne riešenia. Európska únia už reaguje legislatívnymi iniciatívami – nariadenie o umelej inteligencii (AI Act) má ambíciu zaviesť pravidlá pre vysokorizikové systémy vrátane algoritmov používaných pri nábore a výbere pracovníkov.⁷ Otázkou zostáva, či tieto pravidlá budú postačovať na elimináciu diskriminačných praktík alebo či je potrebné doplniť ich o ciele opatrenia v oblasti rodovej rovnosti a ochrany zraniteľných skupín.

Cieľom príspevku je analyzovať problematiku algoritmickej diskriminácie na digitálnom trhu práce s dôrazom na ženy v zraniteľných situáciách. V úvode predstavíme teoretické a právne východiská, následne sa zameriame na európsky a slovenský právny rámec a poukážeme na praktické príklady diskriminačných javov pri používaní algoritmov. V závere budú diskutované možnosti, ako nastaviť digitalizáciu tak, aby nebola hrozbou, ale nástrojom posilňujúcim rovnosť príležitostí a spravodlivý prístup k zamestnaniu.

Teoreticko-právne východiská algoritmickej diskriminácie

Diskriminácia ako právny a spoločenský jav má viacero podôb. Klasicky rozlišujeme priame a nepriame formy diskriminácie. Priama diskriminácia nastáva vtedy, ak sa s osobou zaobchádza menej priaznivo výlučne z dôvodu jej chráneného znaku, napríklad pohlavia či veku. Nepriama diskriminácia je skrytejšia: ide o zdanlivo neutrálne opatrenie alebo postup, ktorý v praxi vedie k nevýhodnému postaveniu určitej skupiny.⁸ V pracovnom práve je tento koncept kľúčový, pretože práve „neutrálne“ algoritmy sa často javia ako objektívne, avšak svojím nastavením generujú systematické nerovnosti.

Algotimická diskriminácia predstavuje špecifický typ nepriamej diskriminácie. K jej vzniku prispievajú tri základné faktory:

⁵ Tobler, Limits and Potential of the Concept of Indirect Discrimination, 2008, s. 6; 24; 40–41.

⁶ EIGE, Artificial intelligence, platform work and gender equality, 2021, s. 11–15; 23; 81–85; 89.

⁷ AI Act (Nariadenie (EÚ) 2024/1689), čl. 6 ods. 2–3; príloha III, bod 4.

⁸ Smernica 2000/78/ES, čl. 2 ods. 2(b).

- dáta – algoritmy sú trénované na historických údajoch, ktoré odrážajú predsudky a stereotypy existujúce v spoločnosti.⁹
- dizajn algoritmu – vývojári pri tvorbe modelu prijímajú rozhodnutia o tom, ktoré premenné zahrnú alebo ako ich vážia, čím môžu nevedome zvýhodniť či znevýhodniť určitú skupinu.¹⁰
- spôsob použitia – aj algoritmus s neutrálnym nastavením môže viesť k diskriminácii, ak sa aplikuje v prostredí, kde už existujú štrukturálne nerovnosti.¹¹

Výsledkom môže byť situácia, že napríklad systém automatického triedenia životopisov systematicky uprednostňuje mužských uchádzačov pred ženskými, pretože historické dáta obsahujú viac úspešných mužov v technických profesiách.¹² Takéto prípady už boli zaznamenané v praxi a upozorňujú na nutnosť dôsledného právneho rámca.

Princíp rovnakého zaobchádzania patrí medzi základné piliere európskeho i slovenského pracovného práva. V európskom kontexte vyplýva z článku 21 Charty základných práv EÚ, ktorý zakazuje diskrimináciu na základe pohlavia, rasy, farby pleti, etnického alebo sociálneho pôvodu, genetických čŕt, jazyka, náboženstva či politického presvedčenia.¹³ Slovenský právny poriadok prevzal tento princíp prostredníctvom antidiskriminačného zákona (zákon č. 365/2004 Z. z.), ktorý zakotvuje všeobecný zákaz diskriminácie v pracovnoprávných vzťahoch.¹⁴

Výzvou však je, že tradičné chápanie diskriminácie bolo vyvinuté pre „ľudské rozhodnutia“, nie pre rozhodovanie automatizovaných systémov. Pri algoritmickej diskriminácii chýba konkrétny „páchateľ“ – diskriminácia vzniká ako vedľajší produkt technického procesu. Otázkou je preto, ako zodpovednosť za tieto následky priradiť – či zamestnávateľovi, ktorý systém používa, alebo vývojárovi softvéru, ktorý algoritmus vytvoril.¹⁵

⁹ Barocas – Selbst, Big Data's Disparate Impact, Cal. L. Rev. 104(3), 2016, s. 672–674; 688–689.

¹⁰ Raghavan – Barocas – Kleinberg – Levy, Mitigating Bias in Algorithmic Hiring, FAT '20, 2020, s. 469–471.

¹¹ Tobler, Limits and Potential of the Concept of Indirect Discrimination, Luxembourg: OPOCE, 2008, s. 6; 24; 40–41.

¹² Destin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, Reuters, 2018.

¹³ Destin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, Reuters, 2018.

¹⁴ Zákon č. 365/2004 Z. z. (antidiskriminačný zákon), § 2a ods. 1–2.

¹⁵ GDPR (nariadenie (EÚ) 2016/679) – čl. 5 ods. 2, čl. 22 a čl. 24; AI Act – čl. 9, 10, 14; Kroll a kol., Accountable Algorithms, U. Pa. L. Rev. 165(3), 2017, s. 633–637; 701; Hacker, Teaching Fairness to Artificial Intelligence..., CMLR 55(4), 2018, s. 1148–1150.

Diskriminácia a transparentnosť algoritmov

Jedným z najväčších problémov je tzv. „black box“ efekt – algoritmy umelej inteligencie, najmä tie založené na hlbokom učení, sú pre používateľov netransparentné. Nemožno jednoducho vysvetliť, prečo bol konkrétny uchádzač odmietnutý. Nedostatok transparentnosti sťažuje obetiam algoritmickej diskriminácie uplatnenie právnej ochrany.¹⁶ Súdy tradične skúmajú motív konania a dôkazné bremeno sa rozdeľuje medzi žalobcu a žalovaného. Ak však zamestnávateľ nevie vysvetliť fungovanie algoritmu, je problematické zistiť, či došlo k diskriminácii a kto je za ňu zodpovedný.¹⁷

Rodová rovnosť má v európskom práve osobitné postavenie. Už od prijatia smernice 76/207/EHS o rovnakom zaobchádzaní medzi mužmi a ženami je právo EÚ vnímané ako významný nástroj pre odstraňovanie rodových nerovností. Napriek tomu sa nové technológie ukazujú ako „gendered technologies“ – odrážajú a reprodukovujú rodové stereotypy. Algoritmická diskriminácia sa môže prejaviť nielen pri samotnom výbere kandidátov, ale aj v určovaní miezd, prideľovaní pracovných zmien či hodnotení pracovného výkonu.¹⁸ Zasiahnuté sú najmä ženy v zraniteľných situáciách – tie, ktoré sa po kariérnej prestávke snažia vrátiť na trh práce alebo ktoré z povahy starostlivosti o rodinu častejšie pracujú na kratší pracovný úväzok.¹⁹

Pri skúmaní algoritmickej diskriminácie sa právna veda opiera o interdisciplinárny prístup. Na jednej strane analyzuje tradičné právne koncepty rovnakého zaobchádzania, na druhej strane čerpá z poznatkov informatiky, etiky a sociológie. V právnej doktríne sa preto čoraz častejšie objavuje potreba tzv. „algorithmic accountability“ – mechanizmov, ktoré umožnia preskúmateľnosť a zodpovednosť algoritmických systémov.²⁰

Právny rámec Európskej únie a Rady Európy

Základom európskeho antidiskriminačného práva je séria smerníc prijatých od konca 70. rokov, ktoré sa postupne rozšírili na viaceré oblasti verejného i súkromného života. Pre pracovné právo majú osobitný význam:

- Smernica 2000/43/ES o rovnakom zaobchádzaní bez ohľadu na rasový alebo etnický pôvod,

¹⁶ Wachter, S. – Mittelstadt, B. – Floridi, L.: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. *International Data Privacy Law* 7(2), 2017, s. 76–81; 90–92.

¹⁷ GDPR (nariadenie (EÚ) 2016/679) – čl. 5 ods. 2 (zásada zodpovednosti), čl. 24 (zodpovednosť prevádzkovateľa), čl. 22 ods. 1–3 (automatizované rozhodovanie).

¹⁸ European Institute for Gender Equality (EIGE): Artificial intelligence, platform work and gender equality. Luxembourg: Publications Office of the EU, 2021, s. 23; 81–85; 89.

¹⁹ EIGE, 2021, s. 11–15; 44–47; Eurostat: Employment rate of women with young children — dataset.

²⁰ Kroll, J. A. – Barocas, S. – Felten, E. W. – Reidenberg, J. R. – Robinson, D. G. – Yu, H.: Accountable Algorithms. *University of Pennsylvania Law Review* 165(3), 2017, s. 633–637; 701.

- Smernica 2000/78/ES ustanovujúca všeobecný rámec pre rovnaké zaobchádzanie v zamestnaní a povolani,
- Smernica 2006/54/ES o rovnakých príležitostiach a rovnakom zaobchádzaní medzi mužmi a ženami v zamestnaní a povolani.

Tieto predpisy ukladajú členským štátom povinnosť zabezpečiť, aby k diskriminácii v pracovnoprávných vzťahoch nedochádzalo, a aby obeť mali účinné prostriedky právnej ochrany.²¹

Algoritmická diskriminácia však odhaľuje limity týchto rámcov. Tradičné kategórie priamej a nepriamej diskriminácie nie vždy dokážu zachytiť komplexné dôsledky automatizovaného rozhodovania. Navyše, dôkazné bremeno je v algoritmických sporoch obzvlášť problematické, pretože uchádzač o zamestnanie nemá prístup k informáciám o fungovaní systému.²²

Kľúčovým nástrojom EÚ v oblasti algoritmického rozhodovania je aj Všeobecné nariadenie o ochrane údajov (GDPR). Článok 22 GDPR priznáva jednotlivcovi právo ne byť predmetom rozhodnutia založeného výlučne na automatizovanom spracúvaní vrátane profilovania, ktoré má právne účinky alebo sa ho obdobným spôsobom významne dotýka.²³ Toto ustanovenie má priamy dopad na algoritmické náborové systémy, pretože rozhodnutie o prijatí či odmietnutí uchádzača možno považovať za rozhodnutie s významnými účinkami.

Diskusia v právnej doktríne sa sústreďuje najmä na tzv. „právo na vysvetlenie“ – či má uchádzač právo poznať dôvody, na základe ktorých bol odmietnutý. Niektorí autori zastávajú názor, že GDPR zakotvuje len obmedzenú informačnú povinnosť, iní tvrdia, že ide o základné právo umožňujúce efektívnu ochranu pred diskrimináciou.²⁴

Súdny dvor EÚ (SDEÚ) zohráva zásadnú úlohu pri výklade princípu rovnakého zaobchádzania. V judikatúre opakovane zdôraznil, že nepriamu diskrimináciu možno ospravedlniť len vtedy, ak je sledovaný legitímny cieľ a zvolené opatrenia sú primerané a nevyhnutné.²⁵ Tieto kritériá budú dôležité aj pri posudzovaní algoritmických systémov – napríklad či ich použitie sleduje legitímny cieľ efektívnejšieho výberu a či existujú menej diskriminačné alternatívy.

Aj keď sa zatiaľ SDEÚ explicitne nevyjadril k algoritmickej diskriminácii, možno predpokladať, že jeho doktrína nepriamych účinkov bude aplikovateľná. Zároveň treba vziať do úvahy, že v kontexte algoritmov ide o tzv. „systemic discrimination“,

²¹ Smernica 2000/43/ES, čl. 7, 8; Smernica 2000/78/ES, čl. 9, 10; Smernica 2006/54/ES, čl. 17, 19.

²² GDPR – čl. 13–15, čl. 22; Wachter – Mittelstadt – Floridi, *Why a Right to Explanation...*, IDPL 7(2), 2017, s. 76–81; 90–92; Kroll a kol., *Accountable Algorithms*, U. Pa. L. Rev. 165(3), 2017, s. 633–637; 701.

²³ GDPR, čl. 22.

²⁴ Wachter – Mittelstadt – Floridi, 2017, s. 76–81; 90–92; Veale – Edwards, *Clarity, Surprises, and Further Questions...*, CLSR 34(2), 2018, s. 398–404.

²⁵ SDEÚ, C-170/84 *Bilka-Kaufhaus v. Weber von Hartz*, bod 36.

teda diskrimináciu, ktorá vzniká nie na základe jedného rozhodnutia, ale opakovanou aplikáciou algoritmu v tisíckach prípadov.²⁶

Nariadenie o umelej inteligencii (AI Act)

V roku 2024 Európska únia prijala Nariadenie (EÚ) 2024/1689 o umelej inteligencii (AI Act) – prvý komplexný právny rámec pre využívanie umelej inteligencie. Ide o prelomový predpis, ktorý zavádza kategorizáciu systémov podľa miery rizika. Náborové a pracovnoprávne algoritmy sú zaradené medzi vysokorizikové systémy, a preto podliehajú najprísnejším požiadavkám.²⁷

AI Act stanovuje povinnosti v oblastiach:

- riadenia rizík a kvality dát – systémy musia byť trénované na relevantných a reprezentatívnych dátach, aby sa minimalizovalo riziko diskriminácie,²⁸
- transparentnosti a dokumentácie – poskytovatelia systémov musia viesť technickú dokumentáciu a umožniť dohľad regulačných orgánov,²⁹
- ľudského dohľadu – algoritmické rozhodnutia musia byť kontrolované kvalifikovanými osobami, ktoré môžu zasiahnuť a zabrániť diskriminácii,³⁰
- ex ante a ex post testovania – povinné hodnotenie spravodlivosti a monitorovanie výstupov systémov.³¹

Pre oblasť rovnakého zaobchádzania je významné, že sa zavádza povinnosť systematicky hodnotiť riziká diskriminácie.³² Aj keď AI Act vytvára pevný právny rámec, otvorenou otázkou zostáva jeho vymáhateľnosť – teda do akej miery budú národné orgány schopné účinne kontrolovať súlad poskytovateľov s novými pravidlami.³³

Okrem EÚ zohráva dôležitú úlohu aj Rada Európy, ktorá prostredníctvom Európskeho dohovoru o ľudských právach (EDĽP) a judikatúry Európskeho súdu pre ľudské práva (ESĽP) poskytuje ochranu pred diskrimináciou. Článok 14 EDĽP zakazuje diskrimináciu pri uplatňovaní práv a slobôd chránených Dohovorom, zatiaľ čo Dodatokový protokol č. 12 rozširuje zákaz diskriminácie na akúkoľvek právom upravenú oblasť.³⁴

²⁶ Veale – Borgesius, Demystifying the EU AI Act, CLSR 43 (2022), s. 2–5; 17–22.

²⁷ AI Act (Nariadenie (EÚ) 2024/1689) – čl. 6 ods. 2–3 a príloha III, bod 4.

²⁸ AI Act, čl. 9, 10.

²⁹ AI Act, čl. 11–13.

³⁰ AI Act, čl. 14.

³¹ AI Act, čl. 9, čl. 15, kap. IX – čl. 7.

³² AI Act, čl. 27.

³³ Veale, M. – Borgesius, F. Z.: Demystifying the EU Artificial Intelligence Act, CLSR 43 (2022), s. 17–22.

³⁴ EDĽP, čl. 14; Dodatokový protokol č. 12, čl. 1.

ESLP v rozhodnutí D.H. a ostatní proti České republice konstatoval, že diskriminácia môže vzniknúť aj z dôvodu neprimeraného účinku zdanlivo neutrálnej politiky.³⁵ Tento prístup je analogicky použiteľný na algoritmickú diskrimináciu – súd sa pravdepodobne nebude zameriavať na úmysel, ale na účinky systému. Rada Európy navyše prijala odporúčania týkajúce sa umelej inteligencie a ľudských práv, v ktorých zdôrazňuje potrebu zodpovedného vývoja a využívania AI v súlade s princípom rovnosti.³⁶

Slovenský právny rámec

Ústredným právnym predpisom v oblasti rovnakého zaobchádzania je zákon č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou (antidiskriminačný zákon). Ten transponuje základné smernice EÚ a upravuje všeobecný zákaz diskriminácie vo všetkých oblastiach spoločenského života, vrátane pracovnoprávných vzťahov.³⁷ Zakazuje priamu aj nepriamu diskrimináciu, obťažovanie, príkaz na diskrimináciu a prenasledovanie. Pre oblasť algoritmickú diskrimináciu je osobitne dôležité ustanovenie § 2 ods. 2 písm. b), ktoré definuje nepriamu diskrimináciu ako zdanlivo neutrálny postup, ktorý znevýhodňuje osoby určitej skupiny. Tento koncept možno analogicky aplikovať na algoritmy využívané pri náboře, ktoré síce formálne uplatňujú neutrálne kritériá, ale ich dôsledkom môže byť systematické znevýhodnenie žien alebo iných skupín.³⁸

Zákon zároveň umožňuje obrátiť dôkazné bremeno – ak žalobca preukáže fakty, z ktorých možno usudzovať, že došlo k diskriminácii, je povinnosťou žalovaného dokázať, že k nej nedošlo. V kontexte algoritmických rozhodnutí to znamená, že zamestnávateľ by mal byť schopný vysvetliť fungovanie systému, ktorý používa. To však v praxi naráža na problém netransparentnosti algoritmov.^{39 40}

Zákonník práce (zákon č. 311/2001 Z. z.) obsahuje viacero ustanovení, ktoré nepriamo súvisia s ochranou pred algoritmickou diskrimináciou. V § 13 ods. 1 je zakotvená zásada rovnakého zaobchádzania, ktorá sa vzťahuje na prístup k zamestnaniu, pracovné podmienky i odmeňovanie. V § 119a je explicitne upravená zásada rovnakého odmeňovania mužov a žien za rovnakú prácu alebo prácu rovnakej

³⁵ ESLP, D.H. a ostatní proti České republice (GC, 13. 11. 2007).

³⁶ Council of Europe, Recommendation CM/Rec(2020)1.

³⁷ Zákon č. 365/2004 Z. z. (antidiskriminačný zákon); Smernica 2000/43/ES, Smernica 2000/78/ES, Smernica 2006/54/ES.

³⁸ Zákon č. 365/2004 Z. z., § 2a ods. 2.

³⁹ Zákon č. 365/2004 Z. z., § 11.

⁴⁰ GDPR - čl. 5 ods. 2, čl. 22 a 24; Wachter – Mittelstadt – Floridi, Why a Right to Explanation..., IDPL 7(2), 2017, s. 76–81; 90–92; Kroll a kol., Accountable Algorithms, U. Pa. L. Rev. 165(3), 2017, s. 633–637; 701.

hodnoty.⁴¹ V štádiu prípravy je samostatný zákon o transparentnosti v odmeňovaní, v prípade ktorého ide o transpozíciu smernice Európskeho parlamentu a Rady (EÚ) 2023/970 z 10. mája 2023 o posilnení uplatňovania zásady rovnakej odmeny pre mužov a ženy za rovnakú prácu alebo prácu rovnakej hodnoty prostredníctvom transparentnosti odmeňovania a mechanizmov presadzovania.

Ak by zamestnávateľ využíval algoritmus na určovanie miezd alebo hodnotenie pracovného výkonu, a tento systém by systematicky znevýhodňoval ženy alebo osoby s určitými charakteristikami (napríklad rodičov malých detí), mohlo by ísť o porušenie uvedených ustanovení. Zákonník práce síce priamo nepredpokladá algoritmické rozhodovanie, ale jeho zásady sa aplikujú aj na nové formy organizácie práce.⁴²

V slovenskom právnom poriadku je ochrana osobných údajov implementovaná prostredníctvom zákona č. 18/2018 Z. z. o ochrane osobných údajov, ktorý vykonáva GDPR. Tento zákon posilňuje práva dotknutých osôb a ukladá prevádzkovateľom povinnosť zabezpečiť, aby spracúvanie osobných údajov bolo zákonné, spravodlivé a transparentné.⁴³

Pri využívaní algoritmov na pracovnoprávne účely je preto nevyhnutné rešpektovať nielen antidiskriminačné normy, ale aj pravidlá ochrany údajov – napríklad obmedziť rozsah zhromažďovaných údajov len na tie, ktoré sú nevyhnutné pre nábor, a zabezpečiť uchádzačom prístup k informáciám o spracúvaní.⁴⁴

V praxi zohrávajú významnú úlohu kontrolné a dohliadacie orgány. V oblasti rovnakého zaobchádzania pôsobí Slovenské národné stredisko pre ľudské práva (SNSLP), ktoré poskytuje právne poradenstvo a vedie spory v oblasti diskriminácie. V kontexte algoritmickej diskriminácie by stredisko mohlo vystupovať ako dôležitý aktér pri monitorovaní nových foriem nerovností.⁴⁵

Ďalším relevantným orgánom je Úrad na ochranu osobných údajov SR, ktorý dohliada na dodržiavanie pravidiel GDPR a zákona o ochrane osobných údajov. Ak by algoritmus porušoval zásadu spravodlivosti alebo transparentnosti, úrad by mohol zasiahnuť sankciami voči prevádzkovateľovi.⁴⁶

Slovenský právny rámec poskytuje základné nástroje na ochranu pred diskrimináciou a na zabezpečenie rovnakého zaobchádzania. Problémom je však praktická aplikácia týchto pravidiel na komplexné algoritmické systémy. Súdny a orgány dohľadu nemajú zatiaľ dostatočné skúsenosti s posudzovaním prípadov algoritmickej diskriminácie.

⁴¹ Zákonník práce, § 13 ods. 1–3 a § 119a.

⁴² Zákonník práce, § 13; § 119a.

⁴³ Zákon č. 18/2018 Z. z. o ochrane osobných údajov.

⁴⁴ GDPR, čl. 5 ods. 1(c), čl. 13–15.

⁴⁵ Slovenské národné stredisko pre ľudské práva (SNSLP): Správa o dodržiavaní zásady rovnakého zaobchádzania, 2023.

⁴⁶ Úrad na ochranu osobných údajov SR: Správa o stave ochrany osobných údajov, 2023; GDPR, čl. 58.

Chýba metodika, ktorá by umožnila identifikovať diskriminačný účinok algoritmu a priradiť zodpovednosť konkrétnemu subjektu.

Osobitnou výzvou je aj nedostatok dát o tom, ako sa algoritmy v skutočnosti používajú na slovenskom trhu práce. Bez empirických analýz je ťažké posúdiť mieru rizika a efektívnosť existujúcich právnych nástrojov. Zároveň sa ukazuje potreba doplniť právny rámec o špecifické ustanovenia reflektujúce digitálne prostredie, prípadne prijať soft-law nástroje (usmernenia, odporúčania), ktoré by zamestnávateľom poskytli jasnejšie pravidlá pre používanie umelej inteligencie.

Príklady z praxe a riziká pre ženy v zraniteľných situáciách

Jedným z najznámejších prípadov algoritmickej diskriminácie je skúsenosť technologickej spoločnosti Amazon, ktorá testovala interný náborový systém založený na umelej inteligencii. Algoritmus, trénovaný na historických dátach, systematicky znevýhodňoval uchádzačky o prácu, pretože v minulosti prevládali v technických profesiách muži.⁴⁷ Hoci bol projekt napokon zrušený, prípad jasne ukázal, že aj renomované spoločnosti nedokážu vždy predísť diskriminačným účinkom.

Podobné výsledky priniesli štúdie z USA a Spojeného kráľovstva, kde sa zistilo, že systémy na analýzu videorozhovorov používané v náboře uchádzačov vyhodnocovali ženských kandidátov menej priaznivo, najmä ak ich prejav alebo mimika nezodpovedali „štandardnému“ modelu úspešného uchádzača.⁴⁸ Tento typ hodnotenia posilňuje rodové stereotypy, pretože preferuje komunikáciu, ktorá je kultúrne spájaná s mužským správaním.

Na Slovensku nie sú doposiaľ zdokumentované medializované prípady algoritmickej diskriminácie, čo však neznamená, že sa nevyskytujú. V praxi už pôsobia medzinárodné spoločnosti, ktoré využívajú digitálne náborové platformy. Rizikom je, že tieto systémy sú často vyvíjané v iných krajinách a na iných dátach, ktoré nereflektujú špecifiká slovenského trhu práce.⁴⁹

Ženy v zraniteľných situáciách – najmä po návrate z rodičovskej dovolenky alebo počas obdobia starostlivosti o deti – patria na Slovensku medzi dlhodobo znevýhodnené skupiny. Štatistiky Eurostatu ukazujú, že zamestnanosť žien s malými deťmi je výrazne nižšia ako u mužov a zároveň pretrváva značný rodový mzdový rozdiel.⁵⁰ Ak sú algoritmy trénované na historických údajoch reflektujúcich tieto

⁴⁷ Dastin, J.: Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women. Reuters, 2018.

⁴⁸ Raghavan, M. – Barocas, S. – Kleinberg, J. – Levy, K.: Mitigating Bias in Algorithmic Hiring. FAT '20*, 2020, s. 469–471; 478–480.

⁴⁹ European Institute for Gender Equality (EIGE): Artificial intelligence, platform work and gender equality. Luxembourg: Publications Office of the EU, 2021, s. 11–15; 23; 81–85; 89.

⁵⁰ Eurostat: Employment rate of women with young children — dataset; EIGE, 2021, s. 28–32.

nerovnosti, je pravdepodobné, že budú znevýhodňovať práve ženy po kariérnej prestávke.

Riziká pre ženy v zraniteľných situáciách sú okrem iných nasledujúce:

1. Návrat na trh práce po kariérnej prestávke

Algoritmy hodnotiace kontinuitu pracovnej histórie môžu penalizovať ženy, ktoré prerušili kariéru z dôvodu materstva. Prestávky v životopise sú často interpretované ako „negatívny signál“, hoci ide o legítimnú životnú situáciu.⁵¹

2. Atypické formy práce

Ženy častejšie pracujú na skrátenej úväzok alebo v dočasných pracovných pomeroch. Algoritmy môžu tieto formy zamestnania hodnotiť ako menej stabilné, a preto menej atraktívne pre zamestnávateľa, čím sa reprodukuje nerovnosť.⁵²

3. Hodnotenie kompetencií a výkonu

Automatizované systémy, ktoré analyzujú reč či neverbálnu komunikáciu, môžu byť nastavené tak, že preferujú „mužský“ komunikačný štýl – sebavedomý, priamočiary a asertívny. Ženské prejavy môžu byť nespravodlivo hodnotené ako menej presvedčivé.⁵³

4. Predikčné modely rizika odchodu zo zamestnania

Niektoré spoločnosti používajú algoritmy na predikciu fluktuácie zamestnancov. Ak systém identifikuje ženy s malými deťmi ako „rizikóvu skupinu“ z hľadiska odchodu, môže to viesť k ich znevýhodneniu pri kariérnom postupe alebo povyšovaní.⁵⁴

Riziká algoritmickej diskriminácie sa zosilňujú, ak sa rodový aspekt kombinuje s inými zraniteľnosťami – napríklad v prípade žien so zdravotným postihnutím, starších žien alebo migrantiek. Práve intersekcionalný prístup je kľúčový pre pochopenie, ako algoritmy môžu reprodukovать viacnásobné nerovnosti. Ak algoritmus zohľadňuje napríklad miesto bydliska či jazykové schopnosti, môže znevýhodňovať ženy z menšín alebo žijúce na vidieku.⁵⁵

Aj keď slovenský a európsky právny rámec formálne chráni pred diskrimináciou, praktické uplatnenie právnej ochrany je v prípade algoritmov náročné. Problémom je:

- nedostatok transparentnosti systémov (uchádzačky nevedia preukázať, že boli odmietnuté z diskriminačných dôvodov),
- finančná a časová náročnosť súdnych konaní,
- nízka informovanosť obetí o ich právach.

⁵¹ EIGE, 2021, s. 11–15; 44–47.

⁵² EIGE, 2021, s. 23; 81–85; De Stefano, V.: The Rise of the “Just-in-Time Workforce”... CLLPJ 37(3), 2016, s. 472–474; 499–502.

⁵³ Raghavan a kol., 2020, s. 469–471; 478–480.

⁵⁴ Barocas – Selbst, 2016, s. 688–689; EIGE, 2021, s. 81–85.

⁵⁵ Cho, S. – Crenshaw, K. – McCall, L.: Toward a Field of Intersectionality Studies. Signs 38(4), 2013, s. 786; 800.

Tieto bariéry vedú k tomu, že diskriminačné účinky algoritmov ostávajú často nepovšimnuté a neadresované, čo má za následok prehĺbovanie nerovností na trhu práce.⁵⁶

Príležitosti digitalizácie pre ženy na trhu práce

Digitalizácia trhu práce nie je iba zdrojom rizík, ale prináša aj viaceré pozitívne príležitosti, ktoré môžu významne prispieť k rovnosti príležitostí medzi ženami a mužmi. Ak sú algoritmy navrhnuté a regulované správne, môžu pôsobiť ako nástroj na znižovanie existujúcich nerovností.⁵⁷

Flexibilné formy práce

Jedným z najväčších prínosov digitalizácie je rozšírenie možností flexibilnej práce – najmä práce na diaľku, práce z domu alebo prostredníctvom digitálnych platforiem. Tieto formy môžu ženám uľahčiť zosúladenie pracovného a rodinného života. Pandémia COVID-19 ukázala, že home office sa stal reálnou alternatívou vo viacerých sektoroch, a mnohé ženy tak získali lepší prístup k zamestnaniu, ktoré by inak bolo skomplikované starostlivosťou o deti či iných členov rodiny.⁵⁸

Flexibilné usporiadanie pracovného času a priestoru je obzvlášť významné pre ženy v zraniteľných situáciách, ktoré sa po kariérnej prestávke vracajú na trh práce. Digitalizácia otvára dvere aj pre čiastočné úväzky alebo projektovú prácu, ktorá môže slúžiť ako mostík k plnohodnotnému zamestnaniu.⁵⁹

Prístup k vzdelávaniu a rekvalifikáciám

Digitálne technológie umožňujú široký prístup k online vzdelávaniu, rekvalifikáciám a celoživotnému učniu. Platformy ako Coursera, edX či lokálne projekty EÚ ponúkajú kurzy, ktoré môžu pomôcť ženám získať nové zručnosti – napríklad v oblasti IT, digitálneho marketingu alebo administratívy. Práve tieto zručnosti sú čoraz viac žiadané na modernom trhu práce.⁶⁰

Výhodou je aj dostupnosť vzdelávania pre ženy z menších miest a vidieka, ktoré by inak mali obmedzené možnosti dochádzania. Online formy umožňujú prístup k

⁵⁶ Veale, M. – Edwards, L.: Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making. CLSR 34(2), 2018, s. 398–404.

⁵⁷ Raghavan, M. – Barocas, S. – Kleinberg, J. – Levy, K.: Mitigating Bias in Algorithmic Hiring. FAT '20*, 2020, s. 478–480.

⁵⁸ Eurofound: Telework and ICT-based Mobile Work: Flexible Working in the Digital Age. Luxembourg: Publications Office of the EU, 2020, s. 1–5; 27–33; Kossek, E. E.: Managing work–life boundaries in the digital age. Organizational Dynamics 45(3), 2016, s. 259–262; 266–268.

⁵⁹ European Institute for Gender Equality (EIGE): Artificial intelligence, platform work and gender equality. Luxembourg: Publications Office of the EU, 2021, s. 44–47.

⁶⁰ European Commission: Digital Education Action Plan 2021–2027.

rovnakým znalostiam ako vo veľkých mestách a môžu tak prispieť k regionálnej vyrovnanosti.⁶¹

Transparentnosť a znižovanie predsudkov

Ak sú algoritmy nastavené správne a podrobené nezávislej kontrole, môžu prispieť k väčšej transparentnosti rozhodovania v náboře. Algoritmické systémy môžu eliminovať subjektívne predsudky personalistov – napríklad stereotypné predstavy o „ideálnom uchádzačovi“ podľa veku alebo rodinného stavu.⁶²

Výskumy ukazujú, že algoritmy, ktoré sú trénované na vyvážených dátach a obsahujú zabudované kontrolné mechanizmy, môžu viesť k spravodlivejšiemu hodnoteniu kandidátov. Týmto spôsobom je možné transformovať algoritmy z potenciálne diskriminačných nástrojov na prostriedky podpory rovnosti.⁶³

Podpora podnikania a nových pracovných príležitostí

Digitalizácia vytvára priestor pre vznik nových podnikateľských modelov – od e-commerce až po mikropodnikanie prostredníctvom online platforiem. Pre ženy môže byť táto cesta atraktívna, pretože im umožňuje začať podnikat' s relatívne nízkymi vstupnými nákladmi a zároveň si flexibilne organizovať pracovný čas.⁶⁴

Zaujímavým trendom je aj rozvoj tzv. gig economy. Hoci so sebou prináša riziká neistoty a absencie sociálneho zabezpečenia, môže predstavovať príležitosť pre ženy, ktoré potrebujú flexibilitu alebo chcú kombinovať prácu s rodinnými povinnosťami. Prepojenie týchto foriem práce s adekvátnymi právnymi zárukami by mohlo vytvoriť stabilný základ pre posilnenie postavenia žien na trhu práce.⁶⁵

Technologická inklúzia a rodová perspektíva

Európska únia zdôrazňuje potrebu rodovo inkluzívneho prístupu k digitalizácii. Programy ako „Women in Digital“ či iniciatívy Európskeho inštitútu pre rodovú rovnosť (EIGE) podporujú zapájanie žien do IT sektora a vývoja technológií. Cieľom je nielen umožniť ženám využívať digitálne technológie, ale aj formovať ich dizajn a hodnoty. Ak sa ženy budú aktívne podieľať na vývoji algoritmov, je väčšia šanca, že budú zohľadnené ich špecifické potreby a že technológie nebudú jednostranne reprodukovat' mužskú skúsenosť.⁶⁶

⁶¹ EIGE, 2021, s. 28–32.

⁶² Kroll, J. A. – Barocas, S. – Felten, E. W. – Reidenberg, J. R. – Robinson, D. G. – Yu, H.: *Accountable Algorithms*. University of Pennsylvania Law Review 165(3), 2017, s. 633–637; 701.

⁶³ Raghavan a kol., 2020, s. 469–471; 478–480.

⁶⁴ EIGE, 2021, s. 11–15; 28–32.

⁶⁵ De Stefano, V.: *The Rise of the “Just-in-Time Workforce”: On-Demand Work, Crowdswork, and Labour Protection in the Gig-Economy*. CLLPJ 37(3), 2016, s. 472–474; 499–502.

⁶⁶ EIGE, 2021, s. 81–85; 89.

Záver

Digitalizácia trhu práce prináša zásadné zmeny, ktoré majú dvojitý charakter. Na jednej strane otvára nové možnosti – flexibilné formy práce, prístup k vzdelávaniu či zvýšenú transparentnosť výberových procesov.⁶⁷ Na druhej strane so sebou nesie významné riziká, najmä ak sa algoritmy stávajú nositeľmi predsudkov a štrukturálnych nerovností.⁶⁸

Analýza ukázala, že algoritmická diskriminácia predstavuje špecifickú formu nepriamej diskriminácie, ktorá je zvlášť citlivá v kontexte pracovného práva. Riziká sú obzvlášť výrazné pre ženy v zraniteľných situáciách – po kariérnej prestávke, počas materstva alebo pri práci na atypických úväzkoch. Algoritmy môžu tieto situácie interpretovať ako „odchýlky od normy“ a následne viesť k systematickému znevýhodňovaniu týchto žien.⁶⁹

Právny rámec EÚ poskytuje robustné základy v podobe antidiskriminačných smerníc, GDPR a nedávno prijatého AI Act-u. Ten zaraďuje náborové algoritmy medzi vysokorizikové systémy a zavádza povinnosti, ktoré majú minimalizovať diskriminačné účinky.⁷⁰ Významná je aj judikatúra Súdneho dvora EÚ, ktorá kladie dôraz na proporionalitu a primeranosť opatrení⁷¹, a judikatúra ESLP, ktorá uznáva diskrimináciu aj bez úmyslu – ak má opatrenie neprimerané účinky.⁷²

Slovenský právny rámec vychádza z antidiskriminačného zákona a Zákonníka práce, ktoré obsahujú jasný zákaz diskriminácie. Problémom však zostáva praktická aplikácia týchto pravidiel na algoritmické systémy. Transparentnosť a preukázateľnosť fungovania algoritmov je nízka, čo komplikuje dôkaznú situáciu pred súdmi.⁷³ Orgány ako Slovenské národné stredisko pre ľudské práva či Úrad na ochranu osobných údajov majú potenciál zohrávať významnú úlohu, no zatiaľ chýba metodika aj skúsenosti s týmto typom sporov.⁷⁴

Z medzinárodných aj domácich skúseností vyplýva, že algoritmická diskriminácia nie je hypotetickým problémom, ale reálnym javom, ktorý už v praxi priniesol negatívne dôsledky. Skúsenosť Amazonu či analýzy videointerview algoritmov ukazujú, že aj

⁶⁷ Eurofound: Telework and ICT-based Mobile Work, 2020, s. 1–5; 27–33.

⁶⁸ Barocas, S. – Selbst, A. D.: Big Data's Disparate Impact. California Law Review 104(3), 2016, s. 672–674; 688–689.

⁶⁹ EIGE: Artificial intelligence, platform work and gender equality. Luxembourg: Publications Office of the EU, 2021, s. 11–15; 44–47; 81–85.

⁷⁰ AI Act – čl. 6 ods. 2–3; príloha III, bod 4; čl. 9–14.

⁷¹ SDEÚ, C-170/84 Bilka-Kaufhaus v. Weber von Hartz.

⁷² ESLP, D.H. a ostatní proti ČR (GC, 13. 11. 2007), §§ 184; 188; 195.

⁷³ Zákon č. 365/2004 Z. z. (antidiskriminačný zákon), § 2a ods. 1–2; Zákonník práce (zákon č. 311/2001 Z. z.), § 13; § 119a.

⁷⁴ Destin, J.: Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women. Reuters, 2018; Raghavan, M. – Barocas, S. – Kleinberg, J. – Levy, K.: Mitigating Bias in Algorithmic Hiring. FAT '20*, 2020, s. 469–471; 478–480.

dobré mienené riešenia môžu viesť k systematickému vylučovaniu žien. Na Slovensku sa tieto prípady zatiaľ výraznejšie neobjavili, no vzhľadom na rastúci vplyv digitálnych platforiem a medzinárodných korporácií je len otázkou času, kedy sa tento problém prejaví aj lokálne.⁷⁵

Odporúčania

Zvýšená transparentnosť – zamestnávateľia by mali byť povinní informovať uchádzačov o tom, akým spôsobom algoritmus vyhodnocuje ich prihlášku a ktoré kritériá sú rozhodujúce.⁷⁶

Metodická podpora a dohľad – štátne orgány a SNSLP by mali vypracovať metodiky pre posudzovanie algoritmickej diskriminácie a poskytovať zamestnávateľom usmernenia.⁷⁷

Rodovo inkluzívny dizajn algoritmov – pri vývoji systémov je potrebné zohľadniť rodové aspekty a zabezpečiť testovanie na reprezentatívnych vzorkách.⁷⁸

Interdisciplinárna spolupráca – právnici, IT odborníci a sociológovia by mali spoločne pracovať na vývoji a hodnotení algoritmov (accountability by design), aby sa minimalizovalo riziko diskriminácie.⁷⁹

Podpora vzdelávania a rekvalifikácií – digitalizácia by mala byť využitá ako nástroj posilnenia postavenia žien prostredníctvom dostupného online vzdelávania a flexibilných pracovných modelov.⁸⁰

Záverom možno konštatovať, že digitalizácia sama osebe nie je hrozbou pre rovnosť príležitostí. Ak je však ponechaná bez regulácie a kontroly, môže viesť k reprodukcii nerovností a diskriminácie. Správne nastavené právne a inštitucionálne rámce, doplnené o rodovo citlivý prístup, môžu naopak premeniť digitalizáciu na príležitosť – na vytvorenie spravodlivejšieho a inkluzívnejšieho trhu práce pre všetkých.

Zoznam použitej literatúry

1. BAROCAS, Solon – SELBST, Andrew D.: Big Data's Disparate Impact. In: California Law Review, 104(3), 2016, s. 671–732. DOI/SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

⁷⁵ EIGE, 2021, s. 81–85; 89.

⁷⁶ GDPR – čl. 13–15; AI Act, čl. 13.

⁷⁷ GDPR, čl. 35; AI Act, čl. 9, čl. 72; Council of Europe, CM/Rec(2020)1, časť B (1.1), 5.2, 6.1.

⁷⁸ AI Act, čl. 10.

⁷⁹ Kroll, J. A. a kol.: Accountable Algorithms. U. Pa. L. Rev. 165(3), 2017, s. 633–637; 701; Veale, M. – Edwards, L.: Clarity, Surprises... CLSR 34(2), 2018, s. 398–404.

⁸⁰ European Commission: Digital Education Action Plan 2021–2027.

2. BELAVUSAU, Uladzislau – HENRARD, Kristin: A Bird's Eye View on EU Anti-Discrimination Law: The Impact of the 2000 Equality Directives. In: *German Law Journal*, 20(5), 2019, s. 614–636. DOI: <https://doi.org/10.1017/glj.2019.53>
3. BOGEN, Miranda – RIEKE, Aaron: Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias. *Upturn Report*, 2018. Dostupné na: <https://www.upturn.org/reports/2018/hiring-algorithms>
4. CHARTA ZÁKLADNÝCH PRÁV EURÓPSKEJ ÚNIE (2012/C 326/02). Ú. v. EÚ C 326, 26. 10. 2012.
5. CHO, Sumi – CRENSHAW, Kimberlé W. – McCALL, Leslie: Toward a Field of Intersectionality Studies. In: *Signs*, 38(4), 2013, s. 785–810. DOI: <https://doi.org/10.1086/669608>
6. COUNCIL OF EUROPE: Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 2020. Dostupné na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809e1154
7. COWGILL, Bo – DELL'ACQUA, Fabrizio – DENG, Samuel – HSU, Daniel – VERMA, Nakul – CHAINTREAU, Augustin: Biased Programmers? Or Biased Data? A Field Experiment in Operationalizing AI Ethics. In: *Proceedings of the 21st ACM Conference on Economics and Computation (EC '20)*, 2020, s. 679–681. Dostupné na: <https://ssrn.com/abstract=3615404>
8. CRIADO PEREZ, Caroline: *Invisible Women: Data Bias in a World Designed for Men*. London: Vintage, 2019. ISBN 978-1-78470-628-9.
9. DASTIN, Jeff: Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women. *Reuters*, 2018. Dostupné na: <https://www.reuters.com/article/amazon-ai-hiring-idUSKCN1MK08G>
10. DE STEFANO, Valerio: The Rise of the "Just-in-Time Workforce": On-Demand Work, Crowdwork, and Labour Protection in the Gig-Economy. In: *Comparative Labor Law & Policy Journal*, 37(3), 2016, s. 471–504. DOI: <http://dx.doi.org/10.2139/ssrn.2682602>
11. DODATKOVÝ PROTOKOL č. 12 k EDLP o všeobecnom zákaze diskriminácie. Rím, 4. 11. 2000, ETS č. 177; vstup do platnosti: 1. 4. 2005.
12. EUROPEAN INSTITUTE FOR GENDER EQUALITY (EIGE): Artificial intelligence, platform work and gender equality. Luxembourg: Publications Office of the EU, 2021. DOI (PDF): 10.2839/372863. Dostupné na: <https://eige.europa.eu/publications-resources/publications/artificial-intelligence-platform-work-and-gender-equality>
13. EUROFOUND: *Telework and ICT-based Mobile Work: Flexible Working in the Digital Age*. Luxembourg: Publications Office of the EU, 2020. Dostupné na:

<https://www.eurofound.europa.eu/publications/report/2020/telework-and-ict-based-mobile-work-flexible-working-in-the-digital-age>

14. EURÓPSKY DOHOVOR O OCHRANE ĽUDSKÝCH PRÁV A ZÁKLADNÝCH SLOBÔD (EDĽP). Rím, 4. 11. 1950.
15. EUROPEAN COMMISSION: Digital Education Action Plan 2021–2027, 2021. Dostupné na: <https://education.ec.europa.eu/focus-topics/digital/education-action-plan>
16. EUROSTAT: Employment rate of women with young children (dataset), 2023. Dostupné na: <https://ec.europa.eu/eurostat/>
17. HACKER, Philipp: Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law. *Common Market Law Review*, 55(4), 2018, s. 1143–1185. SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164973
18. KOSSEK, Ellen Ernst: Managing work–life boundaries in the digital age. In: *Organizational Dynamics*, 45(3), 2016, s. 258–270. DOI: <https://doi.org/10.1016/j.orgdyn.2016.07.010>
19. KROLL, Joshua A. – HUEY, Joanna – BAROCAS, Solon – FELTEN, Edward W. – REIDENBERG, Joel R. – ROBINSON, David G. – YU, Harlan: Accountable Algorithms. In: *University of Pennsylvania Law Review*, 165(3), 2017, s. 633–705. Dostupné na: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/
20. MITTELSTADT, Brent Daniel – ALLO, Patrick – TADDEO, Mariarosaria – WACHTER, Sandra – FLORIDI, Luciano: The Ethics of Algorithms: Mapping the Debate. In: *Big Data & Society*, 3(2), 2016, s. 1–21. DOI: <https://doi.org/10.1177/2053951716679679>
21. NARIADENIE (EÚ) 2016/679 (GDPR): Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov.
22. NARIADENIE (EÚ) 2024/1689 (AI Act): Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (AI Act).
23. O’NEIL, Cathy: *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown, 2016. ISBN 978-0553418811.
24. RAGHAVAN, Manish – BAROCAS, Solon – KLEINBERG, Jon – LEVY, Karen: Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices. In: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT ’20)**, ACM, 2020, s. 469–481. DOI: <https://doi.org/10.1145/3351095.3372828>
25. ROZSUDOK ESLP: D.H. a ostatní proti Českej republike, sťažnosť č. 57325/00, 13. november 2007.

26. ROZSUDOK SÚDNEHO DVORA EÚ: Bilka-Kaufhaus GmbH v. Karin Weber von Hartz (C-170/84), rozsudok z 13. mája 1986.
27. RUBERY, Jill – GRIMSHAW, Damian: Gender and the Minimum Wage. In: LEE, Sangheon – McCANN, Deirdre (eds.): *Regulating for Decent Work: New Directions in Labour Market Regulation*. Basingstoke/Geneva: Palgrave Macmillan & ILO, 2011, s. 226–254. DOI: https://doi.org/10.1057/9780230307834_9
28. SELBST, Andrew D. – BAROCAS, Solon: The Intuitive Appeal of Explainable Machines. In: *Fordham Law Review*, 87(3), 2018, s. 1085–1139. Dostupné na: <https://ir.lawnet.fordham.edu/flr/vol87/iss3/8/>
29. SLOVENSKÉ NÁRODNÉ STREDISKO PRE ĽUDSKÉ PRÁVA (SNSLP): Správa o dodržiavaní zásady rovnakého zaobchádzania, 2023. Dostupné na: <https://www.snslp.sk/>
30. SMERNICA 2006/54/ES Európskeho parlamentu a Rady z 5. júla 2006 o vykonávaní zásady rovnakých príležitostí a rovnakého zaobchádzania medzi mužmi a ženami v oblasti zamestnania a povolania.
31. SMERNICA RADY 2000/43/ES z 29. júna 2000 o rovnakom zaobchádzaní bez ohľadu na rasový alebo etnický pôvod.
32. SMERNICA RADY 2000/78/ES z 27. novembra 2000, ktorou sa ustanovuje všeobecný rámec pre rovnaké zaobchádzanie v zamestnaní a povolani.
33. TOBLER, Christa: *Limits and Potential of the Concept of Indirect Discrimination*. Luxembourg: Office for Official Publications of the European Communities, 2008. ISBN 978-92-79-10150-2. DOI: 10.2767/56607.
34. ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SR: Správa o stave ochrany osobných údajov v Slovenskej republike, 2023. Dostupné na: <https://dataprotection.gov.sk/>
35. VEALE, Michael – ZUIDERVEEN BORGESIOUS, Frederik: Demystifying the EU Artificial Intelligence Act. In: *Computer Law & Security Review*, 43, 2022, 105587. DOI: <https://doi.org/10.48550/arXiv.2107.03721>
36. VEALE, Michael – EDWARDS, Lilian: Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making. In: *Computer Law & Security Review*, 34(2), 2018, s. 398–404. DOI: <https://doi.org/10.1016/j.clsr.2017.12.002>
37. WACHTER, Sandra – MITTELSTADT, Brent – FLORIDI, Luciano: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In: *International Data Privacy Law*, 7(2), 2017, s. 76–99. DOI: <https://doi.org/10.1093/idpl/ixx005>
38. WACHTER, Sandra – MITTELSTADT, Brent: A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. In: *Columbia*

Business Law Review, 2019(2), s. 494–620. SSRN:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

39. ZÁKON č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
40. ZÁKON č. 311/2001 Z. z. (Zákonník práce).
41. ZÁKON č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou (antidiskriminačný zákon).

Kontaktné údaje

JUDr. PhDr. Barbara Faktor Pavlíková, PhD.

barbarapavlikova@gmail.com

Katedra pracovného práva a práva sociálneho zabezpečenia

Právnická fakulta Univerzity Komenského v Bratislave

DIGITÁLNA DÔSTOJNOSŤ ALEBO DIGITÁLNA DISKRIMINÁCIA V PRACOVNOM PRÁVE¹

DIGITAL DIGNITY OR DIGITAL DISCRIMINATION IN LABOUR LAW

Mária Nováková²

Abstrakt: Dynamická digitalizácia zásadným spôsobom mení pracovnoprávne vzťahy a spôsoby organizácie práce. Prináša vyššiu flexibilitu, transparentnosť a dostupnosť príležitostí, no zároveň vytvára nové bariéry a riziká diskriminácie. Príspevok rozvíja koncept „digitálnej dôstojnosti“ ako právno-etický rámec, ktorý má chrániť zamestnanca pred dehumanizáciou a asymetriou moci v dátovo riadenom prostredí. Analyzujeme najmä algoritmické riadenie a automatizované rozhodovanie v nábere, hodnotení výkonu a ukončovaní pracovného pomeru, nerovnomernú úroveň digitálnej gramotnosti a rozdielny prístup k digitálnym technológiám. Na základe medzinárodných a európskych štandardov dôstojnosti a rovnakého zaobchádzania, ako aj slovenskej právnej úpravy, identifikujeme limity existujúceho rámca. Navrhujeme jeho doplnenie o právo na informácie o použití algoritmov, povinný ľudský dohľad a možnosť druhej inštancie pri čisto automatizovaných rozhodnutiach, povinnosť posúdenia vplyvov na práva zamestnancov a uznanie „digitálneho znevýhodnenia“ ako diskriminačného dôvodu. Osobitnú pozornosť venujeme skupine 50+, ktorá čelí kombinácii historických, psychologických, štrukturálnych a zdravotných bariér. V závere formuluje príspevok odporúčania pre legislatívu, kolektívne vyjednávanie a politiku celoživotného vzdelávania, vrátane inkluzívnych rekvalifikácií a primeraných úprav digitálnych nástrojov, s cieľom zosúladiť inováciu s ochranou dôstojnosti a práv zamestnancov a predchádzať digitálnej diskriminácii v praxi verejnej aj súkromnej sféry.

Kľúčové slová: digitálna dôstojnosť, pracovné právo; digitálna diskriminácia; rovnosť príležitostí; algoritmické riadenie; umelá inteligencia

Abstract: Accelerating digitalisation is reshaping labour relations and work organisation. It offers greater flexibility, transparency, and access to opportunities, yet simultaneously creates new barriers and discrimination risks.

¹ Príspevok bol spracovaný pod záštitou projektu VEGA č. 1/0677/24 s názvom „Ženy v kríze“.

²Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta Univerzity Komenského v Bratislave.

This article advances the concept of “digital dignity” as a legal-ethical framework to protect employees from dehumanisation and power asymmetries in data-driven workplaces. We examine algorithmic management and automated decision-making in recruitment, performance evaluation, and dismissal, uneven digital literacy, and unequal access to technologies. Drawing on international and European standards of human dignity and equal treatment and Slovak labour and anti-discrimination law, we identify gaps in the framework. We propose reforms: a right to information about algorithm use; mandatory human oversight and second-instance review of purely automated decisions; impact assessments focused on employees’ rights; and recognition of “digital disadvantage” as a protected ground. Attention is devoted to workers aged 50+, who face psychological, structural, and health barriers. The paper concludes with recommendations for legislation, collective bargaining, and lifelong-learning policy, including reskilling and reasonable accommodation of digital tools, to reconcile innovation with the protection of workers’ dignity, prevent digital discrimination in public and private sectors.

Key words: digital dignity; labour law; digital discrimination; equal opportunities; algorithmic management; artificial intelligence

Úvod

Digitalizácia v posledných desaťročiach zásadným spôsobom mení charakter práce a pracovnoprávných vzťahov. Tradičné formy zamestnania sú dopĺňané alebo nahrádzané digitálnymi nástrojmi, ktoré zasahujú do spôsobu výkonu práce, jej organizácie i riadenia zamestnancov. „Zavádzanie umelej inteligencie (AI) do pracovného prostredia predstavuje jednu z najvýznamnejších výziev súčasnej digitálnej transformácie. Automatizované rozhodovanie, algoritmickej analýza výkonu či prediktívne modely v oblasti riadenia ľudských zdrojov postupne menia tradičný rámec pracovnoprávných vzťahov. Tento vývoj vyvoláva otázky týkajúce sa ochrany základných práv zamestnancov, rovnováhy medzi efektívnosťou a dôstojnosťou na pracovisku, ako aj primeraného nastavenia práv a povinností zamestnancov pri interakcii s AI systémami.“³ Rozvoj práce na diaľku, hybridných foriem zamestnávania a najmä rastúce využívanie algoritmickej riadenia, či umelej inteligencie v personálnych procesoch (nábor,

³ DAŇKO, Martin - PORUBAN, Andrej: Práva a povinnosti zamestnancov v Akte o umelej inteligencii. In Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024. Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie. Trenčín: Trenčianska univerzita Alexandra Dubčeka v Trenčíne, Fakulta sociálno-ekonomických vzťahov, 2025. ISBN 978-80-8295-044-4.

hodnotenie, rozvrhovanie pracovného času) vytvára nové právne i spoločenské výzvy.

Na jednej strane digitalizácia sľubuje zvýšenie efektívnosti, flexibility a dostupnosti pracovných príležitostí, zároveň na druhej strane prináša riziko vzniku nových foriem nerovností a diskriminácie.

Význam skúmania dôstojnosti a rizík diskriminácie v digitálnom pracovnom prostredí

Otázka digitálnej dôstojnosti a digitálnej diskriminácie má v pracovnom práve zásadný význam. Je nepochybné, ako poukázal napr. Liu et al., že digitalizácia môže prispieť k inklúzii na pracovnom trhu prostredníctvom lepšieho prístupu k pracovným príležitostiam, možnosti flexibilnejšie zosúladiť pracovný a rodinný život či zvýšiť transparentnosť procesov.⁴ Prináša však aj pochybnosti o správnosti definície. V tomto kontexte však súčasne hrozí prehĺbenie digitálnej priepasti medzi zamestnancami s rôznou mierou digitálnej gramotnosti alebo prístupu k technológiám.⁵ Rovnako tak algoritmické rozhodovanie môže viesť k nepriamym formám diskriminácie na základe veku, pohlavia či zdravotného postihnutia, pokiaľ nie je dostatočne transparentné a kontrolovateľné. Skúmanie týchto fenoménov je preto kľúčové pre nastavenie rovnováhy medzi inovatívnymi prístupmi a ochranou základných práv zamestnancov.

Medzi priority európskeho sociálneho modelu (zakotveného najmä v kapitolách IV., IX, a X. Zmluvy o fungovaní EÚ a v základných slobodách EÚ) patrí „podpora a zvyšovanie zamestnanosti, podpora vzdelávania, ochrana práv pracovníkov voľne sa pohybujúcich v rámci EÚ, zlepšovanie pracovného prostredia vrátane BOZP, zaistenie rovnosti a rovnakého zaobchádzania medzi mužmi a ženami, boj proti sociálnemu vylúčeniu (chudobe) a modernizácia sociálnych systémov.“⁶ Európska únia týmto akcentuje potrebu podporovať inovatívne formy práce, avšak také, ktoré zaručujú kvalitné pracovné podmienky.

Hoci technologický vývoj býva asociovaný so zmenami ktoré majú tendenciu byť interpretované ako kvalitatívne pozitívne, pokladáme za nevyhnutné venovať pozornosť aj dôsledkom a potenciálnym rizikám, ktoré sú spojené s digitalizáciou vo sfére ľudskej práce.

⁴ LI, Yuanzuan et al.: The Impact of Digital Economy on Flexible Employment: The Mediating Role of Laborer Perceptions. In: Sage Open, Vol.15, No. 1 (2025), s.1-19. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/21582440251327017>>, s. 1-2.

⁵ DALESSANDRO, Cristen - LOVELL, Alexander: The Digital Dignity Divide: Work, Technology, and Well-Being Outcomes Among U.S. Employees. In: Social Currents, Vol. 12, 4 (2025), s.370-388. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/23294965251356407>>, s.372.

⁶ LACKO, Miloš (ed.) Európsky sociálny model a jeho úlohy. Trnava: Právnická fakulta Trnavskej univerzity, 2020, s. 7.

Teoretické a právne východiská

Ochrana ľudskej dôstojnosti patrí medzi fundamentálne princípy moderného právneho štátu. Po druhej svetovej vojne sa dôstojnosť stala ústavným i medzinárodnoprávnym štandardom.⁷ „Dôstojnosť sa stáva bežnou súčasťou právnych textov zabezpečujúcich ochranu ľudských práv v mnohých jurisdikciách a často sa používa v súdnych rozhodnutiach národných súdov.“⁸ Všeobecná deklarácia ľudských práv z roku 1948 v čl. 1 zakotvuje, že „všetci ľudia sa rodia slobodní a rovní v dôstojnosti a právach“. Tento princíp sa premieta aj do čl. 1 Charty základných práv Európskej únie, ktorý dôstojnosť človeka označuje za „nedotknuteľnú“ a požaduje jej rešpektovanie a ochranu. Dôstojnosť ako právna a morálna kategória tak nadobúda význam aj v súvislosti s digitalizáciou práce, ktorá môže byť posilniť inklúziu a rovnosť príležitostí, alebo naopak spôsobiť novú formu vylúčenia.

Pracovné právo má osobitné poslanie vyvažovať nerovné postavenie účastníkov pracovnoprávneho vzťahu, pričom osobitnú ochranu poskytuje slabšiemu subjektu, zamestnancovi. Do tohto rámca prirodzene zapadá aj problematika tzv. digitálnej dôstojnosti, teda uplatňovania základného práva na dôstojnosť v kontexte digitalizovaného pracovného prostredia. Digitálna dôstojnosť predstavuje koncept, ktorý spája tradičné chápanie ľudskej dôstojnosti s výzvami, ktoré prináša technologický rozvoj, predovšetkým v oblasti prístupu k technológiám, digitálnej gramotnosti a férového algoritmického riadenia.

Na európskej úrovni sa uplatňuje rámec práva na rovnaké zaobchádzanie a zákazu diskriminácie, vyjadrený v smernici Rady 2000/78/ES, ktorá zavádza všeobecný rámec pre rovnaké zaobchádzanie v zamestnaní a povolani. V slovenskom právnom prostredí je tento rámec transponovaný najmä do zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov (ďalej len „Zákonník práce“) a zákona č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Antidiskriminačný zákon“). Tieto normy zakazujú priamu i nepriamu diskrimináciu z dôvodu veku, pohlavia, zdravotného postihnutia či iných charakteristík, čo má zásadný význam aj pri posudzovaní digitálnej nerovnosti. Tieto právne predpisy, kľúčové v oblasti boja s diskrimináciou vo svete práce, dopĺňajú na

⁷ PARDO-VERGARA, María: Dignity as Humanness: A Pathway to Understand the Place of Dignity as a Constitutional End. In: *International Journal of Law in Context*, Cambridge University Press, Vol. 21, no. 3 (2025), pp. 514–32. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1017/S1744552325100025>>, s.514

⁸ McCRUDDEN, Christopher: Human Dignity and Judicial Interpretation of Human Rights. In: *European Journal of International Law*, vol. 19, no. 4 (2008), pp. 655–724. [cit. 2025-11-18] Dostupné na internete: <<https://www.ejil.org/pdfs/19/4/1658.pdf>>, s.656.

úrovni EU ďalšie nástroje: všeobecné nariadenie o ochrane údajov (GDPR)⁹ a zákon o umelej inteligencii (AI Act)¹⁰.

Autori Daňko a Poruban konštatujú vo vzťahu ku GDPR a AI act, že „v súčasnej aplikačnej praxi existujú medzery. Napriek ambicióznemu regulačnému rámcu chýbajú konkrétne štandardy pre kontrolu algoritmických rozhodnutí v pracovnom prostredí, čo môže viesť k asymetrii moci medzi zamestnávateľmi a zamestnancami“ a zdôrazňujú, že hoci „právne rámce EÚ poskytujú síce základnú ochranu, no aplikácia týchto noriem do praxe si vyžaduje pravidelný monitoring a prispôsobovanie legislatívy dynamicky sa meniacim technológiám.“¹¹

Diskriminácia a strata dôstojnosti v kontexte digitalizácie

Rozdiely medzi tými, ktorí môžu plne využívať digitálne príležitosti, a tými, ktorí ich nemôžu, vytvárajú sociálne nerovnosti – jav známy ako digitálna priepasť.¹²

Digitalizácia vytvára nové riziká diskriminácie v pracovnom práve, ktoré nemožno redukovať iba na otázku prístupu jednotlivca k internetu alebo zariadeniam. Súčasné chápanie problému sa rozširuje o výrazné rozdiely v digitálnych zručnostiach. Podstatným problémom sa stáva digitálna gramotnosť, ktorá sa nerovnomerne rozdeľuje podľa veku, sociálneho statusu či zdravotných možností. Starší zamestnanci často nedisponujú dostatočnými digitálnymi zručnosťami a zároveň nemajú už ani mentálne či kognitívne kapacity na úplné vyrovnanie sa mladším generáciám v používaní moderných technológií. Obavy z nových technológií môžu ohroziť pocit dôstojnosti pracovníkov na pracovisku.¹³

Najzraniteľnejšou skupinou je vek 55 – 64 rokov, a to najmä z dvoch dôvodov:

- a) počas formálneho vzdelávania nezískali potrebné digitálne kompetencie,

⁹ Nariadenie Európskeho Parlamentu a Rady 2016/679 z 27 apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES Ú. v. EÚ L 119, 4.5.2016, pp. 1–88.

¹⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá pre umelú inteligenciu a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (zákon o umelej inteligencii, AI Act). Ú. v. EÚ L, 2024/1689, 12.7.2024.

¹¹ DAŇKO, Martin - PORUBAN, Andrej: Práva a povinnosti zamestnancov v Akte o umelej inteligencii, s.16.

¹² BARTIKOWSKI, Boris et al.: The Type-of-Internet-Access Digital Divide and the Well-being of Ethnic Minority and Majority Consumers: A Multi-Country Investigation. In: Journal of Business Research, Vol. 82, January 2018, s.373–380. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1016/j.jbusres.2017.05.033>>, s.373 - 374.

¹³ DALESSANDRO, Cristen - LOVELL, Alexander, s. 373.

- b) význam týchto zručností sa stal prioritou pre zamestnávateľov a politikov až v posledných rokoch.¹⁴

Zatiaľ čo adolescenti vo všeobecnosti vnímajú digitálne technológie ako prirodzenú súčasť každodenného života a sebarozvoja, učenia sa a získavania nových kompetencií a „digitálny svet navyše slúži pre dospelávajúcich ako predĺženie offline sveta“,“¹⁵ starší pracovníci vo veku 50+ často čelia spoločenským aj psychologickým bariéram v osvojovaní digitálnych zručností.¹⁶

Táto situácia môže viesť k tzv. digitálnej diskriminácii, ktorá má formu nepriamych prekážok prístupu k zamestnaniu alebo k jeho udržaniu. Ak je výkon práce čoraz viac podmienený digitálnymi kompetenciami, hrozí, že určitá časť populácie bude z trhu práce vytláčaná nie pre nedostatok odbornej kvalifikácie, ale pre nedostatok digitálnych schopností, čo predstavuje novú formu sociálneho vylúčenia.

„V praktickom živote nepochopenie problematiky diskriminácie na strane zamestnávateľov môže viesť k ich neochote zamestnávať uchádzačov, ktorí sa javia ako potenciálne „problémoví“, resp. nezodpovedajú spoločenským stereotypom o „ideálnom“ zamestnancovi.“¹⁷

Strata, resp. absencia digitálnej kompetencie sa pritom neprejavuje iba v rovine pracovnoprávnej, ale aj v rovine psychologickej a hodnotovej. Starší zamestnanci môžu mať pocit zníženej sebaúcty a dôstojnosti, keď sú v pracovnom prostredí konfrontovaní s technológiami, ktoré nedokážu ovládať v rovnakej miere ako ich mladší kolegovia. Tento fenomén je možné chápať ako stratu pracovnej dôstojnosti, ktorá sa stáva nepriamejším, ale o to závažnejším dôsledkom digitalizácie.¹⁸

Zároveň je výskumne potvrdené, že integrácia a podpora kvalifikovaných starších pracovníkov ponúka veľký potenciál pre hospodárstvo i spoločnosť v kontexte starnúcej populácie. „Stratégia nahrádzania starších pracovníkov kvalifikovanými

¹⁴ BALYTSKA, Mariia, et al.: Unlocking the Potential Under Ageing Labor Force and Digitalization Challenges. In: 2023 IEEE 4th KhPI Week on Advanced Technology (KhPI Week 2023) – Conference Proceedings. Kharkiv, Ukraine, 2023, s.1-2.

¹⁵ BITTO URBANOVA, Laura et al: Technology supports me: perceptions of the benefits of digital technology in adolescents. In Frontiers in Psychology, Vol. 13, Art.No. 970395, 30 Jan. 2023, [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.3389/fpsyg.2022.970395>>, s.2.

¹⁶ ČAPLÁNOVÁ, Anetta – DARMO, Ľubomír: Exploration into the Digital Skill Development Needs and Challenges of Older Workers (Case Study of Slovak Ageing Work Force).In: Knowledge Management in Organisations, Springer CCIS Series, vol. 2562, 2025, pp. 104–122. [cit. 2025-11-18] Dostupné na internete: <https://link.springer.com/chapter/10.1007/978-3-031-95898-4_8>, s.104.

¹⁷ CAPÍKOVÁ, Silvia: Rovnaké zaobchádzanie a zákaz diskriminácie. In: NOVÁKOVÁ, M. a kol.: Pracovné právo 1. Bratislava, Wolters Kluwer, 2024, s.66.

¹⁸ DALESSANDRO, Cristen - LOVELL, Alexander, s. 373.

mladšími pracovníkmi, ktorá v hospodárstve prevládala a prevláda, nie je funkčným modelom pre budúcnosť práce, ak priemerný vek pracovníkov neustále rastie.¹⁹ Mnohé súčasné štúdie odporúčajú komplexnejšie politiky zamerané na tréning a podporu starších pracovníkov (50+), aby sa predišlo ich vylúčeniu z trhu práce, ktorý súvisí s ich objektívne nižšou úrovňou digitálnych zručností v tejto vekovej skupine.²⁰

Faktory podmieňajúce nedostatok digitálnych kompetencií zamestnancov 50+

Digitálne kompetencie predstavujú rozhodujúci predpoklad uplatniteľnosti jednotlivcov na súčasnom trhu práce, ktorý je čoraz výraznejšie ovplyvnený technologickým pokrokom a procesmi digitalizácie. Podľa Van Laar a kol., digitálne zručnosti pre 21. storočia sú nie len technické zručnosti, ale tiež práca s informáciami, komunikácia, spolupráca, kreativita, kritické myslenie a riešenie problémov.²¹ Zamestnanci vo vekovej kategórii 50+ sú v tomto kontexte považovaní za rizikovú skupinu, keďže u nich možno identifikovať viacero faktorov podmieňujúcich nižšiu úroveň digitálnych zručností a tým aj zvýšené riziko digitálneho znevýhodnenia či diskriminácie. Tento problém reflektujú aj európske stratégie, ktoré zdôrazňujú potrebu celoživotného vzdelávania a inkluzívnej digitálnej transformácie.

Jedným zo základných faktorov je nedostatočná príležitosť k systematickému rozvoju digitálnych kompetencií v predchádzajúcich fázach profesionálnej dráhy. Mnohí zamestnanci 50+ vstupovali na trh práce v období, keď digitálne technológie neboli súčasťou každodennej pracovnej praxe. Digitálna gramotnosť preto nebola zahrnutá do obsahu základného ani odborného vzdelávania, čo sa dnes prejavuje deficitom v používaní moderných pracovných nástrojov. Európska komisia na tento problém poukazuje v *Digital Education Action Plan (2021–2027)*, ktorý zdôrazňuje potrebu znižovania medzigeneračných rozdielov v digitálnych zručnostiach.²²

¹⁹ KLUGE, Johanna - HILDEBRANDT, Julian - ZIEFLE, Martina: The Golden Age of Silver Workers?. s.520 - 532. In Zhou, J., Salvendy, G. (eds.). Human Aspects of IT for the Aged Population. Social Media, Games and Assistive Environments. HCII 2019. Lecture Notes in Computer Science, vol 11593. Springer, Cham. [cit. 2025-11-18] Dostupné na internete: <https://doi.org/10.1007/978-3-030-22015-0_40>, s.521.

²⁰ LAKOMÝ, Martin – ŠÁCHA, Jakub – VYSTRČIL, Filip: Attitudes of European Older Workers Towards Digitalisation from the Ecological Perspective. In: Information, Communication & Society, vol. 28, no. 5 (2025), p. 1–20. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1080/1369118X.2025.2472944>> s. 3-4.

²¹ 30. VAN LAAR, Ester – VAN DEURSEN, Alexander J. A. M. – VAN DIJK, Jan A. G. M. – DE HAAN, Jos: Determinants of 21st-Century Skills and 21st-Century Digital Skills for Workers: A Systematic Literature Review. In SAGE Open, Vol. 10, No. 1 (2020), pp. 1–14. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/2158244019900176>> s.1.

²² EUROPEAN COMMISSION. *Akčný plán digitálneho vzdelávania 2021–2027: Prispôsobenie vzdelávania a odbornej prípravy digitálnemu veku*. 30 Sept. 2020, COM(2020) 624 final. EUR-Lex. Accessed 18 Sept. 2025. <https://eur-lex.europa.eu>

Ďalším významným faktorom je psychologická bariéra spojená s adaptáciou na nové technológie. Starší zamestnanci môžu pociťovať neistotu, nedôveru či obavy zo zlyhania pri práci s digitálnymi nástrojmi, čo vedie k zníženej motivácii absolvovať rekvalifikácie. Tento jav je často podporovaný vnímaním vekovej stigmatizácie, ktorá oslabuje sebadôveru a posilňuje pocit marginalizácie. V tejto súvislosti Európsky pilier sociálnych práv (2017) stanovuje zásadu rovnakých príležitostí a prístupu k trhu práce bez ohľadu na vek, čím implicitne podporuje aj aktívne opatrenia proti tzv. digitálnemu ageizmu.²³

Významnú úlohu zohrávajú aj štrukturálne faktory spojené s pracovným prostredím. V mnohých odvetviach, najmä v priemyselnej výrobe, doprave alebo manuálne orientovaných službách, dochádzalo k digitalizácii pomalšie než v sektore informačných technológií. Zamestnanci staršej vekovej kategórie tak mali v priebehu svojej kariéry obmedzený prístup k inováciám, čo znižovalo ich schopnosť flexibilne reagovať na nové požiadavky.

Dôležitým faktorom je aj nedostatočná dostupnosť a inkluzívnosť vzdelávacích a rekvalifikačných programov. Kurzy zamerané na digitálne kompetencie nebývajú prispôsobené potrebám starších účastníkov. Navyše, absentuje systém finančnej a organizačnej podpory, ktorý by umožnil zamestnancom 50+ aktívne sa zapájať do celoživotného vzdelávania popri pracovných a rodinných povinnostiach. Iniciatíva *Digital Skills and Jobs Coalition* preto odporúča cielene podporovať školenia pre starších pracovníkov a vytvárať partnerstvá medzi štátom, zamestnávateľmi a občianskou spoločnosťou.²⁴

Opomenúť nemožno ani sociálno-ekonomické faktory, ktoré priamo ovplyvňujú prístup k digitálnym technológiám. Starší zamestnanci môžu disponovať nižším príjmom, čo obmedzuje ich schopnosť investovať do moderných zariadení či kvalitného internetového pripojenia. Regionálne rozdiely, najmä medzi mestským a vidieckym prostredím, zároveň prehľbujú nerovný prístup k technológiám.

V neposlednom rade treba uviesť faktor zdravotného stavu, keďže zhoršený zrak, motorické či kognitívne schopnosti môžu limitovať efektívne používanie digitálnych nástrojov.

Zhrnutím možno konštatovať, že nedostatok digitálnych kompetencií u zamestnancov vo veku 50+ je výsledkom kombinácie historických, psychologických, štrukturálnych, sociálno-ekonomických a zdravotných faktorov. Ak má byť táto veková skupina plnohodnotne integrovaná do digitálne transformovaného trhu práce, je nevyhnutné realizovať komplexné opatrenia reflektujúce tieto špecifické

²³ EUROPEAN COMMISSION. Vytvorenie Európskeho piliera sociálnych práv. 26 Apr. 2017, COM(2017) 250 final. *EUR-Lex*. Accessed 18 Sept. 2025. <https://eur-lex.europa.eu>

²⁴ EU DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY: Digital Skills and Jobs Coalition. Accessed 18 Sept. 2025. <https://www.digital-skills-jobs.europa.eu>

bariéry. Európsky rámec digitálnej politiky tak ponúka nielen normatívny základ, ale aj praktické nástroje na posilňovanie digitálnej dôstojnosti starších pracovníkov a predchádzanie ich marginalizácii v pracovnoprávných vzťahoch.

Podporné opatrenia

Koncept digitálnej dôstojnosti predstavuje v podmienkach dynamickej digitalizácie pracovnoprávných vzťahov nevyhnutnú súčasť ochrany zamestnancov. Digitálne nástroje, s ktorými zamestnanci na rôznych pracovných pozíciách pracujú, sebe vlastným spôsobom zbierajú aj údaje o zamestnancoch. Digitálne nástroje, ktoré sa využívajú pri výbere, hodnotení či prepúšťaní pracovníkov, prinášajú významné výhody v oblasti efektivity, no súčasne vytvárajú riziko vzniku nových foriem diskriminácie a nerovností. Prevencia digitálnej diskriminácie preto vyžaduje implementáciu podporných opatrení na legislatívnej, inštitucionálnej aj aplikačnej úrovni.

Medzi riziká ktoré potenciálne ohrozujú dôstojnosť zamestnanca je penetrácia do súkromia zamestnanca, zhromažďovanie a spôsob spracúvania osobných údajov súvisiacich s vykonávaním pracovných činností v digitálnom prostredí.

V prípade uchádzačov o zamestnanie, „ustanovenie §62 ods.2 a 3. zákona o službách zamestnanosti špecifikuje povinnosti zamestnávateľov realizovať nábor a selekciu uchádzačov založenú na chránených dôvodoch. Kritériá na výber zamestnanca musia zaručovať rovnosť príležitostí pre všetkých občanov.“²⁵

Spracovanie osobných údajov uchádzačov o zamestnanie alebo zamestnancov v digitalizovanom pracovnom prostredí, rovnako aj prostredníctvom umelej inteligencie (či už ide o jednotlivý model alebo celý systém AI), musí byť v súlade s požiadavkami Nariadenia GDPR, najmä pokiaľ ide o zákonnosť, transparentnosť a ochranu práv dotknutých osôb. Prevádzkovateľ je povinný si sám správne určiť právny základ, na základe ktorého spracúva osobné údaje prostredníctvom umelej inteligencie (AI). Nariadenie GDPR upravuje tieto právne základy v článku 6.

Spracúvanie osobných údajov dotknutých osôb v zmysle bodu 23 preambuly GDPR sa riadi týmto nariadením aj keď sa týka sledovania ich správania. Na určenie toho, či spracovateľskú činnosť možno považovať za „sledovanie správania“ dotknutej osoby, by sa malo zistiť, či sú fyzické osoby sledované na internete vrátane prípadného následného využitia technologických riešení spracúvania osobných údajov, ktoré spočívajú buď v profilovaní fyzickej osoby na účely prijatia rozhodnutia týkajúceho sa tejto osoby alebo na účely analýzy či predvídania osobných preferencií, správania a postojov tejto osoby. Vzťahuje sa teda aj na zamestnancov alebo budúcich zamestnancov.

²⁵ CAPÍKOVÁ, Silvia: Rovnaké zaobchádzanie a zákaz diskriminácie. In: NOVÁKOVÁ, M. a kol.: Pracovné právo 1. Bratislava, Wolters Kluwer, 2024, s.70.

Navyše, článok 22 Nariadenia GDPR v ods.1 výslovne ustanovuje, že „Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.“

Článok 22 teda explicitne stanovuje zákaz, aby o človeku bolo rozhodnuté výlučne automatizovane, ak má také rozhodnutie právne účinky (napr. prijatie alebo zamietnutie prijatia do zamestnania, povýšenie, prepustenie, zníženie platu) alebo ho významne ovplyvňuje (napr. profilovanie výkonnosti, hodnotenie správania, prideľovanie úloh podľa algoritmu). Tento zákaz nie je absolútny — explicitne čl. 22 ods. 2 zakotvuje 3 výnimky:

- a) nevyhnutnosť na uzavretie alebo plnenie zmluvy,
- b) povolenie právom EÚ alebo členského štátu,
- c) výslovný súhlas dotknutej osoby.

Poskytovateľ je však v zmysle č. 22 ods. 3 GDPR povinný zabezpečiť v prípade prvej a tretej výnimky ľudský dohľad, možnosť vyjadriť sa a možnosť napadnúť rozhodnutie. Dalo by sa povedať, ako upozornili M. Veale a L. Edwardsová, že nastal v právnej regulácii posun od „práva byť informovaný“ ku „právu na lepšie rozhodnutie“²⁶ a tiež „právu na vysvetlenie.“²⁷ Uvedení autori tiež upozorňujú na aplikačné problémy článku 22, nakoľko text článku diferencuje či rozhodnutie má nie len „právne účinky“ ale prípadne aj „podobne významné“ účinky: „Zatiaľ čo právne účinky sú pomerne jasne obmedzené na prípady, keď sa zmení právny status alebo vzniknú právne povinnosti (napr. posúdenie imigračného statusu; overenie právnej zmluvy), „významné“ účinky sú oveľa nejasnejšie.“

Nazdávame sa, že kritérium „významného účinku“ je pomerne významne reflektované v literatúre s v súvislosti s ochranou spotrebiteľov a ovplyvňovaní spotrebiteľského správania, avšak implikácie v pracovnoprávnej oblasti by si zaslúžilo *pro futuro* intenzívnejší bádateľský záujem ohľadom interpretačných a aplikačných nejasností.

Bude potrebné tiež jasnejšie diferencovať rozhranie zodpovednosti medzi zamestnávateľským subjektom (používateľom) a poskytovateľom digitálneho nástroja, najmä v kontexte novoprijatého nariadenia AI Act pri vysokorizikových systémoch, ale aj pri iných typoch digitálnych resp. automatizovaných nástrojov a softvérových riešení používaných pri riadení zamestnancov.

Jedným z najväčších rizík algoritmickeho rozhodovania je princíp „bias in, bias out“, ktorý znamená, že ak sú vstupné dáta zaujaté, aj výstupy systému budú zaujaté.

²⁶ VEALE, Michael - EDWARDS, Lilien: Clarity, Surprises, and Further Questions in the GDPR's Approach to Automated Decision-Making. In Computer Law & Security Review, Vol. 34, No. 2 (2018), s.399.

²⁷ Ibid., s.402.

V kontexte pracovného práva to znamená, že ak algoritmus bol/je trénovaný na historických dátach, kde boli starší uchádzači systematicky odmietaní, algoritmus sa naučí tento vzorec a bude ho reprodukovat' – hoci explicitne nepracuje s kritériom veku. Takáto nepriama diskriminácia je obzvlášť nebezpečná, pretože pôsobí technicky neutrálne, no má významný účinok na prístup k zamestnaniu.

V kontexte článku 22 GDPR a zásady rovnakého zaobchádzania (čl. 21 Charty základných práv EÚ, § 13 Zákonníka práce SR, Zákon č. 365/2004 Z. z. o rovnakom zaobchádzaní) možno identifikovať viacero typov diskriminačných praktík, ktoré algoritmické systémy môžu nevedomky alebo systémovo reprodukovat'.

1. Priame diskriminačné praktiky môžeme chápať ako situácie, keď algoritmus priamo používa zakázaný diskriminačný znak (napr. pohlavie, vek, etnický pôvod, zdravotný stav, atď.) ako vstupný parameter rozhodovania. Príkladom môže byť Automatizované triedenie uchádzačov o zamestnanie, kedy AI model vyhodnocuje kandidátov a znižuje skóre žien, pretože historické údaje ukazovali, že manažérske pozície zastávali prevažne muži (tzv. gender bias). Alebo ak systém odmieta kandidátov nad 50 rokov, pretože v minulosti mali kratšiu dĺžku pracovného pomeru (diskriminácia na základe veku). Tieto príklady predstavujú porušenie článku 22 GDPR (výlučne automatizované rozhodovanie s právnym účinkom) a zároveň porušenie antidiskriminačných predpisov.

2. Nepriame diskriminačné praktiky vznikajú, keď algoritmus nepoužíva diskriminačný znak priamo, ale využíva korelujúce premenné, ktoré spôsobujú nerovnosť výsledku pre určitú skupinu. Príkladom môže byť automatické hodnotenie výkonnosti: algoritmus penalizuje zamestnancov, ktorí častejšie než iní pracujú z domu, alebo im prideluje menej atraktívne zmeny. Automatické odmeňovanie (pridelovanie bonusov) podľa „objektívnych“ metrík (napr. počet pripojení, aktivít, dĺžka pripojenia) – znevýhodňuje osoby so zdravotnými obmedzeniami alebo pomalším pracovným tempom. Môže sa stať, že model automatizovaného rozhodovania označí za „rizikových“ zamestnancov bez ľudského overenia. Diskriminácia sa môže systematicky ukrývať v dátach na ktorých bol algoritmus trénovaný, alebo v modeli jeho fungovania.

Tieto formy sa môžu prejavujú v rôznych fázach pracovného procesu, od predzmluvných vzťahov cez organizáciu práce, odmeňovanie, organizáciu práce, zamestnanecké benefity, bonusy a malusy, kariérny rast, až po ukončenie pracovného pomeru.

Pri posudzovaní diskriminácie v zamestnaní na základe veku je podľa judikatúry Súdneho dvora Európskej únie (napr. C-144/04 Mangold, C-555/07 Küçükdeveci, C-

159/10 Fuchs²⁸⁾ potrebné aplikovať metodológiu testu proporcionality. Proporcionalita sa posudzuje individuálne. Rozdielne zaobchádzanie na základe veku môže byť prípustné len vtedy, ak sleduje legitímny cieľ sociálnej politiky, je primerané, nevyhnutné a spôsobilé dosiahnuť tento cieľ. Ak opatrenie zamestnávateľa nie je objektívne a primerane odôvodnené, musí súd konštatovať porušenie zásady rovnakého zaobchádzania, priznať primerané zadostučinenie alebo náhradu škody, a prípadne neuplatniť vnútroštátne ustanovenie, ktoré je v rozpore s právom EÚ (priame uplatnenie Charty EÚ a smernice 2000/78/ES).

Z hľadiska zodpovednosti za porušenie povinností, článok 22 GDPR treba chápať ako ochranu pred plne automatizovanými rozhodnutiami bez ľudského zásahu, ktoré spôsobujú právne alebo zásadné účinky, pričom zamestnávateľ (používateľ) je primárne zodpovedný za to, aby systém bol len pomocným nástrojom a neporušoval práva zamestnanca. Poskytovateľ digitálneho nástroja zodpovedá za technickú bezpečnosť, transparentnosť algoritmov a spoluprácu pri dodržiavaní GDPR.

Pre ochranu digitálnej dôstojnosti je preto významné explicitné zakotvenie (a následne dodržiavanie) práva zamestnanca na informácie o využívaní algoritmických systémov. Právna úprava na národnej úrovni by mala reálne zaručovať, že každý zamestnanec bude mať prístup k informáciám o tom, akým spôsobom a v akom rozsahu sa algoritmické nástroje podieľajú na rozhodnutiach o jeho pracovnom statuse. Transparentnosť v tejto oblasti je základným predpokladom pre uplatňovanie zásady rovnakého zaobchádzania a predchádzanie diskriminačným praktikám.

Ďalším opatrením je zavedenie povinnosti zamestnávateľa zabezpečiť ľudský dohľad nad automatizovaným rozhodovaním. Automatizované systémy môžu reprodukovать predsudky alebo vychádzať z nepresných vstupných dát, čo má priamy dosah na zamestnanecké práva. Prítomnosť človeka pri rozhodovaní alebo pri kontrole výsledkov algoritmu pôsobí ako korekčný mechanizmus, ktorý zvyšuje spravodlivosť a legitímnosť rozhodovacieho procesu.

Osobitne relevantné je aj rozšírenie antidiskriminačnej legislatívy o nový diskriminačný dôvod, a to digitálny status alebo digitálne znevýhodnenie. Tento

²⁸⁾ Súdny dvor Európskej únie. Rozsudok z 22. novembra 2005, Werner Mangold proti Rüdiger Helm, vec C-144/04, EU:C:2005:709 [online]. Luxembourg : CURIA, 2005 [cit. 2025-09-09]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=65973&doclang=EN>>

Súdny dvor Európskej únie. Rozsudok z 19. januára 2010, Seda Küçükdeveci proti Swedex GmbH & Co. KG, vec C-555/07, EU:C:2010:21 [online]. Luxembourg : CURIA, 2010 [cit. 2025-09-09]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=72619&doclang=EN>>

Súdny dvor Európskej únie. Rozsudok z 21. júla 2011, Gerhard Fuchs a Peter Köhler proti Land Hessen, spojené veci C-159/10 a C-160/10, EU:C:2011:508 [online]. Luxembourg : CURIA, 2011 [cit. 2025-09-09]. Dostupné na internete:

<<https://curia.europa.eu/juris/showPdf.jsf?docid=130450&doclang=EN>>

dôvod by reflektoval meniace sa podmienky pracovného trhu, kde digitálna gramotnosť a prístup k moderným technológiám determinujú zamestnateľnosť jednotlivcov. Uznatie digitálneho znevýhodnenia ako osobitného diskriminačného dôvodu by rozšírilo ochranu skupín ohrozených exklúziou.

Ďalšou oblasťou je úprava povinností zamestnávateľov vo vzťahu k primeraným úpravám digitálnych nástrojov pre osoby so zdravotným postihnutím. Princíp primeraných úprav, známy z európskeho antidiskriminačného práva, sa musí aplikovať aj v digitálnom prostredí. Zamestnávatelia by mali zabezpečiť dostupnosť a prístupnosť pracovných softvérov a systémov tak, aby ich mohli využívať aj osoby so špecifickými potrebami.

Napokon, významným prvkom politiky prevencie digitálnej diskriminácie sú cieľené aktívne opatrenia trhu práce, zamerané na zvyšovanie digitálnych zručností ohrozených skupín a podporu ich uplatnenia na trhu práce. Okrem rekvalifikačných programov ide aj o vytváranie finančných stimulov pre zamestnávateľov, ktorí sa rozhodnú zamestnávať digitálne znevýhodnených uchádzačov, čím sa podporí inkluzívny charakter trhu práce.

Zavedenie uvedených opatrení by umožnilo nielen reagovať na aktuálne riziká spojené s digitalizáciou pracovného prostredia, ale aj posilniť normatívny rámec ochrany ľudskej dôstojnosti v digitálnom veku. Digitálna dôstojnosť tak prestáva byť len etickým ideálom, ale nadobúda charakter právneho princípu, ktorý vyžaduje systematickú ochranu v rámci pracovnoprávnych vzťahov.

Rekvalifikácia

Teória a aplikačná prax ponúka viacero nástrojov na prekonávanie digitálnej diskriminácie. Jedným z nich je rekvalifikácia a tiež celoživotné vzdelávanie. Demografické starnutie populácie prináša nielen výzvy pre zdravotný systém a sociálne zabezpečenie, ale aj tlak na udržanie starších ľudí na trhu práce.²⁹ Pracovné právo preto musí byť doplnené politikami vzdelávania a aktívneho trhu práce, ktoré umožnia zraniteľným osobám získať aspoň základnú digitálnu gramotnosť.³⁰

Moderné vzdelávacie platformy, vrátane tých, ktoré využívajú umelú inteligenciu, môžu prispieť k prispôsobeniu výučby individuálnym potrebám starších zamestnancov. Vzniká však otázka, či sú tieto nástroje prístupné a zrozumiteľné práve tým, ktorí ich najviac potrebujú. Úlohou štátu i zamestnávateľov je preto

²⁹ BALÁŽ, V. a kol.: Pozor na nerovnosti kvôli veku. Bratislava: Implementačná agentúra Ministerstva práce, sociálnych vecí a rodiny SR. 2023. Accessed 18 Sept. 2025. https://eurofondy.praca.gov.sk/wp-content/uploads/2023/06/Pozor-na-nerovnosti-kvoli-veku-final_AV.pdf, s.170.

³⁰ NIKOLAEVA, Svetlana G. – YANDARBAEVA, Luiza A.: On the Problem of Social and Labor Adaptation of the Age Population in Modern Conditions. s.519-528 In: Anna Rumyantseva & Hod Anyigba & Elena Sintsova & Natalia V. Vasilenko (ed.), Finance, Economics, and Industry for Sustainable Development. Cham, Springer. 2024, s.519.

zabezpečiť inkluzívne vzdelávacie programy, ktoré rešpektujú špecifiká starších zamestnancov, ich tempo učenia a kognitívne obmedzenia.

Národný projekt

Ústredie práce sociálnych vecí a rodiny spustilo národný projekt „Zručnosti pre trh práce“,³¹ ktorý je zameraný na poskytovanie nenávratnej finančnej podpory na vzdelávanie:

- a) nezamestnaných a tiež
- b) zamestnaných záujemcov.

V rámci projektu sú ponúkané online i prezenčné kurzy, ktoré sú zamerané na zlepšenie zručností v oblastiach ako sú IT, marketing, grafika a digitálny dizajn. Cieľom nového národného projektu je podporiť uchádzačov o zamestnanie v snahe nájsť si prácu prostredníctvom rekvalifikácie. Realizácia národného projektu je plánovaná do marca 2026 a je na ňu vyčlenených 42 249 963,50 eur z európskych zdrojov a štátneho rozpočtu Slovenskej republiky.³²

AnalYZovali sme celý rad kurzov a pre ilustráciu uvádzame kurz „IT architekt“, ktorý trvá 6 dní, a to v čase od 9:00 do 15:00 hod. Na základe tohto kurzu sa jeho účastníci uplatnia v oboroch, kde sa vyžaduje komplexné ovládanie programu AutoCad. U záujemcov o kurz sa nepredpokladajú žiadne vstupné vedomosti.

Možno konštatovať, že predmetný kurz má charakter krátko odborného školenia, nie plnohodnotnej rekvalifikácie do praxe.

Je „rýchle zaučenie“ realistické pre uchádzačov 50+? Starší zamestnanci alebo uchádzači o zamestnanie potrebujú prispôsobený dizajn vzdelávania s pomalším tempom a tréning s mentorstvom a dlhším horizontom.

Návrhy „de lege ferenda“

Vo všeobecnosti platí, že „moderné, inštrumentálne právo sa používa s úmyslom presadenia sociálnej zmeny a eliminácie nežiadúcich vzorcov konania v spoločnosti, resp. ich nahradenia inými vzorcami.“³³ Je potrebné, aby právna úprava dokázala regulovať technologický vývoj tak, aby nedochádzalo k digitálnej diskriminácii a ďalším nežiadúcim javom vo sfére zamestnanosti.

³¹ Ústredie práce, sociálnych vecí a rodiny: Národný projekt Zručnosti pre trh práce. ÚPSVR. Accessed 18 Sept. 2025. <https://www.upsvr.gov.sk>

³² Ministerstvo práce, sociálnych vecí a rodiny SR: Úrady práce, sociálnych vecí a rodiny podporia rozvoj zručností. MPSVR SR. Accessed 18 Sept. 2025. <https://www.employment.gov.sk>

³³ ČAPÍKOVÁ, Silvia: Medzi poriadkom a chaosom: právo v období post-komunistickej transformácie na Slovensku. In: Sociologický časopis / Czech Sociological Review, Vol. 41, No. 4 (2005), s. 617–640. <https://doi.org/10.13060/00380288.2005.41.4.06>, s.626.

Rozmach umelej inteligencie (AI) a algoritmických nástrojov v oblasti ľudských zdrojov prináša zásadné výzvy pre pracovnoprávne vzťahy. Tieto technológie sa čoraz viac uplatňujú pri náboře zamestnancov, hodnotení pracovného výkonu či pri rozhodovaní o skončení pracovného pomeru. Hoci umožňujú efektívnejšie spracovanie údajov a prediktívne analýzy, zároveň otvárajú priestor pre riziká spojené s ochranou základných práv zamestnancov, najmä práv na informácie, rovnaké zaobchádzanie a na ochranu pred diskrimináciou. Preto je vhodné uvažovať o systematických novelizáciách kľúčových pracovnoprávnych predpisov Slovenskej republiky.

a) Zákonník práce

Zákonník práce predstavuje základný kódex pracovného práva, ktorý by mal reflektovať technologické zmeny zasahujúce do vzťahu medzi zamestnávateľom a zamestnancom. S ohľadom na aplikačné skúsenosti v zahraničí a dynamicky sa vyvíjajúcu európsku reguláciu umelej inteligencie možno uvažovať o doplnení nasledujúcich inštitútov:

1. Právo na informácie o využívaní algoritmických/AI nástrojov
Zamestnancovi (resp. uchádzačovi o zamestnanie) by malo byť garantované právo na informácie o tom, či a v akom rozsahu sa v pracovnoprávnych procesoch využívajú algoritmické nástroje.
2. Ľudský dohľad a možnosť druhej inštalácie
V prípade, ak rozhodnutie so závažným vplyvom na pracovnoprávne postavenie zamestnanca bolo prijaté výlučne automatizovaným spôsobom, mal by mať zamestnanec právo požadovať jeho preskúmanie kompetentnou ľudskou autoritou. Takáto právna úprava by zabezpečila proporionalitu medzi efektívnosťou AI a ochranou ľudskej dôstojnosti a spravodlivosti v pracovnoprávnych vzťahoch.

b) Antidiskriminačný zákon

Antidiskriminačný zákon plní funkciu všeobecného právneho rámca pre rovnaké zaobchádzanie, pričom technologický rozvoj vyvoláva potrebu jeho doplnenia o nové kategórie ochrany:

1. Do katalógu chránených dôvodov diskriminácie by bolo vhodné doplniť pojem „digitálny status“ alebo „digitálne znevýhodnenie“. Ten by mal zahŕňať prípady, keď je jednotlivец znevýhodnený pre nízku digitálnu gramotnosť spôsobenú objektívnymi dôvodmi (vek, zdravotné postihnutie, sociálne prostredie) alebo pre nedostupnosť asistívnych technológií. Tým by sa vytvorila právna báza pre boj proti novej forme sociálnej exklúzie.
2. Explicitné zakotvenie algoritmickej diskriminácie (priamej aj nepriamej) by reflektovalo osobitné riziká spojené s využívaním AI. Priama algoritmická diskriminácia by spočívala v tom, že algoritmus pracuje s kritériami, ktoré sú explicitne diskriminačné, zatiaľ čo nepriama diskriminácia by vyplývala z

nastavenia parametrov, ktoré nepriamo vedú k vylúčeniu alebo znevýhodneniu určitej skupiny.

Navyše, v sporoch týkajúcich sa automatizovaného profilovania v zamestnaní by sa mohlo uplatniť uľahčené dôkazné bremeno, obdobne ako pri iných formách diskriminácie, keďže jednotlivci často nemajú prístup k technickým detailom fungovania algoritmu.

V sporoch týkajúcich sa digitálnej diskriminácie vrátane algoritmickej diskriminácie možno uplatniť aj štatistické dôkazy, napr. ak by išlo o rozdielnú úspešnosť uchádzačov podľa veku, pohlavia či zdravotného postihnutia resp. kombinácie týchto chránených dôvodov. V prípade C-415/10 Meister³⁴ Súdny dvor potvrdil, že nepriamy dôkaz diskriminácie môže stačiť na presun dôkazného bremena na zamestnávateľa. Prípád C-303/06 Coleman³⁵ rozšíril ochranu pred diskrimináciou aj na nepriamy dopad pracovných rozhodnutí, čo sa môže týkať aj hodnotenia výkonu.

V kontexte AI Act je potrebné špecifikovať zodpovednosť zamestnávateľa ako používateľa systému a poskytovateľa softvéru, najmä pri vysokorizikových systémoch, kde sa vyžaduje posúdenie vplyvov a audit.

Navrhované legislatívne zmeny by posilnili ochranu zamestnancov v digitálne transformovanom pracovnom prostredí. Zavedenie práva na informácie, práva na ľudské preskúmanie a povinnosti posudzovania vplyvov do Zákonníka práce by zodpovedalo základným princípom spravodlivého a dôstojného zamestnávania. Rozšírenie Antidiskriminačného zákona o digitálne znevýhodnenie a algoritmičnú diskrimináciu by reflektovalo nové sociálne a technologické výzvy a poskytlo by účinné prostriedky právnej ochrany. Takto koncipovaná právna úprava by Slovenskú republiku zaradila medzi štáty, ktoré aktívne reagujú na riziká spojené s automatizáciou pracovnoprávných procesov, a posilnila by dôveru verejnosti v reguláciu umelej inteligencie v oblasti práce.

Záver

Slovensko sa v DESI indexe digitálnych zručností umiestnilo na 23. mieste z 27 krajín EÚ, čo potvrdzuje systémový problém.³⁶ Digitalizácia práce nie je neutrálna

³⁴ Súdny dvor Európskej únie. Rozsudok z 19. apríla 2012, Galina Meister proti Speech Design Carrier Systems GmbH, vec C-415/10, EU:C:2012:217 [online]. Luxembourg : CURIA, 2012 [cit. 2025-09-09]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=148434&doclang=EN>>

³⁵ Súdny dvor Európskej únie. Rozsudok z 17. júla 2008, S. Coleman proti Attridge Law a Steve Law, vec C-303/06, EU:C:2008:415 [online]. Luxembourg : CURIA, 2008 [cit. 2025-09-09]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=67793&doclang=EN>>

³⁶ ČAPLÁNOVÁ, Anetta – DARMO, Ľubomír: Exploration into the Digital Skill Development Needs and Challenges of Older Workers (Case Study of Slovak Ageing Work Force). In: Knowledge Management in Organisations, Springer CCIS Series, vol. 2562, 2025, pp. 104–122. Accessed 18 Sept. 2025. Dostupné na: https://link.springer.com/chapter/10.1007/978-3-031-95898-4_8, s.104-105.

technická zmena, ale normatívna voľba, ktorá môže rovnako posilniť dôstojnosť zamestnancov, ako aj reprodukovat' nerovnosti. Analýza ukázala, že existujúci slovenský rámec ochrany, hoci východiskovo vychádza z ústavných princípov dôstojnosti, rovnosti a zákazu diskriminácie, nedokáže bez ďalšieho zachytiť osobitné riziká algoritmického riadenia a digitálnej nerovnosti. Kľúčom je preto presun od deklaratívnych zásad k vynútiteľným procesným, a to zárukám transparentnosti použitia algoritmov, povinnému ľudskému dohľadu, právo na „druhú inštanciu“ pri čisto automatizovaných rozhodnutiach a systematickému posudzovaniu vplyvov na práva zamestnancov.

De lege ferenda to znamená doplniť Zákonník práce o informačné povinnosti a mechanizmy kontroly algoritmických rozhodnutí, a Antidiskriminačný zákon o výslovné zakotvenie algoritmickej diskriminácie a nový chránený dôvod „digitálne znevýhodnenie“.

Osobitnú pozornosť si vyžaduje skupina 50+, ktorá čelí kumulácii historických, štrukturálnych a zdravotných bariér. Rekvalifikácia a celoživotné vzdelávanie musia byť modulárne, projektovo orientované, s mentorstvom a primeraným tempom; štátne programy a zamestnávateľia by mali zaviesť minimálne štandardy kvality a primerané úpravy digitálnych nástrojov.

Napokon, potrebujeme aj empirickú agendu, predovšetkým meranie dopadov HR-AI na prístup k práci, pracovné podmienky a nerovnosti, aby bolo možné reguláciu priebežne korigovať. Len ak sa „digitálna dôstojnosť“ stane operačným princípom tvorby politiky, podnikovej praxe i súdnej ochrany, dokáže slovenské pracovné právo zmysluplne nasmerovať technologickú inováciu k spravodlivej a inkluzívnej práci.

Zoznam použitej literatúry

1. BALÁŽ, V. a kol.: *Pozor na nerovnosti kvôli veku*. Bratislava: Implementačná agentúra Ministerstva práce, sociálnych vecí a rodiny SR. 2023. [cit. 2025-11-18] 194s. <https://eurofondy.praca.gov.sk/wp-content/uploads/2023/06/Pozor-na-nerovnosti-kvoli-veku-final_AV>
2. BALYTSKA, Mariia, et al.: Unlocking the Potential Under Ageing Labor Force and Digitalization Challenges. In: *2023 IEEE 4th KhPI Week on Advanced Technology (KhPI Week 2023) – Conference Proceedings*. Kharkiv, Ukraine, 2023, s. 1-7, [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1109/KhPIWeek61412.2023.10313005>>
3. BARTIKOWSKI, Boris et al.: The Type-of-Internet-Access Digital Divide and the Well-being of Ethnic Minority and Majority Consumers: A Multi-Country Investigation. In *Journal of Business Research*, Vol. 82, January 2018, s.373–380. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1016/j.jbusres.2017.05.033>>

4. BITTO URBANOVA, Laura et al: Technology supports me: perceptions of the benefits of digital technology in adolescents. In *Frontiers in Psychology*, Vol. 13, Art.No. 970395, 30 Jan. 2023, [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.3389/fpsyg.2022.970395>>
5. CAPÍKOVÁ, Silvia: Rovnaké zaobchádzanie a zákaz diskriminácie. In: NOVÁKOVÁ, M. a kol.: *Pracovné právo 1*. Bratislava, Wolters Kluwer, 2024, s.66 – 76. ISBN: 978-80-571-0676-0
6. CAPÍKOVÁ, Silvia: Medzi poriadkom a chaosom: právo v období post-komunistickej transformácie na Slovensku. In *Sociologický časopis / Czech Sociological Review*, Vol. 41, No. 4 (2005), s. 617–640. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.13060/00380288.2005.41.4.06>>
7. ČAPLÁNOVÁ, Anetta – DARMO, Ľubomír: Exploration into the Digital Skill Development Needs and Challenges of Older Workers (Case Study of Slovak Ageing Work Force). In *Knowledge Management in Organisations*, Springer CCIS Series, Vol. 2562, 2025, pp. 104–122. [cit. 2025-11-18] Dostupné na internete: <https://doi.org/10.1007/978-3-031-95898-4_8>
8. DALESSANDRO, Cristen - LOVELL, Alexander: The Digital Dignity Divide: Work, Technology, and Well-Being Outcomes Among U.S. Employees. In *Social Currents*, Vol. 12, No. 4 (2025), 370-388. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/23294965251356407>>
9. DAŇKO, Martin - PORUBAN, Andrej: Práva a povinnosti zamestnancov v Akte o umelej inteligencii. In *Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024. Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie*. Trenčín: Trenčianska univerzita Alexandra Dubčeka v Trenčíne, Fakulta sociálno-ekonomických vzťahov, 2024, s.10 - 19. ISBN 978-80-8295-044-4.
10. EUROPEAN COMMISSION: *Akčný plán digitálneho vzdelávania 2021–2027: Prispôsobenie vzdelávania a odbornej prípravy digitálnemu veku*. 30 Sept. 2020, COM(2020) 624 final. EUR-Lex. [cit. 2025-11-18] Dostupné na internete: <<https://eur-lex.europa.eu>>
11. EUROPEAN COMMISSION: *Vytvorenie Európskeho piliera sociálnych práv*. 26 Apr. 2017, COM(2017) 250 final. EUR-Lex. [cit. 2025-11-18] Dostupné na internete: <<https://eur-lex.europa.eu>>
12. EU DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY: Digital Skills and Jobs Coalition. [cit. 2025-11-18] Dostupné na internete: <<https://www.digital-skills-jobs.europa.eu>>
13. KLUGE, Johanna - HILDEBRANDT, Julian - ZIEFLE, Martina: The Golden Age of Silver Workers?. s.520 - 532. In Zhou, J., Salvendy, G. (eds.). *Human Aspects of IT for the Aged Population. Social Media, Games and Assistive Environments. HCII*

2019. *Lecture Notes in Computer Science*, Vol 11593. Springer, Cham. [cit. 2025-11-18] Dostupné na internete: <https://doi.org/10.1007/978-3-030-22015-0_40>
14. LACKO, Miloš (ed.) *Európsky sociálny model a jeho úlohy*. Trnava: Právnická fakulta Trnavskej univerzity, 2020, 207s. ISBN978-80-568-0204-5
 15. LAKOMÝ, Martin – ŠÁCHA, Jakub – VYSTRČIL, Filip: Attitudes of European Older Workers Towards Digitalisation from the Ecological Perspective. In: *Information, Communication & Society*, vol. 28, no. 5 (2025), p. 1_20. 1–20. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1080/1369118X.2025.2472944>>
 16. LI, Yuanzuan et al.: The Impact of Digital Economy on Flexible Employment: The Mediating Role of Laborer Perceptions. In: *Sage Open*, Vol.15, No. 1 (2025), s.1-19. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/21582440251327017>>
 17. McCRUDDEN, Christopher: Human Dignity and Judicial Interpretation of Human Rights. In: *European Journal of International Law*, vol. 19, no. 4 (2008), pp. 655–724. [cit. 2025-11-18] Dostupné na internete: <<https://www.ejil.org/pdfs/19/4/1658.pdf>>
 18. Ministerstvo práce, sociálnych vecí a rodiny SR: Úrady práce, sociálnych vecí a rodiny podporia rozvoj zručností. *MPSVR SR*. [cit. 2025-11-18] Dostupné na internete: <<https://www.employment.gov.sk>>
 19. Nariadenie Európskeho Parlamentu a Rady 2016/679 z 27 apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov, GDPR). Ú. v. EÚ L 119, 4.5.2016, pp. 1–88.
 20. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá pre umelú inteligenciu a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (zákon o umelej inteligencii, AI Act). Ú. v. EÚ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>
 21. NIKOLAEVA, Svetlana G. – YANDARBAEVA, Luiza A.: On the Problem of Social and Labor Adaptation of the Age Population in Modern Conditions. In: Anna Rumyantseva & Hod Anyigba & Elena Sintsova & Natalia V. Vasilenko (ed.), *Finance, Economics, and Industry for Sustainable Development*. Cham, Springer. 2024, pages 519-528.
 22. PARDO-VERGARA, María: Dignity as Humanness: A Pathway to Understand the Place of Dignity as a Constitutional End. In: *International Journal of Law in Context*, Cambridge University Press, Vol. 21, no. 3 (2025), pp. 514–32. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1017/S1744552325100025>>

23. Smernica Rady 2000/78/ES z 27. novembra 2000, ktorá ustanovuje všeobecný rámec pre rovnaké zaobchádzanie v zamestnaní a povolani. Ú. v. ES L 303, , pp. 16–22.
24. Súdny dvor Európskej únie. Rozsudok z 22. novembra 2005, Werner Mangold proti Rüdiger Helm, vec C-144/04, EU:C:2005:709 [online]. Luxembourg : CURIA, 2005 [cit. 2025-11-07]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=65973&doclang=EN>>
25. Súdny dvor Európskej únie. Rozsudok z 17. júla 2008, S. Coleman proti Attridge Law a Steve Law, vec C-303/06, EU:C:2008:415 [online]. Luxembourg : CURIA, 2008 [cit. 2025-11-07]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=67793&doclang=EN>>
26. Súdny dvor Európskej únie. Rozsudok z 19. januára 2010, Seda Küçükdeveci proti Swedex GmbH & Co. KG, vec C-555/07, EU:C:2010:21 [online]. Luxembourg : CURIA, 2010 [cit. 2025-11-07]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=72619&doclang=EN>>
27. Súdny dvor Európskej únie. Rozsudok z 21. júla 2011, Gerhard Fuchs a Peter Köhler proti Land Hessen, spojené veci C-159/10 a C-160/10, EU:C:2011:508 [online]. Luxembourg : CURIA, 2011 [cit. 2025-11-07]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=130450&doclang=EN>>
28. Súdny dvor Európskej únie. Rozsudok z 19. apríla 2012, Galina Meister proti Speech Design Carrier Systems GmbH, vec C-415/10, EU:C:2012:217 [online]. Luxembourg : CURIA, 2012 [cit. 2025-11-07]. Dostupné na internete: <<https://curia.europa.eu/juris/showPdf.jsf?docid=148434&doclang=EN>>
29. Ústredie práce, sociálnych vecí a rodiny: Národný projekt Zručnosti pre trh práce. (n.d.) Accessed 18 Sept. 2025. <<https://www.upsvr.gov.sk>>
30. VAN LAAR, Ester – VAN DEURSEN, Alexander J. A. M. – VAN DIJK, Jan A. G. M. – DE HAAN, Jos: Determinants of 21st-Century Skills and 21st-Century Digital Skills for Workers: A Systematic Literature Review. In: SAGE Open, vol. 10, no. 1 (2020), pp. 1–14. [cit. 2025-11-18] Dostupné na internete: <<https://doi.org/10.1177/2158244019900176>>
31. VEALE, Michael - EDWARDS, Lilien: Clarity, Surprises, and Further Questions in the GDPR's Approach to Automated Decision-Making. In Computer Law & Security Review, Vol. 34, No. 2 (2018), s.398- 404.
32. Zákon č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov (antidiskriminačný zákon, ADZ), v znení neskorších predpisov.
33. Zákon č. 311/2001 Z. z. Zákonník práce (ZP), v znení neskorších predpisov.
34. Zákon č.5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov

Kontaktné údaje

doc. JUDr. Mária Nováková, PhD.

maria.novakova@flaw.uniba.sk

Katedra pracovného práva a práva sociálneho zabezpečenia

Právnická fakulta Univerzity Komenského v Bratislave

ROVNAKÉ ZAOBCHÁDZANIE V KONTEXTE VIRTUALIZÁCIE MIESTA VÝKONU PRÁCE¹

EQUAL TREATMENT IN CONTEXT OF VIRTUALISATION OF THE PLACE OF WORK

Pavol Rak²

Abstrakt: Zamestnanci, ktorí vykonávajú prácu na iných miestach, ako je pracovisko zamestnávateľa, sú vystavení zvýšenej hrozbe nerovnakého zaobchádzania v porovnaní so zamestnancami pracujúcimi na pracoviskách zamestnávateľa. Technologický pokrok a následné rozšírenie možností výkonu závislej práce na rôznych miestach mimo pracoviska zamestnávateľa priniesol modely výkonu práce, ktoré neboli plne reflektované pracovným právom a ktoré neboli rozšírené pri torbe predpisov antidiskriminačného práva. Zamestnanci pracujúci v domácnosti, zamestnanci vykonávajúci prácu pre digitálne platformy ale i digitálni nomádi predstavujú kategórie zamestnancov, ktorí sú ohrození nerovnakým zaobchádzaním v porovnaní so zamestnancami vykonávajúcimi prácu na pracovisku zamestnávateľa. Platná legislatíva neobsahuje osobitnú úpravu tejto kategórie zamestnancov ale iba všeobecným spôsobom upravuje povinnosť zamestnávateľov proaktívne pristupovať k rovnakému zaobchádzaniu a to aj v povinnosti prijímať opatrenia na ochranu pred diskrimináciou zamestnancov pracujúcich mimo pracoviska zamestnávateľa. Zavedenie transparentného odmeňovania a transparentných procesov a postupov nezávislých od miesta výkonu práce zamestnanca je základným predpokladom pre ochranu pred nerovnakým zaobchádzaním s touto skupinou zamestnancov.

Kľúčové slová: Domácka práca, telepráca, virtuálne miesto, diskriminácia

Abstract: Employees who perform work in locations other than the employer's workplace are exposed to an increased risk of unequal treatment compared to employees working at the employer's premises. Technological progress and the subsequent expansion of opportunities to perform dependent work in various locations have introduced work performance models that were not fully

¹ Príspevok bol spracovaný pod záštitou projektu VEGA č. 1/0677/24 s názvom „Ženy v kríze“.

²Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta Univerzity Komenského v Bratislave

reflected in labor law and were not widely spread when anti-discrimination regulations were adopted. Employees working from home, employees performing work for digital platforms, as well as digital nomads, represent categories of employees who are at risk of unequal treatment compared to employees performing work at the employer's workplace. The current applicable legislation does not contain specific regulations for this category of employees but only generally stipulates the obligation of employers to proactively ensure equal treatment, including the duty to take measures to protect employees working outside the employer's workplace from discrimination. The introduction of transparent remuneration and transparent processes and procedures, independent of the employee's place of work, is a fundamental prerequisite for protection against unequal treatment of this group of employees.

Key words: working from home, telework, virtual workplace, discrimination

Úvod

Pod pojmom „virtualizácia miesta výkonu práce“ možno chápať postupné opúšťanie rigidného chápania miesta výkonu práce v zmysle továrne alebo kancelárskeho priestoru a jeho rozširovanie na iné miesta, než sú priestory poskytnuté alebo zabezpečené zamestnávateľom. Súčasné chápanie miesta výkonu práce vzniklo spolu s prvou priemyselnou revolúciou spojenou s vynálezom a rozšírením využívania parného stroja v 18. storočí. Dovtedy sa veľká časť pracovnej činnosti vykonávala priamo v domácnosti či usadlosti osôb, resp. v prípade poľnohospodárskej produkcie na poli a lúkach. Aktuálny trend rozširovania home office a telepráce preto možno z takéhoto širšieho historického pohľadu chápať ako čiastočný návrat k pôvodnému, domáckemu spôsobu výkonu práce. Zatiaľ čo v minulosti bola práca na diaľku spojená predovšetkým s drobnými manuálnymi prácami, s rozvojom počítačovej techniky sa jej ťažiskom stáva predovšetkým kancelársky typ práce, kde dominujúcim pomocníkom zamestnanca je počítač.³ Štandardná práca v pracovnom pomere na neurčitý čas a na plný úväzok je na ústupe, rozširujú sa najrôznejšie formy atypických zamestnaní, od pracovného pomeru na kratší pracovný čas, či na určitú dobu, cez teleworking, až po on-call contracts.⁴ Je možné dokonca tvrdiť, že sa po dlhšej dobe mení chápanie toho, čo sa všeobecne vníma ako štandardná práca. Zákon

³ TOMŠEJ, J. Zákoník práce v praxi komplexní průvodce řešením problémů, 4. vydání. Praha : GRADA Publishing, a.s., 2022, s.163

⁴ BULLA, M. Nové formy regulácie ako odpoveď na meniaci sa svet práce. In. ŠVEC, M., BULLA, M. Práca 4.0, digitálna spoločnosť a pracovné právo. Bratislava : Friedrich Ebert Stiftung, zastúpenie v SR, 2018, s. 10

č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov (ďalej len „ZP“) doposiaľ nereflektoval na možnosť, že určenie konkrétneho miesta výkonu práce nie je zo strany zamestnávateľa a zamestnanca potrebné alebo žiadané.

Takéto prípady predstavujú najmä virtuálne pracovné miesta, kde fyzické miesto výkonu práce nie je vôbec relevantné. Zamestnávateľ má v týchto prípadoch buď záujem iba na výsledku činnosti zamestnanca alebo zamestnanec môže plnohodnotne vykonávať prácu podľa pokynov zamestnávateľa v rámci dohodnutého druhu práce na akomkoľvek (fyzickom) mieste, obvykle stačí dostatočné pripojenie na internet.

Zamestnanec na hybridnom pracovnom mieste vykonáva prácu kombinovane – čiastočne na dohodnutom (fyzickom) mieste výkonu práce u zamestnávateľa a čiastočne kdekoľvek podľa miesta výskytu zamestnanca. Podľa zahraničných štúdií⁵ viac ako 70% zamestnancov pracujúcich mimo pracoviska zamestnávateľa v celosvetovom meradle sú na hybridnom rozvrhu a obvyklý rozvrh zahŕňa 3 dni v týždni na pracovisku a 2 dni v domácnosti. Moderné informačné a komunikačné technológie spružnili výkon práce, odstránili priestor a čas, čo sa odzrkadlilo aj v zmene obsahu práce. Tento trend prináša aj neštandardné pracovné podmienky.⁶ Zároveň je možné sledovať aj trend znevýhodňovania zamestnancov pracujúcich mimo pracoviska zamestnávateľa, ktorý môže prerásť až do nerovnakého zaobchádzania s týmito zamestnancami, ktoré je podložené práve ja kritériu odlišného miesta výkonu práce.

Formy virtualizácie pracovného miesta

Opúšťanie zaužívaného konceptu miesta výkonu práce v pracovnoprávných vzťahoch prebieha rozličnými formami. Najjednoduchšia a najprirodzenejšia forma (čiastočne) virtualizácie pracovného miesta je príležitostný výkon práce z domácnosti (**home office**), **domácka práca a telepráca**, ktoré sú už v právnej úprave zakotvené. Predstavujú základné a aprobované formy hybridne určeného miesta výkonu práce. O domácku prácu/teleprácu ide, ak ide o prácu, ktorá sa môže vykonávať aj na pracovisku zamestnávateľa, ale prenáša sa do domácnosti zamestnanca. Nie je to teda práca, ktorá sa na pracovisku nedá vykonávať, resp. jej povaha je výlučne terénna.⁷

⁵ BLOOM, N., HAN, R., LIANG, J. Hybrid working from home improves retention without damaging performance. *Nature* 630, s.920 [cit. 23.09.2025]

⁶ TRELOVÁ, S. Digitalizácia pracovného prostredia – bezpečnosť, riziká a vplyv na zamestnanca. *Týn nad Vltavou - Malá strana: Nová Forma*, 2021, s. 45

⁷ ŠVEC, M., TOMAN, J. a kol. : Zákonník práce. Zákon o kolektívnom vyjednávaní. Komentár Zväzok I. 2. doplnené a prepracované vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2023, s. 512

Ďalšou formou je výkon **platformovej práce**. Kým prechod výkonu práce z domácností do priestorov zamestnávateľa bol výsledkom prvej priemyselnej revolúcie, platformová práca je dôsledkom ostatnej, štvrtej priemyselnej revolúcie. Pri výkone platformovej práce dochádza k úplnému oddeleniu zamestnanca a jeho miesta výkonu práce od zamestnávateľa. Pri posudzovaní pracovnoprávných aspektov je významným faktorom skutočnosť, do akej miery digitálne pracovné platformy organizujú výkon práce, jej odmeňovanie a vzťah medzi zákazníkmi a osobami pracujúcimi pre platformu. Odhaduje sa, že najväčšie príjmy v sektore platformovej práce sa generujú v odvetví doručovacích služieb a taxislužieb, ktoré už inherentne sú oddelené od priestorov zamestnávateľa. Ďalšou problematickou črtou platformovej práce je pokrývanie výkonu závislej práce obchodnoprávnymi inštitútmi. Smernica Európskeho parlamentu a Rady o zlepšení pracovných podmienok v oblasti práce pre platformy preto **upravuje prezumpciu pracovnoprávneho vzťahu** medzi prevádzkovateľom digitálnej platformy a osobami pracujúcimi pre túto platformu. Jedným z deklarovaných cieľov smernice je boj s nelegálnym zamestnávaním práve vo forme nepravnej samostatne zárobkovej činnosti v oblasti práce pre platformy. Ako nástroj boja bola zvolená metóda zavedenia vhodných identifikačných postupov na národnej úrovni, potom ako zlyhala snaha o zavedenie presných a spoločných definičných kritérií na úrovni celej Európskej únie. Spoločné kritériá by jednotne chránili fyzické osoby pracujúce pre digitálne platformy tým, že by sa tieto osoby považovali za zamestnancov prevádzkovateľa digitálnej platformy a vzťah s prevádzkovateľom digitálnej platformy by sa považoval za pracovnoprávny vzťah, pokiaľ sa nepreukáže opak. Prvotný návrh smernice upravoval prezumpciu pracovnoprávneho vzťahu za splnenia najmenej dvoch z nasledujúcich piatich podmienok: 1. určovanie úrovne odmeňovania alebo stanovovanie horných hraníc odmeňovania, 2. dohľad nad vykonávaním práce elektronickými prostriedkami, 3. obmedzovanie slobody zvoliť si pracovný čas alebo obdobia neprítomnosti, prijať alebo odmietnuť úlohy alebo využiť subdodávateľov alebo náhradníkov, 4. stanovenie osobitných záväzných pravidiel týkajúcich sa vzhľadu, správania voči príjemcovi služby alebo výkonu práce, alebo 5. obmedzenie možnosti vybudovať si klientsku základňu alebo vykonávať prácu pre akúkoľvek tretiu stranu.

Zavedenie prezumpcie pracovnoprávneho vzťahu do práva EÚ je vítaným krokom k zjednoteniu ochrany zamestnancov. Čl. 5 ods. 1 smernice zakotvil vyvrátiteľnú právnu domnienku, podľa ktorej ak sa zistia skutočnosti, ktoré naznačujú riadenie a kontrolu v súlade s vnútroštátnym právom, kolektívnymi zmluvami alebo zaužívanou praxou platnými v členských štátoch a s prihliadnutím na judikatúru Súdneho dvora, je takýto právny vzťah považovaný za pracovnoprávny vzťah. Fenomén pokrývania pracovnoprávných vzťahov obchodnoprávnymi inštitútmi nie je nový a pracovnoprávna literatúra naňho upozorňuje dlhodobo. Barancová napr. uvádza,

že v ostatnom čase sa rozširuje pracovná kategória fyzických osôb, ktoré nie sú v pracovnom pomere, ale v inom zmluvnom vzťahu k odberateľovi práce, vykonávajú práce nie tak v osobnej závislosti, ale v hospodárskej závislosti.⁸

Digitálni nomádi predstavujú osobitnú kategóriu osôb, ktoré vykonávajú pracovné činnosti z miesta, ktoré si sami zvolia a ktoré sa môže signifikantne a veľmi často meniť. Za autora pojmu digitálny nomád sa označuje Tsugio Makimoto, ktorý tento pojem použil už v roku 1997. Za digitálnych nomádov sú považované fyzické osoby, ktoré využívajú digitálne technológie na spojenie práce, oddychu a cestovania. Ako uvádzajú niektorí autori, nomádske správanie síce vedie digitálnych nomádov k používaniu IT platforiem obdobne ako pri telepráci, avšak odlišuje ich dĺžka zotrvania na určitom mieste vzhľadom na ich rozhodnutie vzdať sa konkrétného stáleho miesta (adresy) pobytu. Digitálni nomádi navyše častokrát vykazujú znaky podnikateľského správania a nevykonávajú závislú prácu v pravom slova zmysle. Pokiaľ digitálni nomádi vykonávajú závislú prácu, z pohľadu slovenského pracovného práva je ich de lege lata potrebné zaradiť do kategórie zamestnancov pracujúcich v režime telepráce.

Rovnaké zaobchádzanie

Medzi ústredné požiadavky spravodlivosti a rovnosti patrí aj požiadavka, aby človek nebol znevýhodnený iba z dôvodu, že je súčasťou istej skupiny alebo kolektívu – zákaz diskriminácie na základe pôvodu, pohlavia, zdravotného postihnutia, veku atď.⁹ Zásada rovnakého zaobchádzania býva charakterizovaná ako pozitívne vyjadrenie zákazu diskriminácie.¹⁰

Diskrimináciou je také konanie alebo opomenutie spočívajúce v neoprávnenom rozlišovaní alebo znevýhodňovaní určitej skupiny vo vzťahu k inej skupine, ktoré vo svojom dôsledku môže privodiť jedincovi alebo celej skupine újmu peňažnej alebo nepeňažnej povahy (väčšinou narušiť dôstojnosť).¹¹

Zamestnanci pracujúci mimo pracoviska zamestnávateľa predstavujú skupinu zamestnancov, ktorí sú potenciálne vystavení nerovnakému zaobchádzaniu v porovnaní so svojimi „analogovými“ zamestnancami. Neprítomnosť na pracovisku a absencia sociálnych väzieb s ostatnými zamestnancami a najmä vedúcimi zamestnancami, nepredstavujú skutočnosť, ktorá by patrila medzi typické diskriminačné dôvody. Výpočet diskriminačných dôvodov je relatívne otvorený,

⁸ BARANCOVÁ, H. Slovenské a európske pracovné právo. Žilina : Poradca podnikateľa, spol. s r.o., 2004, s.94

⁹ FÁBRY, B., KASINEC, R., TURČAN, M. Teória práva. Druhé prepracované vydanie. Bratislava : Wolters Kluwer SR, 2019. s. 54

¹⁰ ŠTANGLOVÁ, V. Rovné zacházení a zákaz diskriminace v pracovním právu. Plzeň : Aleš Čeněk, 2010. s. 47

¹¹ KLODINSKÁ, K a kol. Právo sociálního zabezpečení. 1. Vydání. Praha : C. H. Beck, 2022, s. 422

keďže diskriminačný dôvod iného postavenia zahŕňa aj situácie, ktoré nie sú výslovne uvedené v enumerácii týchto dôvodov a predstavuje variabilný prvok v prípade situácií, ktoré zákonodarca nepredvídal.¹² Odlišné miesto výkonu práce preto možno subsumovať pod „iné postavenie“ v zmysle § 2 ods. 1 zákona č. 365/2004 Z.z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov (antidiskriminačný zákon) v znení neskorších predpisov (ďalej len „ADZ“). Civilnoprocesnú ochranu v prípade diskriminácie zabezpečujú osobitné procesné predpisy sporov so slabšou stranou. K vyrovnaní nerovnovážneho postavenia medzi zamestnancom a zamestnávateľom v súdnom spore významne prispeje aj obrátené dôkazné bremeno či priam inkvizičná právomoc súdu pri dokazovaní.¹³

Nárast výkonu práce mimo pracoviska zamestnávateľa predstavuje už aj zo štatistického hľadiska vyššiu pravdepodobnosť vzniku nerovnakého zaobchádzania. Diskriminácia môže mať rozličné podoby od priamej a nepriamej diskriminácie až po rôzne formy šikanózneho správania. U zamestnancov pracujúcich mimo pracoviska zamestnávateľa sa zvýšené riziko nerovnakého zaobchádzania prejavuje početnými formami, spomedzi ktorých vyberáme tie najrozšírenejšie:

(i) kontrola

Zamestnávatelia majú vyššiu tendenciu kontrolovať zamestnancov, ktorí vykonávajú prácu z domácnosti alebo na inom mieste. Výkon práce je zvyčajne spojený s používaním elektronických prostriedkov a zamestnávatelia majú softvérové možnosti ako sledovať činnosť resp. nečinnosť zamestnancov. Tieto kontrolné mechanizmy podliehajú režimu podľa § 13 ZP ods. 4 ZP. Freel poukazuje na skutočnosť, že zamestnávateľ by mal predovšetkým informovať zástupcov zamestnancov (ak u zamestnávateľa pôsobia) o formách kontroly zamestnancov, mal by informovať zamestnancov o rozsahu uskutočnených kontrol, spôsobe ich uskutočnenia a tiež o ich trvaní.¹⁴ Ako upozorňuje Dolobáč, zamestnávatelia odôvodňujú monitoring emailovej komunikácie snahou o zvyšovanie efektivity práce a z právneho pohľadu argumentujú zákonnou povinnosťou zamestnanca využívať pracovný čas na prácu a povinnosťou riadne hospodáriť s prostriedkami, ktoré mu boli zverené.¹⁵ Typickými kontrolnými mechanizmami sú softvérové nástroje na sledovanie pohybov kurzora na obrazovke a tým aj využívania myši resp. touchpadu, počet klikov na klávesnici alebo transfer dát z internetového prehliadača. Zamestnávatelia prirodzene inklinujú k vyššiemu podozrievaniu zamestnancov

¹² Rozsudok KS TT, spis. zn. 10CoPr/2/2018 zo dňa 26.9.2018

¹³ HOMOLA NEVICKÁ, D.: Menštruačné voľno ako nástroj rodovej rovnosti v pracovnoprávných vzťahoch. 1. vydanie. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2025. s. 29

¹⁴ NOVÁKOVÁ, M. a kol. Pracovné právo 1. 1. Vydanie. Bratislava : Wolters Kluwer SR s.r.o., 2024, s. 127

¹⁵ DOLOBÁČ, M. a kol. Zákoník práce. Veľký komentár. Žilina : Eurokódex, s.r.o., 2023, s. 116

mimo ich fyzický dosah z neefektívnosti, prípadne z výkonu inej práce (starostlivosť o rodinných príslušníkov, výkon domáckych práca a pod.), než práce pre zamestnávateľa v zmysle pracovnej zmluvy.

(ii) proximity bias¹⁶

Zamestnanci vykonávajúci závislú prácu na pracovisku majú prirodzene lepšiu šancu na kariérny rast a na získanie zaujímavejších alebo dôležitejších pracovných úloh. Vďaka možnosti neformálneho kontaktu a rozličných neorganizovaných spoločenských podujatí (fajčiarske prestávky, príprava kávy alebo ohrievanie jedla v kuchyni zamestnávateľa) umožňujú zamestnancom na pracovisku získať viac informácií, než je poskytovaných v oficiálnej komunikácii zamestnávateľa adresovanej na všetkých zamestnancov. Takáto informačná asymetria znevýhodňuje zamestnancov pracujúcich mimo pracoviska zamestnávateľa. Práca na významnejších projektoch a s tým spojené výsledky a úspechy zlepšujú šance na kariérny rast zamestnancov fyzicky prítomných na pracovisku zamestnávateľa. Hodnotenie zo strany zamestnávateľov môže byť skreslené pocitom, že zamestnanci pracujúci mimo pracoviska zamestnávateľa sú ťažšie zastihnuteľní alebo menej výkonní ako ich kolegovia na pracovisku.

(iii) sociálna izolovanosť

Vo vzťahu k ostatným zamestnancom majú zamestnanci pracujúci mimo pracoviska zamestnávateľa menšiu šancu na vytvorenie spoločenských kontaktov a sú vystavení zvýšenému riziku vzniku sociálnej izolácie. Výkon závislej práce je spojený aj s napĺňaním potreby uplatnenia a sebarealizácie zamestnancov, prípadne aj spoločenského uplatnenia. Zamestnanci sú častejšie terčom kyberšikany, nakoľko majú menšiu možnosť sa brániť bez fyzickej prítomnosti na pracovisku. Z pohľadu zamestnávateľa predstavuje protipól sociálnej izolovanosti zamestnancov nízka miera lojality zamestnancov voči zamestnávateľovi.

(iv) odmeňovanie a náklady

Zamestnanci pracujúci mimo pracoviska zamestnávateľa majú v zmysle v § 52 ods. 8 písm. c) ZP nárok na náhradu preukázateľne zvýšených výdavkov spojených s používaním vlastného náradia, vlastného zariadenia a vlastných predmetov potrebných na výkon domáckej práce alebo telepráce. Zamestnávateľia majú v aplikačnej praxi snahu minimalizovať akékoľvek náklady zamestnancov a zamestnanci majú problém preukázať zvýšené náklady. Tu je de lege ferenda potrebná podrobnejšia úprava, ktorá by chránila zamestnanca a nezaťažovala zamestnávateľa zbytočnou administratívou. Príkladom by bolo zavedenie paušálnych náhrad zvýšených nákladov zamestnancov, ktoré by zamestnanec nemusel preukazovať a ktoré by zamestnávateľovi boli zo strany daňovej správy uznané ako daňové výdavky. Veľkí zamestnávateľia sa snažia obmedzovať výkon

¹⁶ Angl. zaujatosť z dôvodu priestorovej blízkosti

práce mimo priestory zamestnávateľa aj vytváraním odmeňovacích štruktúr, ktoré sú nevýhodné pre zamestnancov nepracujúcich v priestoroch zamestnávateľa. Príkladom je aj gigant Google, ktorý oznámil osobitnú odmeňovaciu politiku pre zamestnancov pracujúcich výlučne z domácnosti.¹⁷ Zamestnanci, ktorí pracujú v regiónoch s nižšími mzdami, budú odmeňovaní podľa úrovne miezd v danom regióne. Takýto postup by bol v rozpore s § 119a ZP resp. s pripravovaným zákonom o uplatňovaní zásady rovnakej odmeny pre mužov a ženy za rovnakú prácu alebo za prácu rovnakej hodnoty a o zmene a doplnení niektorých zákonov.

(v) pracovný čas

Na rozdiel od zvýšenej kontroly výkonu práce zo strany zamestnávateľa, kontrola pracovného času je zo strany zamestnávateľov opomínaná. Zamestnávateľ má povinnosť viesť evidenciu pracovného času, práce nadčas, nočnej práce, aktívnej časti a neaktívnej časti pracovnej pohotovosti zamestnanca tak, aby bol zaznamenaný začiatok a koniec časového úseku, v ktorom zamestnanec vykonával prácu. Domácka práca a telepráca, ale ani práca z domu nie je vyňatá z plnenia povinností podľa § 99 ZP.¹⁸ Zároveň ale zamestnávateľ nemá priamu možnosť kontrolovať dodržiavanie pracovného času a mať priamy dohľad nad evidenciou pracovného času zamestnancov, hoci v zmysle § 99 ods. 1 ZP je to jeho zákonná povinnosť. Zamestnancom hrozí riziko nedodržiavania prestávok v práci a dôb odpočinku v tom zmysle, že zamestnanci len fiktívne vykážu v dochádzke dobu odpočinku, ale fakticky ju nevyužijú na odpočinok. Ako upozorňuje Barancová, nevyhnutnosť dodržiavania maximálnych zákonných limitov týždenného a denného pracovného času vyplýva aj z rozsudku Súdneho dvora EÚ v právnej veci C-55/18 (Deutsche Bank) zo 14. mája 2019.¹⁹ Túto pozíciu potvrdil aj recentný rozsudok v právnej veci C-531/23 (Loredas), ktorým sa všeobecná povinnosť evidencie pracovného času deklarovala aj vo vzťahu k zamestnancom pracujúcim v domácnosti. Z pohľadu slovenského pracovného práva tým bol potvrdený výklad, že § 99 ZP sa v plnej miere vzťahuje aj na zamestnancov pracujúcich mimo pracoviska zamestnávateľa.

(vi) zvýšená psychologická záťaž

Popri aspekte pracovného času a dôb odpočinku v zmysle predošlého bodu, zamestnanci sú vystavení zvýšenej psychickej záťaži aj z pohľadu priestorového aspektu. Stieranie rozdielov medzi miestom výkonu práce a miestom rodinného alebo iného súkromného života predstavuje ďalší znevýhodňujúci faktor pre zamestnancov pracujúcich mimo pracoviska zamestnávateľa. Kým zamestnanci,

¹⁷ Google's Salary Cuts for Remote Workers Renew Location-Based Pay Debate. Dostupné na <https://www.shrm.org/topics-tools/news/benefits-compensation/googles-salary-cuts-remote-workers-renew-location-based-pay-debate> (navštívené 28.9.2025)

¹⁸ ŠVEC, M., TOMAN, J. a kol. : Zákoník práce. Zákon o kolektívnom vyjednávaní. Komentár Zväzok I. 2. doplnené a prepracované vydanie. Bratislava: Wolters Kluwer SR s.r.o., 2023, s. 1061

¹⁹ BARANCOVÁ, H. a kol. Zákoník práce. Komentár. 3. vydanie. Bratislava : C. H. Beck, 2022, s.585

ktorí pracují z domácnosti iba príležitostne vnímajú možnosť výkonu práce z domácnosti ako benefit, zamestnanci pracujúci výlučne z domácnosti môžu toto pociťovať ako zaťažujúci faktor. Zamestnávateľa taktiež len zriedka dokážu alebo sú ochotní vybaviť domácnosť zamestnanca v rovnakom štandarde, aký je na pracovisku zamestnávateľa (napr. možnosť kopírovania a skenovania dokumentov, občerstvenie formou kávy alebo drobného občerstvenia nad zákonný pitný režim a pod.). Zamestnanec pracujúci mimo pracoviska zamestnávateľa taktiež môže pociťovať (opodstatnený či neopodstatnený) pocit tlaku byť neustále zastihnutelný a dostupný pre akékoľvek požiadavky zamestnávateľa. Stonjek uvádza príklady okolností nútiacich zamestnancov vykonávať práce mimo pracovný čas: 1. zadávanie pracovných úloh mimo pracovný čas, 2. povedomie o tom, že sa to „patrí“, aby zamestnanec na určitej pozícii (spravidla lepšie platenej) pracoval i mimo pracovnú dobu, 3. tlak zo strany kolegov, ktorí pracujú aj mimo pracovnú dobu, alebo 4. skutočnosť, že nevykonávanie práce mimo pracovnú dobu by mohlo predstavovať problém z pohľadu profesného rastu, pretože zamestnanec nebol dostatočne flexibilný alebo výkonný.²⁰

Záver

Právna úprava rovnakého zaobchádzania de lege lata je postačujúca pre potreby ochrany zamestnancov pracujúcich mimo pracoviska zamestnávateľa. Niektoré aspekty práce mimo pracoviska zamestnávateľa, ktoré ale neboli predmetom nášho skúmania, ako napríklad dodržiavanie bezpečnosti a ochrany zdravia pri práci alebo náhrady nákladov, je potrebné de lege ferenda podrobnejšie upraviť. Zamestnávateľa majú v rámci zákonnej povinnosti dodržiavania zásady rovnakého zaobchádzania aj povinnosť prijímať opatrenia na ochranu pred diskrimináciou. Zamestnávateľa by preto mali nielen prešetrovať vzniknuté prípady diskriminácie nahlásené zamestnancami, prípadne aj chránenými oznamovateľmi (ochrana ex post). Dôsledné plnenie § 2 ods. 3 ADZ naopak zaväzuje zamestnávateľov podnikáť aktívne kroky na zabránenie vzniku nerovnakého zaobchádzania so zamestnancami (ochrana ex ante).

Identifikácia a poukázanie na zvýšenú hrozbu nerovnakého zaobchádzania vo vzťahu k zamestnancom vykonávajúcim prácu na miestach iných, ako je pracovisko zamestnávateľa, je prvým krokom zabezpečenia rovnakého zaobchádzania. Zavedenie transparentného odmeňovania a transparentných procesov a postupov nezávislých od miesta výkonu práce zamestnanca je základným predpokladom pre ochranu pred nerovnakým zaobchádzaním s touto skupinou zamestnancov.

²⁰ STONJEK, P. Zaměstanecké „benefity“ vs. právo odpojit se aneb prolínání soukromého a pracovního života. in PICHRT, J., TOMŠEJ, J. (eds) Balancování na hraně work-life balance a transparentnosti. Praha : Wolters Kluwer ČR, 2022, s.51

Zoznam použitej literatúry

1. BARANCOVÁ, H. a kol. Zákoník práce. Komentár. 3. vydanie. Bratislava : C. H. Beck, 2022, 1624 s. ISBN 978-80-8232-024-7
2. BARANCOVÁ, H. Slovenské a európske pracovné právo. Žilina : Poradca podnikateľa, spol. s.r.o., 2004, 992 s., ISBN: 80-88931-32-0
3. BLOOM, N., HAN, R., LIANG, J. Hybrid working from home improves retention without damaging performance. *Nature* 630, 920–925 (2024). <https://doi.org/10.1038/s41586-024-07500-2> [cit. 23.09.2025]
4. DOLOBÁČ, M. a kol. Zákoník práce. Veľký komentár. Žilina : Eurokódex, s.r.o., 2023, 894 s. ISBN: 978-80-8155-118-5
5. FÁBRY, B., KASINEC, R., TURČAN, M. Teória práva. Druhé prepracované vydanie. Bratislava : Wolters Kluwer SR, 2019, 321 s. ISBN: 978-80-571-0127-7
6. HOMOLA NEVICKÁ, D. Menštruačné voľno ako nástroj rodovej rovnosti v pracovnoprávných vzťahoch. 1. vydanie. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2025. 72 s. ISBN 978-80-7160-745-8
7. KLODINSKÁ, K a kol. Právo sociálneho zabezpečení. 1. Vydání. Praha : C. H. Beck, 2022. 497 s. ISBN 978-80-7400-902-0
8. NOVÁKOVÁ, M. a kol. Pracovné právo 1. 1. Vydanie. Bratislava : Wolters Kluwer SR s.r.o., 2024, 236 s., ISBN: 978-80-0676-0
9. STONJEK, P. Zaměstanecké „benefity“ vs. právo odpojit se aneb prolínání soukromého a pracovního života. in PICHRT, J., TOMŠEJ, J. (eds) Balancování na hraně work-life balance a transparentnosti. Praha : Wolters Kluwer ČR, 2022, 156 s. ISBN 978-80-7676-278-7
10. ŠTANGLOVÁ, V. Rovné zacházení a zákaz diskriminace v pracovním právu. Plzeň : Aleš Čeněk, 2010, 230 s. ISBN 978-80-7380-277-6
11. ŠVEC, M., TOMAN, J. a kol. Zákoník práce. Zákon o kolektívnom vyjednávaní. Komentár Zväzok I. 2. doplnené a prepracované vydanie. Bratislava : Wolters Kluwer SR s.r.o., 2023, 1479 s. ISBN 978-80-571-0584-8
12. TOMŠEJ, J. Zákoník práce v praxi komplexní průvodce řešením problémů, 4. vydání. Praha : GRADA Publishing, a.s., 2022, 199 s. ISBN 978-80-271-3538-7
13. TREĽOVÁ, S. Digitalizácia pracovného prostredia – bezpečnosť, riziká a vplyv na zamestnanca. Týn nad Vltavou - Malá strana: Nová Forma, 2021. ISBN 978-80-7612-342-7.
14. Rozsudok KS TT, spis. zn. 10CoPr/2/2018 zo dňa 26.9.2018
15. Google's Salary Cuts for Remote Workers Renew Location-Based Pay Debate. Dostupné na <https://www.shrm.org/topics-tools/news/benefits-compensation/googles-salary-cuts-remote-workers-renew-location-based-pay-debate> (navštívené 28.9.2025)

Kontaktné údaje

JUDr. Pavol Rak, PhD.

pavol.rak@flaw.uniba.sk

Katedra pracovného práva a práva sociálneho zabezpečenia

Právnická fakulta, Univerzita Komenského v Bratislave

KONTROLA DODRŽIAVANIA ZÁSADY ROVNAKÉHO ZAOBCHÁDZANIA INŠPEKTORÁTMÍ PRÁCE V SLOVENSKEJ REPUBLIKE

MONITORING COMPLIANCE WITH THE PRINCIPLE OF EQUAL TREATMENT BY LABOUR INSPECTORATES IN SLOVAK REPUBLIC

Marián Lizanec¹

Abstrakt: Tento príspevok sa zaoberá otázkou kontroly dodržiavania zásady rovnakého zaobchádzania inšpektorátmi práce v Slovenskej republike. Zamestnanci a zamestnankyne sa častokrát predtým než úplne rezignujú na obranu svojich práv v prípade, že boli obeťmi diskriminácie rozhodnú obrátiť sa so svojim podnetom na orgány inšpekcie práce. Jedným z prejavov ochrannej funkcie pracovného práva je práve ingerencia orgánu verejnej moci do kontroly povinností, ktoré zamestnávateľom ukladá príslušný právny predpis. Zabezpečenie účinnej ochrany pred diskrimináciou je zároveň medzinárodnoprávnym záväzkom. Napriek skutočnostiam, že počet podnetov z oblasti diskriminácie doručených inšpektorátom práce medziročne narastá, ako aj tomu, že kontrola zákazu diskriminácie nepochybne patrí medzi oblasti, ktorých dodržiavanie dozoruje inšpektorát práce, v jej efektívnej kontrole stále pretrvávajú určité bariéry. Príspevok sa venuje analýze existujúcej právnej úpravy, a to od podania podnetu až po presadzovanie práva, teda uloženie sankcie. Taktiež sa zaoberá prekážkami a výzvami, ktorým čelia inšpektoráty práce a ponúka úvahy na zlepšenie aktuálneho stavu a to či už na potenciálnu zmenu právnej úpravy, alebo iné nelegislatívne opatrenia.

Kľúčové slová: dodržiavanie zásady rovnakého zaobchádzania, inšpektorát práce, kontrola, podnet, zamestnanec, zamestnávateľ

Abstract: This article deals with the issue of monitoring compliance with the principle of equal treatment by labour inspectorates in the Slovak Republic. Employees often decide to turn to labour inspection authorities with their complaints before completely giving up on defending their rights in cases where they have been victims of discrimination. One of the manifestations of the protective function of labour law is precisely the intervention of public authorities in monitoring the obligations imposed on employers by the relevant

¹ Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky

legislation. Ensuring effective protection against discrimination is also an international legal obligation. Despite the fact that the number of complaints of discrimination received by the labour inspectorate is increasing year on year, and that the enforcement of the prohibition of discrimination is undoubtedly one of the areas supervised by the labour inspectorate, certain barriers to effective enforcement remain. This paper analyses the existing legal framework, from the filing of a complaint to the enforcement of the law, i.e., the imposition of sanctions. It also addresses the obstacles and challenges faced by labour inspectorates and offers ideas for improving the current situation, whether through potential changes to the legal framework or other non-legislative measures.

Key words: compliance with the principle of equal treatment, labor inspectorate, inspection, complaint, employer, employee

Úvod

V uplynulom období sme si na Slovensku pripomenuli rôzne výročia, či už to bolo 20. výročie od prijatia antidiskriminačného zákona do nášho právneho poriadku alebo 55. výročie pôsobenia inšpekcie práce.

Na druhej strane nám však zároveň neslávne zarezonovali výsledky prieskumu Agentúry EÚ pre základné práva (FRA), z ktorých vyplynulo, že až 52,9 % žien na Slovensku počas svojej pracovnej kariéry zažilo sexuálne obťažovanie, pričom až 9,4 % respondentiek ho zažilo v uplynulých 12 mesiacoch.² Sexuálne obťažovanie je jednou z foriem diskriminácie a predstavuje porušenie dodržiavania zásady rovnakého zaobchádzania. Obzvlášť v dobe digitalizácie k sexuálnemu obťažovaniu na pracovisku môže častokrát dochádzať práve na sociálnych sieťach (napr. posielaním nevyžiadaných obrázkov, nevhodných vtipov a pod.), alebo prostredníctvom e-mailu, čo v končnom dôsledku vytvára toxické pracovné prostredie.

Ako ďalší príklad porušenia zásady dodržiavania zaobchádzania u zamestnávateľov možno uviesť odmeňovanie zamestnancov a zamestnankyň formou tzv. „bonusu za dochádzku“.

Jednou z možností, ako sa voči spomenutým javom na pracovisku brániť je aj možnosť obrátiť sa s podnetom na miestne príslušný inšpektorát práce. Bude ale tento prostriedok ochrany pred diskrimináciou dostatočne účinný? Čo sú prípadné

² FRA, EIGE, Eurostat, EU gender-based violence survey – Key results. Experiences of women in the EU-27, Publications Office of the European Union, Luxembourg. 2024, s. 37 [online]. [cit. 2025-09-28]. Dostupné na: https://fra.europa.eu/sites/default/files/fra_uploads/eu-gender_based_violence_survey_key_results.pdf

bariéry efektívnej kontroly zásady rovnakého zaobchádzania? Odpovede na tieto otázky sa pokúsime zodpovedať si v tomto príspevku.

Inšpektoráty práce ako orgány dozoru nad dodržiavaním zásady rovnakého zaobchádzania

V zmysle Dohovoru Medzinárodnej organizácie práce (MOP) č. 81 o inšpekcii práce v priemysle a obchode z roku 1947 je funkciou systému inšpekcie práce, cit: „zabezpečiť presadzovanie právnych ustanovení o podmienkach práce a ochrane pracovníkov pri výkone ich práce(...)“.³ Zároveň je úlohou inšpektorátov práce poskytovať zamestnávateľom a zamestnancom odborné informácie a rady o najúčinnějších prostriedkoch dodržiavania právnych predpisov, ktoré dozorujú.⁴ Tieto články sú v slovenskom právnom poriadku premietnuté v príslušných ustanoveniach zákona o inšpekcii práce.⁵ V súlade s Dohovorom MOP č. 81 intervencia orgánov inšpekcie práce prebieha predovšetkým formou prevencie a poradenstva, zberu a vybavovania podnetov a v monitoringu pracoviska.⁶

V zmysle platnej právnej úpravy zamestnanci, ktorí sú poškodení porušením práv alebo povinností vyplývajúcich z pracovnoprávnych vzťahov môžu podať **podnet** na príslušnom inšpektoráte práce.⁷ Toto právo prislúcha aj zástupcom zamestnancov, ktorí sú v pracovnom pomere u zamestnávateľa.⁸

Z dostupných dát je možné vidieť, že toto právo zamestnanci v posledných rokoch čoraz častejšie využívajú v prípadoch, ak sú obeťami nerovnakého zaobchádzania. Počet podaní na inšpektoráty práce, týkajúci sa porušenia zásady rovnakého zaobchádzania má teda rastúci trend. V roku 2024 inšpektoráty práce prijali **286** takýchto podnetov.⁹ Z toho bolo konštatovaných iba **66** porušení relevantných ustanovení Zákonníka práce vo vzťahu k zákazu diskriminácie.¹⁰ Na druhej strane však treba dodať, že tento počet podaní z oblasti zákazu diskriminácie predstavuje

³ Čl. 3 ods. 1, písm. a) Dohovoru MOP č. 81

⁴ Čl. 3 ods. 1 písm. b) Dohovoru MOP č. 81

⁵ Pozri § 2 ods. 1 písm. a) a c) zákona č. 125/2006 Z. z. o inšpekcii práce inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov.

⁶ MEDZINÁRODNÁ ORGANIZÁCIA PRÁCE. Labour inspection and non-discrimination. Ženeva: ILO, september 2022. [online]. [cit. 2025-09-28]. Dostupné na: <https://www.ilo.org/resource/training-material/labour-inspection-and-non-discrimination>

⁷ KRIŽAN, Viktor. § 150 [Inšpekcia práce]. In: BARANCOVÁ, Helena a kol. Zákonník práce. 3. vydanie. Bratislava: C. H. Beck, 2022, s. 1271, marg. č. 1.

⁸ § 150 ods. 2 zákona č. 311/2001 Z. z. Zákonník práce

⁹ Národný inšpektorát práce. Informatívna správa o diskriminácii a rodovej rovnosti v pracovnoprávnych vzťahoch za rok 2024. str. 5. [online]. [cit. 2025-09-28]. Dostupné na: <https://www.ip.gov.sk/diskriminacia-a-rodova-rovnost-v-pracovnopravnych-vztahoch/>

¹⁰ Tamže str. 5

iba **3,1%** z celkového počtu podnetov, ktoré boli prijaté inšpektorátmi práce v roku 2024.¹¹

Výhodou podania podnetu na inšpektorát práce oproti napr. orgánu v oblasti rovnosti je možnosť inšpektorátu práce uložiť zamestnávateľovi administratívnoprávnu sankciu za porušenie právnych predpisov. Nevýhodou orgánu inšpekcie práce je to, že diskriminovanej osobe nemôže priznať žiadne peňažné nároky.¹² Protokol o výsledku inšpekcie práce resp. právoplatné rozhodnutie o uložení pokuty však môže slúžiť ako dôkaz v prípadnom súdnom spore.¹³

Po obdržaní podnetu je inšpektorát práce povinný vykonať inšpekciu práce (pozn. nielen ju vykonať, ale aj prerokovať protokol o výsledku inšpekcie práce so zamestnávateľom) do 30 dní od doručenia podnetu, a v odôvodnených prípadoch do 90 dní od doručenia podnetu. V odôvodnených prípadoch môže túto lehotu primerane predĺžiť Národný inšpektorát práce, pričom inštitút predĺženia lehoty zákonodarca mienil upraviť ako výnimočný inštitút, ktorý sa nemá využívať automaticky.¹⁴

Nesporňovanou výhodou, ktorou inšpektoráty práce disponujú oproti orgánom Equality bodies¹⁵ pri šetrení podnetov, týkajúcich sa diskriminácie je aj to, že majú prístup na pracovisko a majú právo požadovať si od zamestnávateľa prístup k dátam (rozumej dokumentácii, záznamom, možnosť vyhotoviť si kópie a pod.) potrebným pre výkon inšpekcie práce.¹⁶

Inšpektori a inšpektorky práce sú zároveň povinní zachovávať mlčanlivosť o podnetoch na vykonanie inšpekcie práce, o ich obsahu a subjektoch, ktoré podnet podali, a zachovávať mlčanlivosť o ďalších skutočnostiach týkajúcich sa inšpekcie práce, o ktorých sa dozvedeli pri výkone inšpekcie práce.¹⁷ V prípade zistenia nedostatkov sú oprávnení navrhnúť organizačné a iné opatrenia na zlepšenie stavu resp. nariadiť odstránenie zistených nedostatkov.¹⁸ Platná legislatíva taktiež umožňuje využívanie inštitútu prizvaného odborníka pri výkone inšpekcie práce.¹⁹

Inšpektoráty práce môžu v prípade porušenia povinnosti uložiť sankciu až do výšky 100. 000,- EUR za použitia správnej úvahy.²⁰ V praxi však častokrát nejde iba o osamotené porušenie povinností vyplývajúcich z kontroly nad dodržiavaním

¹¹ Celkový počet podaní a podnetov v roku 2024 bol 9239.

¹² TOMŠEJ J. Diskriminace na pracovišti, s. 147

¹³ HAMÁČKOVÁ M. Obťažovaní a šikana na pracovišti a jak je řešit. s. 60

¹⁴ § 7 ods. 8 písm. c) zákona č. 125/2006 Z. z.

¹⁵ Subjekty pre rovnaké zaobchádzanie boli prvýkrát upravené v smernici č. 2000/43/ES. V Slovenskej republike patrí kompetencia Slovenskému národnému stredisku pre ľudské práva.

¹⁶ § 12 ods. 1 zákona č. 125/2006 Z. z. písm. a) a d).

¹⁷ § 8 ods. 1 zákona č. 125/2006 Z. z.

¹⁸ § 12 ods. 2 písm. a) a b) zákona č. 125/2006 Z. z.

¹⁹ § 15 zákona č. 125/2006 Z. z.

²⁰ § 19 ods. 1, písm. a) v spojitosti s § 19 ods. 6 zákona č. 125/2006 Z. z.

zásady rovnakého zaobchádzania, ale ide aj o porušenia týkajúce sa ďalších ustanovení pracovnoprávných predpisov, resp. predpisov na zaistenie BOZP. Účinne a dostatočne vysoké sankcie by pritom mohli docieľiť, že potieranie diskriminácie by v spoločnosti bolo účinnejšie.²¹ V praxi sa totiž často stáva, že napr. pokuty za porušenie práva na rovnakú mzdu za rovnakú prácu alebo prácu rovnakej hodnoty nebývajú vôbec vysoké. Rádovo sa pohybujú v priemere vo výške 1000,- EUR.

Aktuálne bariéry efektívnej kontroly dodržiavania zásady rovnakého zaobchádzania a úvahy na zlepšenie stavu

Požiadavka na **posilnenie úloh inšpektorátov práce** sa tu vyskytla už aj v minulosti, konkrétne bola súčasťou Záverečných zistení k zlúčenej piatej a šiestej periodickej správe Slovenska Výboru pre odstránenie diskriminácie žien (CEDAW) z roku 2015. Výbor vyjadril znepokojenie v súvislosti s ochranou žien pred sexuálnym obťažovaním a diskrimináciou na pracovisku. Podľa názoru Výboru bola situácia nedostatočná z dôvodu chýbajúcich adekvátnych nástrojov na riešenie prípadov diskriminácie. Výbor odporučil SR posilniť orgány inšpekcie práce a sankcionovať diskriminačné konanie zamestnávateľov z dôvodu tehotenstva a nadväzujúcej rodičovskej dovolenky. Výbor ďalej odporúčal zabezpečiť efektívnu implementáciu opatrení na prevenciu, monitorovanie a primeranú nápravu prípadov sexuálneho obťažovania a diskriminácie na pracovisku posilnením úloh inšpektorátov práce.²² Samozrejme vo vzťahu k týmto odporúčaniam, je potrebné vnímať aj druhú stranu mince, a tou je realita, že na Slovensku majú v porovnaní s inými členskými štátmi EÚ inšpektoráty práce pomerne široký rozsah pôsobnosti. Dozorujú o. i. aj sociálnu legislatívu v doprave, či dokonca vykonávajú dohľad nad výrobkami určenými na trh a do prevádzky. Do budúcnosti bude potrebné taktiež väčšiu pozornosť zamerať aj na tzv. mäkké zručnosti inšpektorov práce, ktoré taktiež môžu napomôcť efektívnejšiemu výkonu inšpekcie práce.

Pomerne často sa vyskytujúcim javom pri orgánoch verejnej moci, ktorý možno považovať za bariéru vo vzťahu k efektívnej kontrole je častokrát príliš formalistické vnímanie jednotlivých ustanovení právneho poriadku, resp. striktný gramatický výklad právnych noriem. Na strane druhej však inšpektorátom práce nemožno vytýkať to, že sa snažia presne identifikovať porušenie konkrétnych ustanovení právneho predpisu, keďže správne orgány musia dostatočne zistiť skutkový stav

²¹ Diskriminácia na Slovensku. Hľadanie bariér v prístupe k účinnej právnej ochrane pred diskrimináciou. S. 107

²² Záverečné zistenia k zlúčenej piatej a šiestej periodickej správe Slovenska [online]. [cit. 2025-09-28]. Dostupné na: https://www.gender.gov.sk/wp-content/uploads/2012/06/CEDAW_preklad-ZZ-SK_final.pdf

v správnom konaní²³. Uvedené by však ale nemalo byť na ujmu podávateľom podnetov. Vo svetle uvedeného sa ako nedostatok na ceste k efektívnejšej kontrole dodržiavania zásady rovnakého zaobchádzania môže javiť chýbajúce výslovné **prepojenie na antidiskriminačný zákon v zákone o inšpekcii práce**. V samotnom zákone o inšpekcii práce sa totiž takéto prepojenie v poznámke pod čiarou č. 2 nenachádza. Napriek tomu sa však prikláňame k názoru, keďže výpočet v poznámke pod čiarou je demonštratívny a v prípadoch porušenia zásady rovnakého zaobchádzania teda nemožno neaplikovať antidiskriminačný zákon, keďže ako Zákonník práce v § 13 ods. 1²⁴, tak aj zákon o štátnej službe v § 4 ods. 1 naň vyslovene odkazujú. Povinnosť dodržiavať zásadu rovnakého zaobchádzania je teda integrálnou súčasťou právnych predpisov, ku ktorým sa vykonáva inšpekcia práce.²⁵ Zároveň jednotlivé ustanovenia právneho poriadku nie je možné vnímať izolovane, ale je potrebné ich predovšetkým chápať vo vzájomnej súvislosti. V prípade obťažovania nejde nepochybne len o porušenie zásady rovnakého zaobchádzania, ale zároveň má tento jav aj negatívny vplyv na duševné zdravie, ovplyvňuje dynamiku pracovného tímu, zvyšuje absencie a znižuje produktivitu práce.²⁶ Povinnosťou zamestnávateľa je nielen dodržiavať zásadu rovnakého zaobchádzania a prijímať opatrenia na ochranu pred diskrimináciou²⁷, ale zároveň aj zabezpečovať, aby pracoviská neohrozovali bezpečnosť a zdravie zamestnancov.²⁸ Inak povedané, v takomto prípade zamestnávateľ zároveň porušil aj povinnosti vyplývajúce z predpisov na zaistenie BOZP.

Taktiež by sa inšpektoráty práce pri šetrení podnetov týkajúcich sa diskriminácie nemali uspokojiť iba so samotným vyjadrením zamestnávateľa, nakoľko je viac než pravdepodobné, že zamestnávateľ všetko poprie a zistený stav bude predstavovať len tvrdenie proti tvrdeniu. Orgány inšpekcie práce by mali preto riadne zistiť skutkový stav.²⁹

²³ POTÁŠCH, Peter, HAŠANOVÁ, Janka, VALLOVÁ, Jana, MILUČKÝ, Jozef, MEDŽOVÁ, Daniela. § 3 [Základné pravidlá konania]. In: POTÁŠCH, Peter, HAŠANOVÁ, Janka, VALLOVÁ, Jana, MILUČKÝ, Jozef, MEDŽOVÁ, Daniela. Správny poriadok. 4. vydání. Praha: C. H. Beck, 2022, s. 32.

²⁴ PLAZA J., Starý problém, nové výzvy: Diskriminácia na základe veku. s. 210

²⁵ DEBRECENIOVÁ Janka a kol. Inšpekcia práce a zásada rovnakého zaobchádzania s dôrazom na pohlavie a rod: právne rámce, bariéry, príklady dobrej praxe a odporúčania pre legislatívu, politiky a prax v SR, s.

²⁶ Harassment at work [online]. [cit. 2025-09-28]. Dostupné na: [Harassment at work - OSHwiki | European Agency for Safety and Health at Work](#).

²⁷ § 2 ods. 1 a 3 zákona č. 364/2004 Z. z.

²⁸ § 6 ods. 1, písm. d) zákona č. 124/2006 Z. z.

²⁹ Inšpektorát práce se musí zabývat celým podnětem, i námitkou diskriminace. [online]. [cit. 2025-09-28]. Dostupné na: [Inšpektorát práce se musí zabývat celým podnětem, i námitkou diskriminace | Ombudsman](#)

Modelovým príkladom, ktorý by tiež mohol tvoriť obsah podnetu podaného na príslušný inšpektorát práce by mohli byť v úvode nami spomenuté „bonusy za dochádzku“. Podmienky vyplácania bonusu za dochádzku zamestnávateľ častokrát zverejňuje v interných normách, napr. v mzdovom predpise.³⁰ V tomto prípade by sme zákonné ustanovenie, ktoré by vyslovene zakazovalo použitie dochádzkového bonusu v právnom poriadku nenašli. Napriek tomu, že ide o často sa vyskytujúci jav dochádzkové bonusy nenachádzame osobitne spomenuté ani v Správe, ktorú zverejňuje Národný inšpektorát práce ako príklady častých resp. namietaných porušení s ktorými by sa zamestnanci na inšpektorát práce obracali, resp. ktoré by boli inšpektorátmi práce sankcionované³¹. Domnievame sa však aj s prihliadnutím na názor odbornej verejnosti v ČR³², že takúto prax zamestnávateľa by mal inšpektorát práce v rámci kontroly vyhodnotiť ako nepriamo diskriminačnú a teda v protokole o výsledku inšpekcie práce by mohol konštatovať porušenie § 13 ods. 1 Zákonníka práce, ktorý odkazuje na antidiskriminačný zákon.

Zlepšenie stavu rovnosti v odmeňovaní za rovnakú prácu alebo prácu rovnakej hodnoty (a tým pádom aj kontrolu v tejto oblasti) je možné očakávať v blízkej budúcnosti a to najmä v súvislosti s transpozíciou smernice 2023/970, ktorou sa posilňuje uplatňovanie zásady rovnakej odmeny pre mužov a ženy za rovnakú prácu alebo prácu rovnakej hodnoty prostredníctvom transparentnosti odmeňovania a mechanizmov presadzovania, ktorej cieľom je zlepšiť efektivitu kontroly dodržiavania zákazu diskriminácie aj inšpektorátmi práce.³³ Po novom by na inšpektoráty práce mala prejsť kompetencia v oblasti kontroly pracovnej inzercie³⁴, ktorú doposiaľ mali úrady a Ústredie práce, sociálnych vecí a rodiny.³⁵

³⁰ Pozri Zmena vo vyplácaní dochádzkového bonusu [online]. [cit. 2025-09-28]. – Dostupné na: <https://www.podbrezovan.sk/zmena-vo-vyplacani-dochadzkového-bonusu/>

³¹ Národný inšpektorát práce. Informatívna správa o diskriminácii a rodovej rovnosti v pracovnoprávných vzťahoch za rok 2024 [online]. [cit. 2025-09-28]. Dostupné na: <https://www.ip.gov.sk/diskriminacia-a-rodova-rovnost-v-pracovnopravnych-vztahoch/>

³² TOMŠEJ J., Dochádzkové bonusy: motivační nástroj na tenkém lede. [online]. [cit. 2025-09-28]. Dostupné na: <https://rovnaodmena.cz/dochazkove-bonusy-motivacni-nastroj-na-tenkem-lede/>

³³ Šestáková, Barbora. Plaza, Juraj. Rozdielna pláca za rovnakú prácu: gender pay gap na Slovensku. In: Milníky práva v stredoeurópskom priestore 2024 [elektronický dokument] / Ťažká, Veronika [Zostavovateľ]. 1. vyd. Bratislava (Slovensko) : Univerzita Komenského v Bratislave, 2024. [online]. [cit. 2025-09-28]. Dostupné z: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/Milniky_zborniky/Milniky_2024.pdf

³⁴ Pozri LP/2025/475 [online]. [cit. 2025-09-28]. – Dostupné na: <https://www.slovlex.sk/pripomienky/legislativne-procesy/SK/LP/2025/475/pripomienky/zobraz>

³⁵ § 62 ods. 2 zákona č. 5/2004 Z. z. o službách zamestnanosti

Nelegislatívne opatrenia za účelom efektívnejšej kontroly dodržiavania povinností

Na ceste k efektívnejšej kontrole dodržiavania povinností vyplývajúcich zo zásady rovnakého zaobchádzania nemožno opomenúť ani nelegislatívne návrhy.

Podľa nášho názoru prvým by mohlo byť **špecifické zameranie jednej z kontrolných úloh** v rámci Plánu hlavných úloh pre konkrétny rok, čím by sa akcentovala dôležitosť kontroly v tejto oblasti.³⁶

Ďalším krokom pre zlepšenie efektivity kontrol by v tejto oblasti malo byť aj **vytvorenie** a následne **používanie osobitnej Metodiky** zameranej na kontrolu dodržiavania zásady rovnakého zaobchádzania.³⁷ Metodika pre inšpektoráty práce na zisťovanie a posudzovanie prípadov diskriminácie so zameraním na rodovú diskrimináciu³⁸ síce bola jedným z výstupov Národného projektu Prevencia a eliminácia rodovej diskriminácie, no do aplikačnej praxe orgánov verejnej moci sa žiaľ nedostala.

Zároveň je potrebné do budúcnosti uvažovať aj o **posilnení doterajšej spolupráce** so Slovenským národným strediskom pre ľudské práva a pokračovaní vo využívaní existujúcej podpory, ktorú ponúka Európsky orgán práce členským štátom, ktorou sú napr. študijné návštevy za účelom získania dobrej praxe z iných členských štátov.

V neposlednom rade je dôležitým faktorom pre zlepšenie efektivity kontrol aj neustále **zvyšovanie povedomia** verejnosti o tom, tzn. realizovanie osvetových aktivít o tom čo je a čo nie je možné považovať za diskrimináciu³⁹, resp. iných aktivít ako sú napr. raňajky so zamestnávateľmi aj na tieto témy Totižto nielen dôkladná kontrolná činnosť, ale aj preventívne aktivity vedia prispieť k zvýšeniu dodržiavania príslušných ustanovení právnych predpisov, ktoré sa týkajú zásady rovnakého zaobchádzania.⁴⁰

Záver

Diskriminácia predstavuje nežiadúci jav, ktorí sa častokrát vyskytuje na rôznych pracoviskách. Jednou z možností, ako sa môžu voči nej zamestnanci brániť je podanie

³⁶ Plán hlavných úloh na rok 2024. Dostupné na: <https://www.ip.gov.sk/narodny-inspektorat-prace-predstavuje-plan-hlavnych-uloh-na-rok-2024/>

³⁷ Vytvorenie Metodiky sa predpokladá v súvislosti s transpozíciou smernice 2023/970.

³⁸ LAJČÁKOVÁ J., Metodika pre inšpektoráty práce na zisťovanie a posudzovanie prípadov diskriminácie so zameraním na rodovú diskrimináciu. [online]. [cit. 2025-09-28]. Dostupné z: [metodika_pre_inspektoraty_prace_zistovanie_diskriminacie.pdf](#)

³⁹ LAJČÁKOVÁ J., Metodika pre inšpektoráty práce na zisťovanie a posudzovanie prípadov diskriminácie so zameraním na rodovú diskrimináciu. S. 41 [online]. [cit. 2025-09-28]. Dostupné z: [metodika_pre_inspektoraty_prace_zistovanie_diskriminacie.pdf](#)

⁴⁰ ŠIMEČKOVÁ Eva. Nežiadoucí chování na pracovišti: šikana, diskriminace, monitorování, whistleblowing. S. 142

podnetu či už priamo alebo prostredníctvom zástupcov zamestnancov na inšpektorát práce.

Domnievame sa, že inšpektoráty práce majú v oblasti kontroly dodržiavania zásady rovnakého zaobchádzania kompetencie pre efektívny výkon kontroly v súčasnosti upravené dostatočne. Napriek tomu však stále pretrvávajú určité bariéry vo vzťahu k efektívnej kontrole, čo potvrdzujú aj verejne dostupné dáta. Najdôležitejšou prekážkou vo vzťahu k účinnejšej kontrole podľa nášho názoru inšpektoráty práce je predovšetkým chýbajúca osobitná metodika pre výkon kontroly v tejto oblasti. Určitý posun vpred by v tomto smere mala priniesť transpozícia smernice 2023/970.⁴¹ Samozrejme, mohli by sme uvažovať aj o zintenzívnení vzdelávania odborných kapacít inšpektorátov práce, resp. uchádzačov, avšak pri týchto úvahách je potrebné vnímať aj druhú stránku a tou je stále pomerne široký rozsah pôsobnosti, ktorá je inšpektorátom práce v Slovenskej republike zverená.

Domnievame sa však, že pre posun v tejto téme by mal byť kľúčovým o. i. aj častejší diskurz v tejto problematike a zvyšovanie povedomia u širokej verejnosti o diskriminácii ako takej a o možnostiach ochrany pred ňou.

Zoznam použitej literatúry

1. BARANCOVÁ, Helena a kol. Zákoník práce. Komentár. 3. vydanie. Bratislava: C. H. Beck, 2022, S. 1624
2. DEBRECENIOVÁ, Janka a kol. Inšpekcia práce a zásada rovnakého zaobchádzania s dôrazom na pohlavie a rod: právne rámce, bariéry, príklady dobrej praxe a odporúčania pre legislatívu, politiky a prax v SR. Bratislava: Centrum vzdelávania MPSVR SR, 2014, S. 138. ISBN 978-80-969824-3-1.
3. Diskriminácia na Slovensku. Hľadanie bariér v prístupe k účinnej právnej ochrane pred diskrimináciou. Košice: Poradňa pre občianske a ľudské práva, 2012. S. 107 ISBN 978-80-97052-1-6.
4. HAMÁČKOVÁ M. Obtěžování a šikana na pracovišti a jak je řešit. Zákaz diskriminace v pracovním právu. Praha: Univerzita Karlova, Právnická fakulta, 2022, S. 60. ISBN 978-80-7630-022-4.
5. LAJČÁKOVÁ Jarmila. Metodika pre inšpektoráty práce na zisťovanie a posudzovanie prípadov diskriminácie so zameraním na rodovú diskrimináciu. Inštitút pre výskum práce a rodiny 2020. S. 41 [online]. [cit. 2025-09-28]. Dostupné z:

metodika_pre_inspektoraty_prace_zistovanie_diskriminacie.pdf

⁴¹ NEVICKÁ, Denisa. LADIVEROVÁ, Eva. Is the right to equal pay for equal work or work of equal value distant reality or only utopia? The Lawyer Quarterly. 2022, roč. 12, č. 3, s. 282–289. ISSN 1805-840X. Dostupné z: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/519>

6. MEDZINÁRODNÁ ORGANIZÁCIA PRÁCE. Labour inspection and non-discrimination. Ženeva: ILO, september 2022. [online]. [cit. 2025-09-28]. Dostupné na: <https://www.ilo.org/resource/training-material/labour-inspection-and-non-discrimination>
7. Národný inšpektorát práce. Informatívna správa o diskriminácii a rodovej rovnosti v pracovnoprávných vzťahoch za rok 2024 [online]. [cit. 2025-09-28]. Dostupné na: <https://www.ip.gov.sk/diskriminacia-a-rodova-rovnost-v-pracovnopravnych-vztahoch/>
8. NEVICKÁ, Denisa. LADIVEROVÁ, Eva. Is the right to equal pay for equal work or work of equal value distant reality or only utopia? The Lawyer Quarterly. 2022, roč. 12, č. 3, s. 282–289. ISSN 1805-840X. Dostupné z: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/519>
9. POTÁSCH, Peter, HAŠANOVÁ, Janka, VALLOVÁ, Jana, MILUČKÝ, Jozef, MEDŽOVÁ, Daniela. Správny poriadok. 4. vydání. Praha: C. H. Beck, 2022, S. 32 ISBN 978-80-7400-908-2
10. PLAZA, Juraj. Starý problém, nové výzvy: Diskriminácia na základe veku Acta Facultatis Iuridicae Universitatis Comenianae [online]. 2025, roč. XLIV, č. 1, s. 200–222. ISSN 1336-6912. [cit. 28. 9. 2025]. Dostupné na : <https://doi.org/10.62874/afi.2025.1.10>
11. ŠIMEČKOVÁ Eva. Nežadoucí chování na pracovišti: šikana, diskriminace, monitorování, whistleblowing. Praha: Leges, 2023. S. 142. ISBN 978-80-7502_698-9.
12. TOMŠEJ, Jakub. Dochádzkové bonusy: motivační nástroj na tenkém lede. [online]. [cit. 2025-09-28]. Dostupné na: <https://rovnaodmena.cz/dochazkove-bonusy-motivacni-nastroj-na-tenkem-lede/>
13. TOMŠEJ, Jakub. Diskriminace na pracovišti. Praha: Grada Publishing, a.s., 2020, S. 147. ISBN 978-80-271-1014-8.
14. ŠESTÁKOVÁ, Barbora. PLAZA, Juraj. Rozdielna pláca za rovnakú prácu: gender pay gap na Slovensku. In: Milníky práva v stredoeurópskom priestore 2024. Ťažká, Veronika [Zostavovateľ]. 1. vyd. Bratislava (Slovensko) : Univerzita Komenského v Bratislave, 2024. [online]. [cit. 2025-09-28]. Dostupné z: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/Milniky_zborniky/Milniky_2024.pdf

Kontaktné údaje

JUDr. Marián Lizanec

Marian.lizanec@employment.gov.sk

Ministerstvo práce, sociálnych vecí a rodiny SR

SPRAVEDLIVÉ ODMĚŇOVÁNÍ (NEJEN) V DIGITÁLNÍM VĚKU Z POHLEDU ČESKÉ LEGISLATIVY A JUDIKATURY¹

FAIR REMUNERATION (NOT ONLY) IN THE DIGITAL AGE FROM THE POINT OF VIEW OF CZECH LEGISLATION AND JURISPRUDENCE

Jakub Morávek²

Abstrakt: Text se zaměřuje na problematiku spravedlivého odměňování. Pojednává o smyslu a účelu evropské právní regulace v podobě směrnice Rady 75/117/EHS ze dne 10. února 1975 o sbližování právních předpisů členských států týkajících se uplatňování zásady stejné odměny za práci pro muže a ženy, která byla později nahrazena směrnicí Evropského parlamentu a Rady 2006/54/ES ze dne 5. 7. 2006 o zavedení zásady rovných příležitostí a rovného zacházení pro muže a ženy v oblasti zaměstnání a povolání. Na to navazuje vymezení smyslu a účelu právní úpravy spravedlivého odměňování v právním řádu České republiky.

Autor poukazuje na právní úpravu České republiky a na její problematické aspekty. Pokládá si otázku, zda z hlediska zákonné úpravy existuje stejná práce a práce stejné hodnoty. Dále poukazuje na procesněprávní aspekty problematiky a na související problémy civilního a přestupkového řízení.

Platnou právní úpravu hodnotí z hlediska testu proporcionality a pokládá si otázku, zda lze očekávat nápravu stávajících nedostatků při příležitosti transpozice směrnice Evropského parlamentu a Rady (EU) 2023/970 ze dne 10. května 2023 o posílení uplatňování zásady stejné odměny za stejnou nebo rovnocennou práci mezi muži a ženami prostřednictvím mechanismů transparentnosti odměňování a vymáhání.

Závěrem autor připojuje souhrnné hodnocení a úvahy *de lege ferenda*.

Klíčové slová: pracovní právo; spravedlivá odměna; transparentní odměňování; zákaz diskriminace

¹Příspěvek vznikl díky podpoře poskytované v rámci výzkumného projektu Cooperatio/SOC/LAWS 10 „Labour Law and Social Security Law“ a zohledňuje stav právní úpravy ke dni 27. září 2025.

² Autor působí na katedře pracovního práva a práva sociálního zabezpečení Právnické fakulty Univerzity Karlovy jako docent. Je vedoucím katedry pracovního práva a práva sociálního zabezpečení Právnické fakulty Západočeské univerzity v Plzni, místopředsdou České společnosti pro pracovní právo a právo sociálního zabezpečení a advokátem v Praze.

Abstract: The text is focussed on the issue of fair remuneration. It examines the rationale and objectives underlying European legal regulation, specifically Council Directive 75/117/EEC of 10 February 1975 on the approximation of the laws of the Member States relating to the application of the principle of equal pay for men and women, which was subsequently repealed and replaced by Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation. This analysis is followed by a delineation of the purpose and intent of the legal framework governing fair remuneration within the Czech legal system. The author draws attention to the Czech Republic's legislative framework and its problematic aspects. He poses the question of whether, under the applicable statutory provisions, the concepts of "equal work" and "work of equal value" are adequately defined and distinguished. Furthermore, the text highlights procedural legal issues and related challenges arising in civil and administrative infraction proceedings. The current legal regulation is assessed through the lens of the proportionality test, and the author considers whether the transposition of Directive (EU) 2023/970 of the European Parliament and of the Council of 10 May 2023—on strengthening the application of the principle of equal pay for equal or equivalent work between men and women through pay transparency and enforcement mechanisms—may serve as an opportunity to rectify existing deficiencies. In conclusion, the author provides a comprehensive evaluation and presents *de lege ferenda* considerations.

Key words: labour law; fair remuneration; transparent remuneration; prohibition of discrimination

Úvod

Česká republika si, zdá se, definitivně ujednotila stanovisko k transpozici evropské legislativy, nejméně jde-li o právní úpravu pracovněprávních vztahů. Její pozici by bylo možné stručně charakterizovat jako: „*pozdě ale přece, gold plating však v každém případě*“.

Odklon od tohoto trendu není (bohužel) důvod očekávat ani v případě směrnice Evropského parlamentu a Rady (EU) 2023/970 ze dne 10. května 2023 o posílení uplatňování zásady stejné odměny za stejnou nebo rovnocennou práci mezi muži a ženami prostřednictvím mechanismů transparentnosti odměňování a vymáhání, u níž je transpoziční lhůta stanovena na 7. června 2026.

Podle Plánu legislativních prací vlády na rok 2024³ měl být návrh transpozičního zákona předložen místopředsedou vlády a ministrem práce a sociálních věcí Vládě České republiky v květnu 2024. Účinnost byla plánována od ledna 2025. To se však ukázalo být pro ministerskou legislativu, která se pravděpodobně vyčerpala na, upřímně řečeno z velké části zbytečné,⁴ tzv. flexibilizační novele zákoníku práce přijaté v roce 2025,⁵ jako příliš ambiciózní a v konečném důsledku jako nezvladatelný úkol.

Návrh zákona tak nebyl předložen Vládě České republiky (a z povahy věci tedy ani Poslanecké sněmovně Parlamentu České republiky) ani v květnu roku 2024, ani v květnu roku 2025 a ani na žádném dalším jednání až do dnešního dne.

Byť na návrhu úřednický aparát Ministerstva práce a sociálních věcí pracuje a podle kuloárových informací by měl být hotov v říjnu tohoto roku, širší odborné veřejnosti k odborné opONENTUŘE prozatím nic poskytnuto nebylo a s vysokou mírou pravděpodobnosti ani nebude, neboť přístup ministerské legislativy posledních let by bylo možné charakterizovat jako „*názor akademiků a ani praktiků (až na pár vybraných) nás nezajímá, zvládneme to sami, a když se to náhodou zase nepovede, v brzké době předpis párkrát znovelizuje, dokud nebude úprava nějak životaschopná*“.⁶ Funkční období Poslanecké sněmovny Parlamentu České republiky končí na podzim roku 2025. V říjnu se konají parlamentní volby.

Za těchto okolností se zachování transpoziční lhůty směrnice 2023/970, tj. 7. červen 2026, zdá být spíše jako nepravděpodobné.

Pokud bude zákon přece jen bezprostředně po volbách přijat tak, aby nabyl účinnosti včas, pak jediné (opět – nikoli výjimečně) v aranžmá, kdy projde legislativním procesem s příznakem „*povinná evropská regulace na hraně termínu, nesahat*“, tedy bez připomínek v podobě zpracované ministerstvem a předložené Vládou.

³ Plán legislativních prací vlády pro rok 2024 viz <https://vlada.gov.cz/scripts/detail.php?id=211219&tmplid=50>

⁴ V této souvislosti v podrobnostech viz například MORÁVEK, J. Výpovědní doba z hlediska „flexibilizační“ novely zákoníku práce In MORÁVEK, J. (ED.) Zákoník práce a sociální zabezpečení 2024. Praha: Právnická fakulta Univerzity Karlovy. 2024. s. 51-62, MORÁVEK, J. Nejen k pracovnímu poměru na dobu určitou z hlediska novely zákoníku práce In BŘEZINY, P., CVRČEK, F. (EDS.) Metamorfózy práva ve střední Evropě VIII. Alfeus a Augiášův chlév. Plzeň: Právnická fakulta Západočeské univerzity v Plzni. 2024. s. 382-404, nebo VYSOKAJOVÁ, M. Tzv. flexinovela zákoníku práce. Praha: Wolters Kluwer. 2025. sv. 5. s. 5 an.

⁵ Zákon č. 120/2025 Sb., kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a některé další zákon

⁶ V této souvislosti lze poukázat například na ust. § 324a zákoníku práce, který nabyl účinnosti 1. ledna 2024, aby byla následně 1. srpna téhož roku novelizován.

Bez znalosti podoby návrhu těžko hodnotit, zda by takový přístup ke schvalování byl ku prospěchu anebo spíše ke škodě; zkušenost s několika posledními legislativními počiny však hovoří spíše pro druhou z variant.⁷

Nelze přitom pominout, že na potřebu včas přistoupit k diskusi o přípravě transpoziční legislativy bylo v rámci kulatých stolů pořádaných Ministerstvem práce a sociálních věcí poukazováno v diskusím ke stávající a budoucí pracovněprávní legislativě již na přelomu května a června 2023.⁸

Důvodem volání po široké a podrobné odborné diskusi přitom nebyla jen nová evropská legislativa a zájem o její efektivní a racionální transpozici, nýbrž i (stále aktuální) judikatura Nejvyššího soudu České republiky⁹ vztahující se k zásadě rovného odměňování, jmenovitě k ust. § 110 zákona č. 262/2006 Sb., zákoník práce,¹⁰ dle něž *„za stejnou práci nebo za práci stejné hodnoty přísluší všem zaměstnancům u zaměstnavatele stejná mzda, plat nebo odměna z dohody.“*

Připomeňme, že rozhodnutí a přístup Nejvyššího soudu České republiky (srov. zejména Nejvyšší soud ve věci sp. zn. 21 Cdo 3955/2018), z jistého hlediska potvrzený navazujícím rozhodnutím Ústavního soudu České republiky (srov. Ústavní soud ve věci sp. zn. I. ÚS 2820/20), byl v rámci odborného diskurzu podroben kritice.¹¹

Odbornou veřejností bylo mj. poukazováno na to, že Nejvyšší soud:

- byť k tomu měl i s přihlédnutím ke své dřívější judikatuře vztahující se primárně k rozvázání pracovního poměru (dle ust. § 52 písm. a) a b) ZPr) prostor, pojem „zaměstnavatel“ v ust. § 110 ZPr nijak nekorigoval a nevztáhl jej k organizační složce (závodu) zaměstnavatele, naopak jej vyložil zcela obecně, čehož je důsledkem, že povinnost poskytovat stejnou odměnu za stejnou práci a práci stejné hodnoty tíží zaměstnavatele napříč závody, ať již se nacházejí (prozatím jen v České republice) kdekoli;

⁷ Srov. op. cit. sub. 4.

⁸ Diskuse se zástupci odborné veřejnosti bez bližší charakteristiky jejich obsahu zmiňuje mj. důvodová zpráva k zákonu č. 120/2025 Sb. – viz Parlament České republiky, Poslanecká sněmovna. 9. volební období. tisk 775/0, část závěrečné zprávy RIA s. 2.

⁹ Primárně se jedná o rozhodnutí Nejvyššího soudu ve věci sp. zn. 21 Cdo 3955/2018.

¹⁰ Dále jen ZPr

¹¹ Viz například ŠTEFKO, M. Mzdová (ne)svoloba zaměstnavatele v judikatuře českých soudů. Právní rozhledy, 2022, č. 17, s. 598-602 a dále MORÁVEK, J. Ke spravedlivému odměňování v pracovněprávních vztazích. Právní rozhledy, 2020, č. 20, s. 705-709, MORÁVEK, J. Spravedlivé odměňování po Česku In Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia / NIKOLA BEŽÁKOVÁ, ÁDÁM SÍPOS, VERONIKA ŤAŽKÁ (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 233 s. ISBN 978-80-7160-698-7., s. 6 – 17.

- nereflexuje smysl a účel evropské právní úpravy,¹² která má být odkazovaným ustanovením transponována, a tedy ani smysl a účel rozhodné zákonné úpravy (viz bod 1 níže),
- ve svých úvahách a argumentaci pomíjí realitu mezinárodního působení právnických osob,¹³
- přehlíží hospodářskou realitu a vnější okolnosti stejně jako individualitu a s ní související fakt, že zaměstnanec může být pro zaměstnavatele cenný z řady důvodů a jím odvedená práce může být jen jedním z nich,
- nereflexuje, že cílem racionálního zákonodárce nemůže být unifikovat cenu práce napříč republikou bez ohledu na regionální rozdíly a v konečném důsledku tak zlikvidovat konkurenceschopnost vůči zahraničí a přivodit (i kvůli tomu) ukončení činnosti nezanedbatelného počtu zaměstnavatelů.

Nad to se v návaznosti na pandemii COVID-19 a následné legislativní změny zejména v oblasti výkonu práce mimo pracoviště zaměstnavatele (práce na dálku) objevily i další aspekty a momenty, které by bylo minimálně vhodné při nastavování podoby legislativy v oblasti spravedlivého odměňování reflektovat.

Předložený příspěvek se věnuje vybraným otázkám právní úpravy spravedlivého odměňování v České republice s přihlédnutím k aspektům souvisejícím s výkonem práce mimo pracoviště zaměstnavatele, konkrétně z bydliště. Ke stávající právní úpravě a zejména jejímu výkladu ze strany Nejvyššího soudu České republiky se jeho prostřednictvím připojují kritické poznámky a spolu s tím se předkládají související úvahy *de lege ferenda* stavící na výchozích maximách demokratického právního státu a (což spolu úzce souvisí) předpokladech fungování hospodářství v globálním kontextu.

Smysl a účel právní úpravy – ztraceno v překladu?

Nikoli výjimečně v základu jednoznačný (a bohužel) účel sledovaný při přijímání právní úpravy projde postupem času (třeba i nechtěně a nepřímou v důsledku novelizací textace právního předpis) řadou obrátů, posunů a proměn, až se zcela vytratí, anebo je překryt či negován tolika souvisejícími a jinými dílčími efekty a cíli, až se stane marginálním a lze jej identifikovat jen obtížně.

¹² Primárně se jedná o směrnici Rady 75/117/EHS ze dne 10. února 1975 o sbližování právních předpisů členských států týkajících se uplatňování zásady stejné odměny za práci pro muže a ženy, která byla později nahrazena směrnicí Evropského parlamentu a Rady 2006/54/ES ze dne 5. 7. 2006 o zavedení zásady rovných příležitostí a rovného zacházení pro muže a ženy v oblasti zaměstnání a povolání.

¹³ Viz MORÁVEK, J. Ke spravedlivému odměňování v pracovněprávních vztazích. Právní rozhledy, 2020, č. 20, s. 705-709, MORÁVEK, J. Spravedlivé odměňování po Česku In Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia / NIKOLA BEZÁKOVÁ, ÁDÁM SÍPOS, VERONIKA ŤAŽKÁ (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 233 s. ISBN 978-80-7160-698-7., s. 6 - 17

Takový osud do značné míry, zdá se, stihl i českou právní úpravu spravedlivého odměňování, jde-li o odměnu za stejnou práci a za práci stejné hodnoty, jak je obsažena v ust. § 110 ZPr.

Zákonné ustanovení je v základu transpozicí evropské legislativy, konkrétně směrnice Rady 75/117/EHS ze dne 10. února 1975 o sbližování právních předpisů členských států týkajících se uplatňování zásady stejné odměny za práci pro muže a ženy, která byla později nahrazena směrnicí Evropského parlamentu a Rady 2006/54/ES ze dne 5. 7. 2006 o zavedení zásady rovných příležitostí a rovného zacházení pro muže a ženy v oblasti zaměstnání a povolání.

Již podle názvu je patrné, že primárním cílem evropské legislativy je eliminovat nedůvodné rozdíly v odměňování mužů a žen a nikoli zajišťovat obecnou rovnost v odměňování. Na této základní tezi a základním cíli se nic nemění ani s přijetím směrnice 2023/970.

Při zohlednění:

- principu subsidiarity a proporcionality, jako výchozích předpokladů evropské regulace,
- socioekonomické reality a odlišné hospodářské vyspělosti a bohatství jednotlivých evropských regionů v době přípravy a vydání směrnic stejně jako dnes,
- potenciálu pracovních sil a ceny práce jak mezi členskými státy, tak v jejich rámci v jednotlivých regionech,
- faktu, že odměna za práci by v tržním hospodářství měla odrážet cenu práce na relevantním trhu, jímž může být v globalizovaném světě nikoli jen území státu,
- skutečnosti, že unifikace odměňování může mít (kvůli narušení trhu) za důsledek ztrátu lokální i globální konkurenceschopnosti kvůli zvýšení ceny práce,
- faktu, že unifikace odměn může vést ke snížení iniciačního a inovačního potenciálu kvůli potlačení motivace,

není důvod se domnívat, že by v liberálně demokratickém hodnotovém systému mělo být cílem racionálního evropského či českého zákonodárce pravidlo o stejné odměně za stejnou práci a práci stejné hodnoty napříč všemi organizačními složkami (závody) zaměstnavatele ať již napříč unií nebo i jen napříč jediným členským státem, v jehož rámci existují relevantní regionální rozdíly v životních nákladech a dalších faktorech ovlivňujících cenu práce.

Uvedený závěr staví dále na tom, že primárním smyslem právní úpravy má být odstranit zásahy do osobnostní sféry mužů a žen způsobené rozdíly v jejich odměňování za stejnou práci a práci stejné hodnoty, jejichž důvodem je pouze pohlaví; v zásadě shodné lze vztáhnout i na ostatní možné obecné diskriminační znaky.

Jinak řečeno, v jádru by měla být předmětná právní úprava odrazem vážení mezi na jedné straně zásahem do lidské důstojnosti způsobeným nedůvodným rozdílem mezi výší odměny za stejnou práci a práci stejné hodnoty a na druhé straně veřejným zájmem v podobě zachování tržních principů a funkčního tržního hospodářství (nepřímo tudíž i ochrany pracovních míst), při reflexi vedlejšího negativního projevu spočívajícího v potlačení autonomie vůle, zásahu do majetkové sféry zaměstnavatele a principu, že každý má právo brát se o své štěstí.

V testu proporcionality¹⁴ může pravidlo o stejné odměně za stejnou práci a práci stejné hodnoty obstát pouze na lokální úrovni, neboť (pokud je formulováno tak, aby mohlo fungovat efektivně – výhrady k ust. § 110 ZPr viz bod 2) jde o opatření

- vhodné k prevenci nedůvodného zásahu do osobnostní sféry,
- nutné, kdy není jiné, méně invazivní řešení z hlediska základních práv a svobod a veřejného zájmu, a
- přiměřené, když negativní projevy a efekty (potlačení zejména autonomie vůle a osobní iniciativy, zásahu do majetkové sféry zaměstnavatele) jsou vyváženy ochranou osobnostních práv a důstojnosti zaměstnance.

V režimu svobodného trhu, mimo centrálně plánovanou ekonomiku, záměr zajistit stejnou odměnu za stejnou práci a práci stejné hodnoty napříč pracovišti/závody, resp. organizačními složkami zaměstnavatele napříč unií či jen členským státem sestávajícím se z hospodářsky odlišně silných regionů, v testu proporcionality zcela jistě neobstojí; ve třetím kroku testu, zjednodušeně řečeno, nemůže zásah do osobnostní sféry, který je oslaben geografickou vzdáleností, ale i vědomostí o regionálních rozdílech, převážit zásah do majetkové sféry zaměstnavatele plynoucí z pokřivení působení tržních mechanismů spolu právě s ohrožením fungování trhu a hospodářství (narušení mechanismu určování ceny práce v daném místě).

Pod prizmatem naznačených cílů evropské právní úpravy (tedy restriktivně) by z povahy věci mělo být vykládáno i ust. § 110 ZPr, a to i přes to, že jak textace ustanovení, tak důvodová zpráva, dle které „*aplikace zásady stejné mzdy za stejnou práci nebo za práci stejné hodnoty je vztažena na všechny zaměstnance u jednoho zaměstnavatele. Zaměstnanec může požadovat za stejnou práci nebo za práci stejné hodnoty stejnou odměnu pouze v rámci svého zaměstnavatele*“,¹⁵ nabízí prostor pro extenzivní výklad.

K nabízenému prostoru pro *gold plating* vedoucímu z jistého úhlu pohledu ke snaze o (absurdní) absolutní rovnost se ve shora zmíněném rozhodnutí *de facto* přihlásil Nejvyšší soud. To se však ze sebezáchovných důvodů pro konkurenceschopnost českého hospodářství a fungování zdejší ekonomiky (zejména, jde-li o globální konkurenceschopnost z hlediska ceny práce) a z řady dalších důvodů, které byly

¹⁴ Srov. například Ústavní soud České republiky ve věci sp. zn. Pl. ÚS 4/94.

¹⁵ Parlament ČR, Poslanecká sněmovna, 2002–2006, tisk č. 1153/0.

v podrobnostech rozebrány na jiném místě,¹⁶ zdá být (jako u řady dalších otázek řešených Nejvyšším soudem České republiky v posledních letech)¹⁷ výstřel na slepo.

Existuje stejná práce a práce stejné hodnoty?

Nejvyšší soud České republiky ve své judikatuře, stejně jako inspektoráty práce ve své kontrolní činnosti se prozatím omezují, jde-li o stejnou práci a práci stejné hodnoty, téměř výlučně na posuzování shodnosti práce ve smyslu předmětu a způsobu jejího výkonu; v případě České pošty (NS ve věci sp. zn. 21 Cdo 3955/2018) šlo v základu o to, že druhem práce dotčeného zaměstnance byl řidič s kódovým označením (432050), a shodný druh práce měli i zaměstnanci v jiných regionech, včetně Prahy, přičemž stěžejní otázkou z hlediska předmětu řízení bylo, zda se práce řidiče se shodným kódovým označením vykonávaná zaměstnanci v různých regionech liší z hlediska složitosti, odpovědnosti a namáhavosti.

Ust. § 110 ZPr však povinnost poskytnout srovnatelnou odměnu nevztahuje pouze k situaci, kdy zaměstnanci vykonávají stejnou práci z hlediska jejího předmětu. Povinností zaměstnavatele je poskytovat stejnou odměnu i zaměstnancům, kteří vykonávají práci stejné hodnoty.¹⁸

Pokud by tehdy (hypoteticky) z hlediska zákonem předepsaných hodnotících kritérií byla jako práce stejné hodnoty vyhodnocena práce sekretářky statutárního zástupce a na druhé straně práce vedoucího účetního oddělení, měla by být odměna obou zaměstnanců totožná.

Nedostatečnou iniciativu ve směru k využití plné šíře právní úpravy lze v tomto případě spíše kvitovat.

Zákonná úprava v ust. § 110 ZPr uvádí řadu kritérií pro posouzení stejnosti prací, resp. pro posouzení hodnoty práce, přičemž textace zákonného ustanovení vede k závěru o jejich souborném kumulativním uplatnění.¹⁹

Z hlediska ust. § 110 ZPr není bez významu, že směrnice 75/117/EHS a ani směrnice 2006/54/ES obdobný výčet hodnotících kritérií neobsahuje, tzn. jde o iniciativu zdejšího zákonodárce (ministrské legislativy).

Hodnotícími kritérii jsou:

¹⁶ Viz MORÁVEK, J. Spravedlivé odměňování po Česku In Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia / NIKOLA BEZÁKOVÁ, ÁDÁM SÍPOS, VERONIKA ŤAŽKÁ (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 233 s. ISBN 978-80-7160-698-7., s. 6 - 17

¹⁷ Viz například rozhodnutí Nejvyššího soudu ve věci 21 Cdo 2523/2022.

¹⁸ Z kritérií pro hodnocení shodnosti práce se mj. podává, že linii absolutní objektivní hodnota práce – subjektivní relativní hodnota práce, tj. hodnota, kterou práci konkrétního zaměstnance přisuzuje zaměstnavatel, by měl být rozhodující prvý z uvedených významů.

¹⁹ Shodně srov. ROTHOVÁ, E.. In: BĚLINA, M., DRÁPAL, L. a kol. Zákoník práce. 4. vydání. Praha: C. H. Beck, 2023, s. 708, marg. č. 4.

- a) složitost práce;
- b) odpovědnost spojená s prací;
- c) namáhavost práce;
- d) pracovní podmínky, při nichž se práce koná;
- e) pracovní výkonnost;
- f) výsledky práce.

Z hlediska zaměření tohoto příspěvku je přitom rozhodující, že:

- složitost, odpovědnost a namáhavost práce se posuzuje mj. i podle fyzické, smyslové a duševní zátěže a působení negativních vlivů práce, a dále, že
- pracovní podmínky se posuzují podle obtížnosti pracovních režimů vyplývajících z rozvržení pracovní doby, například do směn, dnů pracovního klidu, na práci v noci nebo práci přesčas, podle škodlivosti nebo obtížnosti dané působením jiných negativních vlivů pracovního prostředí a podle rizikovosti pracovního prostředí.

Pracovním prostředím v obecném smyslu slova lze přitom rozumět veškeré podmínky a vlivy (prostředí i sociální – hluk, prašnost, teplota, stres atd.), při nichž dochází k výkonu práce.

U stejných prací vykonávaných na jednom pracovišti tak bude mít kritérium pracovního prostředí z povahy věci spíše zanedbatelný význam. Nijak tomu ovšem může být při stejných prací vykonávaných na různých pracovištích, anebo u prací různé hodnoty.

Prozatím jednou z mnoha judikaturou neřešených otázek je význam kritéria pracovních podmínek při výkonu práce mimo pracoviště zaměstnavatele, a to jak u prací, které jsou mimo pracoviště zaměstnavatele vykonávány permanentně, tak u prací, které jsou konány jak na pracovišti zaměstnavatele, tak mimo něj.

S přihlédnutím k předmětu tohoto příspěvku a současně částečně pro zjednodušení se dále zaměříme pouze na důsledek plynoucí z rozdílnosti pracovních režimů při výkonu práce z domova u prací, které jsou současně a převážně vykonávány na pracovišti zaměstnavatele.²⁰

Před pandemií COVID-19 byl výkon práce mimo pracoviště zaměstnavatele, konkrétně výkon práce z domova, spíše občasným benefitem nežli pravidelným způsobem výkonu práce u zaměstnanců, u nichž povaha práce přenesení jejího výkonu z pracoviště do bydliště umožňuje. Covidová pandemie z výkonu práce

²⁰ K výkonu práce mimo pracoviště zaměstnavatele viz ŠTEFKO, M. in BĚLINA, M. DRÁPAL, L. a kol. *Zákoník práce*. 4. vydání. Praha: C. H. Beck, 2023, s. 1407, marg. č. 1., VYSOKAJOVÁ, M. in HŮRKA, P., RANDLOVÁ, N., DOLEŽÍLEK, J., ROUČKOVÁ, D., VYSOKAJOVÁ, M., DOUDOVÁ, S., KOŠNAR, M., HORNA, V. a kol. *Zákoník práce: Komentář*. Wolters Kluwer. 2024, MORÁVEK, J. in PICHRT, J. A KOL. *Pracovní právo*. 2. vydání. Praha: C.H.Beck. 2025, s. 587, či dále také například CIBULKOVÁ, M., CHLADA, O., LANDWEHRMANN, T., PROCHÁZKOVÁ, E., VRAJÍK, M. Stanovisko CzELA k právním otázkám práce na dálku. *Právní rozhledy*, 2024, č. 22, s. 1.

z domova učinila (pravděpodobně) nejen v České republice široce rozšířený jev, který se sice někteří zaměstnavatelé s ohledem na jeho negativní aspekty (nedostatečná výkonnost, složitá organizace práce, snížený inovativní potenciál, nedostatečné budování soudržnosti pracovního kolektivu a loajality k zaměstnavateli) v poslední době snaží alespoň částečně potlačit, i tak však počet zaměstnanců vykonávající práci z bydliště dalece přesahuje stav v roce 2019.²¹

Při výkonu práce z domova se pracovní podmínky zaměstnanců mohou zásadně lišit, ať již jde o uspořádání pracoviště, o přítomnost členů domácnosti v místě, kde je práce vykonávána, či o vnější vlivy, jako je teplota, hluchost, prašnost atd. Pracovní podmínky při výkonu práce z domova přitom zaměstnavatel nemá možnost nijak významněji ovlivnit.

Bez významu z hlediska stejné odměny za stejnou práci a práci stejné hodnoty rovněž (možná – viz níže) není, že zaměstnanci vykonávající práci z domova práci nikoli výjimečně konají v pracovním režimu (rozvržení pracovní doba), který si po dohodě se zaměstnavatelem (větší či menší měrou) určují sami. Pracovní režimy jednotlivých zaměstnanců se tak mohou i nezanedbatelným způsobem různit.

Nabízí se dvě otázky:

- postačuje pro závěr o rozdílnosti prací jakákoli odlišnost v jakémkoli z hodnotících kritérií podle ust. § 110 ZPr anebo musí odlišnost dosahovat určité míry?²²
- mají mít vlivy pracovního prostředí, které zaměstnavatel nemůže ovlivnit, z hlediska ust. § 110 ZPr význam?

V odpovědi lze uvažovat v základu trojím způsobem.

První řešení *de facto* nabízí Nejvyšší soud České republiky ve shora odkazovaném rozhodnutí ve věci České pošty. Jde o striktní až textualistický přístup směřující k bezvýjimečnému uplatnění zákonných kritérií a podmínek bez jakékoli korekce či teleologické redukce.

Z tohoto hlediska postačí být jen dílčí rozdíl v jednom z hodnotících kritérií (jedna směna v kalendářním měsíci vykonávaná z domova za odlišných podmínek) a jelikož zákonná dikce výslovně nehovoří o přiměřenosti, nejedná se o stejnou práci, resp. o práci stejné hodnoty. Určení odměny je tudíž v dispozici zaměstnavatele a jediným korektivem zůstávají dobré mravy.

Druhý možný přístup, který mj. navazuje na diskuse vztahující se k absentující komplexní právní úpravy výkonu práce mimo pracoviště zaměstnavatele, jde-li o

²¹ V této souvislosti viz BUREŠOVÁ, K. Práci z domova umožňuje až 59 podniků za 100. Statistika&My. Časopis Českého statistického úřadu. On-line 27.9.2025. dostupné na <https://statistikaamy.csu.gov.cz/praci-z-domova-umoznuje-59-podniku-ze-100> 30. září [cit. 2025-9-30].

²² Jakási podotázka v této souvislosti zní, zda v případě rozdílnosti ve vykonávané práci má být rozdílnost ve stejném poměru promítnuta i do odměny za práci.

aspekty bezpečnosti a ochrany zdraví při práci, pracovních úrazů a nemocí z povolání, resp. přičitatelnosti negativních důsledků projevu vnějších vlivů při výkonu práce mimo pracoviště zaměstnavatele, které jsou důsledkem volby zaměstnance, a které zaměstnavatel nemůže fakticky ovlivnit,²³ vede k závěru, že k vnějším okolnostem, které působí na zaměstnance anebo jím vykonávanou práci mimo pracoviště zaměstnavatele, jež jsou důsledkem rozhodnutí zaměstnance, a které zaměstnavatel nemůže ovlivnit, by se nemělo přihlížet.

Důsledkem by bylo nezohledňování pracovních podmínek při výkonu práce z domova, což by v konečném důsledku vedlo k povinnosti poskytnout stejnou odměnu za stejnou práci a anebo práci stejné hodnoty, pokud by se jinak ve všech ostatních hodnotících kritériích vykonávaná práce shodovala.

Třetí možné řešení se nachází, obrazně řečen, uprostřed a staví na srovnávání vykonávané práce podle pracovního prostředí a podmínek.

Přístupy jsou možné dva.

Budťo se k práci z domova při hodnocení stejnosti práce, resp. stejné hodnoty práce nepřihlíží, tato se z celkového objemu práce vyloučí a z hlediska stejnosti či stejné hodnoty se posuzuje pouze práce jako taková a podmínky na pracovišti zaměstnavatele.

Anebo se jednotlivé režimy oddělí a vzájemně se poměřují z hlediska stejnosti, resp. stejné hodnoty vždy jen práce v jednotlivých režimech, tj. práce z domova proti práci z domova, práce na pracovišti proti práci na pracovišti atd.

Jaké řešení je správné? Z následně připojených závěrů lze dospět k závěru, že možná i žádné.

Procesněprávní alotria nespravedlivého odměňování

Při předpokladu, že jedním ze základních prvků právní normy je její efektivita, musí být neodmyslitelnou součástí úvah při formulaci právní normy a při jejím prosazování z hlediska funkčnosti způsob její procesněprávní realizace. Zjednodušeně řečeno, „*hmota žije v procesu*“.

V souvislosti se spravedlivým odměňováním je třeba vnímat primárně dvojí procesní rovinu:

- a) uplatňování práva na náhradu škody spočívající v odlišné odměně za stejnou práci anebo práci stejné hodnoty v **civilní procesu**.

Mohlo by se zdát, že z hlediska procesního postupu bude rozhodující důvod nespravedlivého odměňování, tedy zda:

²³ V této souvislosti srov. například MORÁVEK, J. Změna některých výchozích sociálních paradigmat a její reflexe v právní úpravě pracovněprávních vztahů a sociálního zabezpečení. Právník. Praha: Ústav státu a práva Akademie věd České republiky. Sv. 2. 2021.s. 136 - 141

- důvodem nerovného odměňování za stejnou práci jeho práci stejné hodnoty je některý z diskriminačních znaků nebo jiný z důvodů (dotčený zaměstnanec je například chráněným oznamovatelem podle zákona č. 171/2023 Sb., o ochraně oznamovatelů) vypočtených v ust. § 133a zákona č. 99/1963 Sb., občanského soudního řádu,^{24, 25} anebo zda
- důvodem nespravedlivého odměňování za stejnou práci nebo práci stejné hodnoty je jiný důvod než ten, který předvídá ust. § 133a o.s.ř. V těchto případech se uplatní základní procesní povinnosti (povinnost tvrzení a povinnost důkazní) a na ně navazující břemena (břemeno tvrzení a břemeno důkazní) v obvyklé podobě.

Ve skutečnosti však otázce, jaký je důvod nespravedlivého odměňování, musí předcházet vyřešení výchozího momentu spočívajícího v tom, zda se o nespravedlivé odměňování, tj. odlišné odměňování za stejnou práci anebo práci stejné hodnoty, může vůbec jednat.

Konkrétně řečeno, napřed je třeba prokázat, že se jedná o stejnou práci nebo o práci stejné hodnoty ve smyslu § 110 ZPr, a že odměna za stejnou práci anebo za práci stejné hodnoty byla různá. Procesní aktivita by přitom měla být na straně žalobce; závěr o stejnosti práce, resp. o stejné hodnotě práce přitom z hlediska ust. § 110 ZPr nelze postavit pouze na tom, že druh práce zaměstnanců je shodný.

Prokáže-li se, že se jedná o stejnou práci anebo o práci stejné hodnoty a spolu s tím, že odměna je různá, z hlediska základu nároku není za stávajícího právního stavu důvod rozhodný. Důvod nerovného odměňování může mít význam pro uplatnění nároku na náhradu nemotné újmy.

Problém stávajícího přístupu k ust. § 110 ZPr v procesní rovině, který je patrný i ve věci Česká pošta, spočívá v tom, že naznačené schéma není respektováno; i když není tvrzen žádný diskriminační důvod, soud zpravidla procesní povinnosti realizuje tak, že po žalovaném požaduje, aby prokázal, že k nerovnému odměňování nedošlo.

b) veřejnosprávní kontrolu dodržování povinností na úseku rovného zacházení a spravedlivého odměňování v pracovněprávních vztazích ze strany inspektorátu práce a na ni případně navazující **přestupkové řízení**.

²⁴ Dále jen **o.s.ř.**

²⁵ Obecně v této pozici platí, že pokud žalobce uvede před soudem skutečnosti, ze kterých lze dovodit, že ze strany žalovaného došlo k nerovnému zacházení z některého se zákonem aprobovaných důvodů, je žalovaný povinen dokázat, že nedošlo k porušení zásady rovného zacházení. Jak ukazuje judikatura Nejvyššího soudu (srov. například Nejvyšší soud ve věci sp. zn. 21 Cdo 246/2008, 21 Cdo 230/2015, 21 Cdo 1577/2022) a Ústavního soudu (srov. například Ústavní soud ve věci sp. zn. III. ÚS 880/15, III. ÚS 1136/13, Pl. ÚS 37/04 atd.), i pokud spadá věc pod ust. § 133a o.s.ř., je třeba určitá procesní aktivita žalobce.

Z hlediska zákona č. 251/2005 Sb., o inspekci práce, jsou v této souvislosti rozhodné primárně skutkové podstaty podle ust. § 11 a § 24, resp. podle ust. § 13 a § 26 zákona. Skutkové podstaty lze zobecnit následovně:

- zaměstnavatel se dopustí přestupku na úseku rovného zacházení tím, že nezajistí rovné zacházení se všemi zaměstnanci, pokud jde o jejich pracovní podmínky, odměňování za práci a poskytování jiných peněžitých plnění a plnění peněžitě hodnoty, a odbornou přípravu a příležitost dosáhnout funkčního nebo jiného postupu v zaměstnání,
- zaměstnavatel se dopustí přestupku na úseku odměňování zaměstnanců tím, že neposkytne zaměstnanci za stejnou práci nebo práci stejné hodnoty stejnou mzdu, plat nebo odměnu z dohody jako jinému zaměstnanci.

Jde tedy o skutkové podstaty vystavěné tradičním způsobem, kdy k naplnění objektivní stránky přestupku nedochází *de facto* neprokázáním splnění určité povinnosti, nýbrž prokázáním v rozsahu, o němž nejsou důvodné pochybnosti, že k porušení povinnosti došlo. To však kvůli rozsahu kritérií obsažených v ust. § 110 ZPr může být, je-li postupováno striktně podle zákona, složité až fakticky nemožné, neboť rozdíl v jediném kritériu má za důsledek závěr o rozdílnosti prací (viz shora).

I z toho důvodu se pravděpodobně inspektoráty práce uchylují k procesně vadnému přístupu. V kontrole, u níž je z povahy věci předpoklad, že její případný závěr o porušení pracovněprávních povinností bude podkladem pro přestupkové řízení, aniž by kontrolovaného poučili o právu odmítnout aktivní součinnost, pokud by jí způsobil nebezpečí trestního stíhání sobě nebo osobně blízké, pod pohrůzkou pořádkové pokuty vyžadují od zaměstnavatele, aby tvrdil a prokázal důvodnost rozdílného odměňování. V případě neprokázání rozdílnosti následně v kontrolním protokolu konstatují porušení zákonné povinnosti, které následuje vydání příkazu a uložením pokuty.

Připomeňme, že dle stanoviska odboru veřejné správy, dozoru a kontroly Ministerstva vnitra č. 3 z roku 2018 *„dle našeho názoru zákaz sebeobviňování musí platit i v rámci kontroly (byť je otázka v jakém rozsahu), a to již s ohledem na jeho ústavní zakotvení. Podobně máme za to, že ačkoliv to stávající kontrolní řád výslovně nestanoví, musí i při kontrole platit ochrana utajovaných informací (a ochrana povinnosti mlčenlivosti), neboť obecný procesní předpis „neruší“ hmotné právo. 10 Je tedy možno shrnout, že v rámci kontroly nemůže správní orgán zjišťovat od kontrolované osoby (pozdějšího účastníka řízení) skutečnosti, které by v navazujících procesních postupech (postup před zahájením správního řízení a správní řízení) od účastníka řízení zjišťovat*

nemohl, protože tomu brání procesní ustanovení správního řádu nebo zákona o odpovědnosti za přestupky a řízení o nich“.²⁶

Závěrečné poznámky

Smyslem předloženého intelektuálně lingvistického cvičení bylo poukázat na vybrané problematické (hmotněprávní a procesněprávní) momenty právní úpravy spravedlivého odměňování v České republice. Jejich výčet a výklad k nim není zdaleka vyčerpávající. Postačí však k závěru, který se jasně podává.

Právní úprava spravedlivého odměňování v právním řádu České republiky primárně kvůli své podrobnosti nabízí širokou škálu možností, jak její uplatnění fakticky eliminovat. Z druhé strany však (v důsledku přístupu soudů a inspektorátu práce) při nedostatečné či nesprávné procesní aktivitě zaměstnavatele má potenciál působit silně destruktivně ve vztahu k tuzemskému hospodářství, narušovat fungování trhu a nežádoucím způsobem ovlivňovat cenu práce.

Bez větších legislativních zásahů je jedinou možnou cestou (z hlediska předmětu tohoto příspěvku) k alespoň nějak rozumnému řešení, formulaci rozumného pravidla v oblasti spravedlivého odměňování, použití teleologické redukce ve vztahu k ust. § 110 ZPr ve smyslu omezení právní úpravy na jeden závod/jediné pracoviště spolu s vyloučením vnějších vlivů působících při práci mimo pracoviště zaměstnavatele, které jsou důsledkem rozhodnutí zaměstnance, a které zaměstnavatel nemůže ovlivnit.

Z dosavadního přístupu Nejvyššího soudu nejen ve vztahu k problematice spravedlivého odměňování, ale třeba i ve vztahu k problematice odvolání a vzdání se vedoucího pracovního místa²⁷ a stejně jako v řadě dalších,²⁸ se však zdá, že teleologická redukce je (nejméně) v oblasti pracovněprávních vztahů Nejvyššímu soudu spíše cizí a místo toho tenduje k textualistickému přístupu.

Nelze tak vyloučit, že se můžeme dočkat toho, že zejména zaměstnance, kteří vykonávají práci, jejíž povaha umožňuje výkon práce z domova, bude možné odměňovat relativně volně, neboť výkon práce z domova, odlišnost pracovního režimu při samorozvrhování pracovní doby či jiná obdobná rozdílnost, bude sloužit jako argument pro závěr o rozdílnosti vykonávané práce; paradoxně se nezanedbatelnou měrou může jednat o zaměstnance, kteří pečují o děti a měla by jim být poskytována vyšší míra ochrany.

²⁶ V této souvislosti v podrobnostech viz rovněž MORÁVEK, J. (ED.) *Zákaz nucení k sebeobviňování při činnosti inspektorátu práce*. Praha: Právnická fakulta Univerzity Karlovy. 2020.

²⁷ Srov. op. cit. sub. 11 a 13.

²⁸ Srov. MORÁVEK, J. Ohlédnutí se za pracovněprávní legislativou a judikaturou (zejména) pandemických let in SOCIETAS ET IURISPRUDENTIA - *Medzinárodný internetový vedecký časopis zameraný na právne otázky v interdisciplinárnych súvislostiach*. Právnická fakulta Trnavské univerzity v Trnavě. Trnava. 2022 sv. 2., ročník X. s. 19 – 50.

Vedle toho pro zaměstnance vykonávající stejnorodé práce na různých pracovištích zaměstnavatele napříč republikou bude platit povinnost poskytovat stejnou odměnu fakticky bezvýjimečně a bez ohledu na regionální odlišnosti v ceně práce. O negativních důsledcích s tím spojených zde již byla řeč.

Příležitost pro legislativní zásah se přitom nabízí. Je jí již zmíněná transpozice směrnice 2023/970.

Byť prozatím není návrh transpoziční legislativy k dispozici, lze být z několika důvodů k očekávání, že bude zjednána rozumná náprava, skeptický.

Směrnice v čl. 3 odst. 1 písm. a) vymezuje pojem odměna značně extenzivně, když uvádí „obvyklá základní či minimální mzda nebo plat a veškeré ostatní odměny, jež zaměstnavatel přímo nebo nepřímo, v hotovosti nebo v podobě věcného plnění (doplňkové nebo proměnné složky) vyplácí pracovníkovi v souvislosti se zaměstnáním“

V této souvislosti recitál 21 směrnice 2023/970 uvádí „tyto doplňkové nebo proměnlivé složky by mohly mimo jiné zahrnovat bonusy, odměny za přesčasy, cestovné, příspěvky na bydlení a stravování, náhrady za účast na školení, platby v případě propuštění, zákonné nemocenské, zákonem požadované náhrady a zaměstnanecké penzijní pojištění. Pojem „odměna“ by měl zahrnovat všechny prvky odměny stanovené právními předpisy, kolektivními smlouvami nebo zvyklostmi v každém členském státě.“

Vedle toho čl. 19 spolu s recitálem 29 směrnice 2023/970 předvídá koncept jediného zdroje ve vztahu k určení odměny.²⁹

Pravidla, která mají být transponována, tak mohou v konečném důsledku spíše problémy prohloubit, když například koncept jediného zdroje nabízí místo restriktce pojmu zaměstnavatel naopak prostor pro ještě extenzivnější přístup, než prezentoval Nejvyšší soud ve věci sp. zn. 21 Cdo 3955/2018. Stejně tak může další problémy přinést široké vymezení pojmu odměna.³⁰

²⁹ K tématu viz například na TOMŠEJ, J. Jediný zdroj: na cestě ke koncernovému pracovnímu právu? Právní rozhledy, 2024, č. 17, s. 561.

³⁰ Příkladmo se nabízí poukázat na dva.

Pokud se za odměnu mají považovat i náhrady související s výkonem práce, při absenci jakéhokoli zákonného rozlišování režimů výkonu práce mimo pracoviště zaměstnavatele, mohou být problematické různé zaměstnavatelem určené režimy poskytování (nebo neposkytování) náhrad při výkonu práce z domova ve smyslu ust. § 190a ZPr.

Mezi platby poskytované zaměstnanci při skončení pracovního poměru lze počítat vedle odstupného i „odchodné“, jímž lze rozumět peněžitou platbu poskytnutou zaměstnanci na základě dohody v souvislosti se skončením pracovního poměru, jejímž účelem je motivovat jej ke skončení pracovního poměru.

Výše odstupného nad zákonné minimum, stejně tak jako výše odchodného je přitom často důsledkem působení řady vlivů a okolností; schopnosti zaměstnance či jeho právního zástupce vyjednávat, obav ze soudního sporu či snahy o jeho eliminaci kvůli zachování určitého auditního hodnocení

Uzavřít lze s tím, že stávající zákonná úprava (pod prizmatem výkladu plynoucím z judikatury Nejvyššího soudu) spravedlivého odměňování, jak je zavedena ust. § 110 ZPr, postrádá dva ze tří výchozích předpokladů pro kvalifikaci pravidla, co by (relevantní) právní normy. Konkrétně se jedná o nedostatek legitimacy a o nedostatek efektivity. Důsledkem je nepřiměřený zásah do autonomie vůle zaměstnavatele a v konečném důsledku taktéž do jeho majetkových práv.

Závěr o nedostatku legitimacy pramení z nedostatečného prostoru pro reflexi s prací souvisejících sociálních, ale i socioekonomických faktorů, které mohou být pro určení ceny práce, resp. možná spíše ceny konkrétního zaměstnance a jeho působení u zaměstnavatele stejně významné, nebo (v některých případech) dokonce i významnější než výkon práce sám. Z toho hlediska působí právní úprava, jak kdyby byla připravena pro společnost robotů pohybujících se ve sterilním světě bez vnějších vlivů.³¹

Některé z uvedených momentů jsou rozhodné i pro závěr o nedostatku efektivity právní úpravy.

Nejsilnějším argumentem ve vztahu k nedostatku efektivity je však v něčem jiném. Jde o širší aspekty, které je třeba kumulativně hodnotit při posuzování shodnosti vykonávané práce, resp. hodnoty práce jednotlivých zaměstnanců. Opakovaně poukazovaná přílišná podrobnost právní úpravy promítající se do mnohosti hodnotících kritérií přímo vybízí s poukazem na (byť dílčí) odchylky v pracovním režimu anebo pracovních podmínkách u řady zaměstnavatelů uplatnění právní úpravy vyloučit.

Stavět právní úpravu spravedlivého odměňování na odosobněných pravidlech bez reflexe reálného fungování pracovněprávních vztahů a vnějšího světa vyžadující až laboratorní posuzování a vážení širokého spektra kritérií ve snaze usilovat o dokonalou spravedlnost a rovnost není rozumné a ani reálné.

zaměstnavatele kvůli získání zakázky, snahy eliminovat například negativní publicitu, snahy eliminovat podnět orgánu veřejné moci anebo zahraničnímu vlastníkovu zaměstnavatele atd.

Bude snad zaměstnavatel napříště muset důvody svého přístupu k jiným zaměstnancům v tomto směru v podrobnostech vysvětlovat? Nebo takové „lidské“ důvody nebudou po vzoru stávající úpravy ust. § 110 ZPr vůbec relevantní?

³¹ Částečně se sociální stránku výkonu práce pokusil reflektovat Nejvyšší správní České republiky ve věci sp. zn. 2 Ads 335/2018. Učinil tak nicméně relativně neumně, což následně sám nepřímo přiznal svou argumentací v rozhodnutí ve věci sp. zn. 10 Ads 33/2023.

Zcela stranou nelze nechat ani rozhodnutí Nejvyšší soud ve věci sp. zn. 21 Cdo 3471/2024, v němž Nejvyšší soud jako možné kritérium, jímž lze podmínit vznik práva na část mzdy, vzal dodržování pracovní kázně. Byť se podobný názor objevuje i v odborné literatuře, je, s přihlédnutím ke předpokladu, že mzda je odměnou za práci a dále ke kritériím podle ust. § 110 ZPr k ust. § 346b ZPr, dle kterého zaměstnanci mj. nelze za porušení pracovněprávních povinností ukládat peněžité postihy, minimálně k diskusi.

Cílem jak tuzemské, tak i evropské právní úpravy by mělo být zabránit tomu, aby dva lidé, kteří dělají (v obecném smyslu slova) shodnou práci na stejném pracovišti, měli bez legitimního důvodu různou odměnu. Legitimním důvodem přitom může být jak jejich pracovní výkonnost, tak jejich význam pro pracovní kolektiv či podobně.

Aspirovat o dosažení absolutní rovnosti ve (stále ještě) globalizovaném světě, v němž může být reálný konkurent na druhé straně planety, ve světě, v němž jsou (a snad i nadále budou) lidé různí ve svých schopnostech a osobních projevech, ale ve svých životních potřebách a nákladech, je bláhové. Jde o jistý druh totalitarismu a rovnostářství, který je se svobodou a volným trhem slučitelný jen stěží.

Zoznam použitej literatúry

1. BĚLINA, M. DRÁPAL, L. a kol. Zákoník práce. 4. vydání. Praha: C. H. Beck, 2023,
2. BUREŠOVÁ, K. Práci z domova umožňuje až 59 podniků za 100. Statistika&My. Časopis Českého statistického úřadu. On-line 27.9.2025. dostupné na <https://statistikaamy.csu.gov.cz/praci-z-domova-umoznuje-59-podniku-ze-100>. 30. září [cit. 2025-9-30].
3. CIBULKOVÁ, M., CHLADA, O., LANDWEHRMANN, T., PROCHÁZKOVÁ, E., VRAJÍK, M. Stanovisko CzELA k právním otázkám práce na dálku. Právní rozhledy, 2024, č. 22
4. HŮRKA, P., RANDLOVÁ, N., DOLEŽÍLEK, J., ROUČKOVÁ, D., VYSOKAJOVÁ, M., DOUDOVÁ, S., KOŠNAR, M., HORNA, V. a kol. *Zákoník práce: Komentář*. Wolters Kluwer. 2024
5. MORÁVEK, J. Ke spravedlivému odměňování v pracovněprávních vztazích. Právní rozhledy, 2020, č. 20, s. 705-709
6. MORÁVEK, J. Nejen k pracovnímu poměru na dobu určitou z hlediska novely zákoníku práce In Březiny, P., Cvrček, F. (eds.) *Metamorfózy práva ve střední Evropě VIII*. Alfeus a Augiášův chlév. Plzeň: Právnická fakulta Západočeské univerzity v Plzni. 2024. s. 382-404
7. MORÁVEK, J. Ohlédnutí se za pracovněprávní legislativou a judikaturou (zejména) pandemických let in SOCIETAS ET IURISPRUDENTIA - *Medzinárodný internetový vedecký časopis zameraný na právne otázky v interdisciplinárnych súvislostiach*. Právnická fakulta Trnavské univerzity v Trnavě. Trnava. 2022 sv. 2., ročník X. s. 19 – 50
8. MORÁVEK, J. Spravedlivé odměňování po Česku In Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia / Nikola Bezáková, Ádám Sípó, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 233 s. ISBN 978-80-7160-698-7., s. 6 – 17

9. MORÁVEK, J. Výpovědní doba z hlediska „flexibilizační“ novely zákoníku práce In Morávek, J. (ed.) Zákoník práce a sociální zabezpečení 2024. Praha: Právnická fakulta Univerzity Karlovy. 2024. s. 51-62,
10. MORÁVEK, J. Změna některých výchozích sociálních paradigmat a její reflexe v právní úpravě pracovněprávních vztahů a sociálního zabezpečení. Právník. Praha: Ústav státu a práva Akademie věd České republiky. Sv. 2. 2021.s. 136 – 141
11. PICHRT, J. A KOL. Pracovní právo. 2. vydání. Praha: C.H.Beck. 2025
12. ROTHOVÁ, E.. In: BĚLINA, M.v, DRÁPAL, L. a kol. Zákoník práce. 4. vydání. Praha: C. H. Beck, 2023, s. 708, marg. č. 4.
13. ŠTEFKO, M.. Mzdová (ne)sloboda zaměstnavatele v judikatuře českých soudů. Právní rozhledy, 2022, č. 17, s. 598-602
14. VYSOKAJOVÁ, M. Tzv. flexinovela zákoníku práce. Praha: Wolters Kluwer. 2025. sv. 5. s. 5 an.

Kontaktné údaje

doc. JUDr. Jakub Morávek, Ph. D.
moravek@prf.cuni.cz
Právnická fakulta Univerzity Karlovy

RODOVÝ ROZMER SKONČENIA EKONOMICKEJ ČINNOSTI A JEHO REFLEXIA V SYSTÉME SOCIÁLNEHO POISTENIA

THE GENDER DIMENSION OF ENDING ECONOMIC ACTIVITY AND ITS REFLECTION IN THE SOCIAL SECURITY SYSTEM

Ján Matlák¹, Silvia Treľová²

Abstrakt: Skončenie ekonomickej činnosti ženy má často nepriaznivé dôsledky pre ňu aj jej rodinu. Kľúčové je zabezpečiť kontinuitu sociálnej ochrany najmä počas prechodných období života ženy – ako je tehotenstvo, materstvo, rodičovská dovolenka, prerušenie ekonomickej činnosti či odchod z trhu práce. V tejto súvislosti je potrebné venovať pozornosť otázke spravodlivosti a rovnosti v systéme sociálneho zabezpečenia. Príspevok skúma, do akej miery systém sociálneho zabezpečenia reflektuje reálne životné situácie žien a aké rodové nerovnosti v oblasti sociálneho poistenia pretrvávajú – najmä v nemocenskom, dôchodkovom a poistení v nezamestnanosti. Zároveň autori navrhujú opatrenia na podporu rodovej rovnosti a identifikujú systémové nedostatky, čím prispievajú k diskusii o spravodlivosti a udržateľnosti sociálneho zabezpečenia v tejto oblasti. Autori zdôrazňujú potrebu komplexného prístupu, ktorý zohľadňuje nielen legislatívne rámce, ale aj kultúrne a spoločenské faktory ovplyvňujúce postavenie žien v systéme sociálneho zabezpečenia.

Kľúčové slová: rodová rovnosť, zamestnanie, poistenie, dávky sociálneho poistenia

Abstract: The termination of a woman's economic activity often has adverse consequences for her and her family. It is essential to ensure continuity of social protection, especially during transitional periods in a woman's life, such as pregnancy, motherhood, parental leave, interruption of economic activity, or departure from the labour market. In this context, attention must be paid to the issue of fairness and equality in the social security system. The paper examines the extent to which the social security system reflects the real-life

¹Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta Univerzity Komenského v Bratislave

² Katedre informačného manažmentu a podnikových systémov, Fakulta managementu Univerzity Komenského v Bratislave

situations of women and what gender inequalities persist in the area of social insurance, particularly in sickness, pension, and unemployment insurance. At the same time, the authors propose measures to promote gender equality and identify systemic shortcomings, thereby contributing to the debate on fairness and sustainability of social security in this area. The authors emphasize the need for a comprehensive approach that takes into account not only legislative frameworks but also cultural and social factors affecting the position of women in the social security system.

Key words: gender equality, employment, insurance, social security benefits

Úvod

Rodová nerovnosť nie je len naliehavou morálnou a sociálnou otázkou, ale je tiež kľúčová pre inkluzívny a udržateľný hospodársky rast. Rodové rozdiely v prístupe aj k sociálnym službám majú vplyv na ekonomickú produktivitu žien³, rodová nerovnosť ovplyvňuje reálne hospodárske výsledky.⁴

Skončenie ekonomickej činnosti má rôzny dopad na mužov a ženy. Tento rozdiel sa často odvíja od pretrvávajúcich rodových nerovností na trhu práce, ale aj v systéme sociálneho zabezpečenia.

Keďže veľká časť otcov čerpá veľmi málo alebo vôbec žiadnu rodičovskú dovolenku, je celospoločenským cieľom zvýšiť podiel otcov na rodičovskej dovolenke.⁵ Chuard vo svojej štúdii odhalila negatívne vplyvy na zdravie matiek v prípade dlhej rodičovskej dovolenky (v dĺžke 2,5 roka), a preto rastúci trend v čerpaní rodičovskej dovolenky otcami môže zmierniť negatívne účinky v podobe zhoršujúceho sa duševného zdravia matiek.⁶

Sú to teda práve ženy, ktoré častejšie prerušujú a vykonávajú ekonomickú činnosť na podhodnotených alebo flexibilných pracovných miestach z dôvodu starostlivosti o

³ KOCHHAR, Kalpana - JAIN-CHANDRA, Sonali – NEWIAK, Monique: Women, Work, and Economic Growth: Leveling the Playing Field. Washington, DC: International Monetary Fund. 2017, p. 2.

https://www.google.sk/books/edition/Excerpt_Women_Work_and_Economic_Growth/KVoZEAAQBAJ?hl=sk&gbpv=1&dq=inauthor:%22Ms.Kalpana+Kochhar%22&printsec=frontcover

⁴ BERTAY, Ata Can, DORDEVIC, Ljubica, SEVER, Can: Gender Inequality and Economic Growth: Evidence from Industry-Level Data. IMF Working Paper No. 20/119. Singapore: International Monetary Fund. 2020, p. 2. <https://www.imf.org/en/Publications/WP/Issues/2020/07/03/Gender-Inequality-and-Economic-Growth-Evidence-from-Industry-Level-Data-49478>.

⁵ JØRGENSEN, Thomas Høgholm – SØGAARD, Jakob Egholt: The division of parental leave: Empirical evidence and policy design. In Journal of Public Economics, 2024. p. 18. [The division of parental leave: Empirical evidence and policy design](#)

⁶ CHUARD, Caroline: Negative effects of long parental leave on maternal health In *Journal of Health Economics*. 2023. p. 16. [Negative effects of long parental leave on maternal health: Evidence from a substantial policy change in Austria](#)

deti alebo blízke osoby. To vedie k nižšiemu počtu rokov ekonomickej činnosti, k nižším príjmom zo zárobkovej činnosti, a tým aj k nižším sociálnym odvodom v rámci sociálno-poistovacích právnych vzťahov. Tieto faktory sa následne premietajú do nižších súm dávok nemocenského a dôchodkového poistenia, a teda do celkovej ekonomickej neistoty osoby. „Prostredníctvom sociálno-poistovacích právnych vzťahov sa „realizuje ochrana ekonomicky činných subjektov, najmä zamestnancov a samostatne zárobkovo činných osôb v období znevýhodnenia voči ostatným jednotlivcom alebo sociálnym skupinám, ktoré nedosahujú príjmy zo zárobkovej činnosti.“⁷ Z hľadiska sociálno-poistovacích právnych vzťahov sú ženy často nedostatočne chránené v porovnaní s mužmi, a tak častejšie čelia situácii, keď sú odkázané na systém štátnej sociálnej podpory, prípadne systém sociálnej pomoci. Rodový rozmer ukazuje, že súčasné nastavenie systému sociálneho poistenia a podmienky na trhu práce nedostatočne reflektujú špecifickú životnú dráhu žien, čím prehľbujú rodové nerovnosti v oblasti ekonomickej istoty, ako aj v oblasti sociálneho zabezpečenia.

Skončenie ekonomickej činnosti ženy so sebou prináša viaceré praktické i legislatívne otázky: Kedy zaniká účasť na povinnom poistení? Aké sú možnosti dobrovoľnej účasti na sociálnom poistení? Aké podmienky musí žena spĺňať pre vznik nároku na peňažné plnenia v rámci sociálneho poistenia? Je systém nastavený tak, aby reflektoval špecifiká ženského pracovného života? Odpovede na tieto otázky sú často kľúčové pre zabezpečenie kontinuity sociálnej ochrany, najmä v prechodných obdobiach života ženy – v tehotenstve, v materstve, počas čerpania materskej dovolenky, rodičovskej dovolenky, pri prerušení ekonomickej činnosti alebo pri definitívnom skončení zárobkovej činnosti. Za účelom zlepšenia výsledkov v oblasti rodovej rovnosti bol realizovaný výskumný program Gender-Responsive Age-Sensitive Social Protection (GRASSP, 2018-2023) vedený Úradom UNICEF. Výskum bol zameraný na oblasť, ako môže sociálna ochrana zohľadňujúca rodové hľadisko dosahovať rodovú rovnosť, a to vytvorením solídnej základne zameranej na to, „čo funguje“, „ako“ a „prečo“ v oblasti sociálnej ochrany. Aktéri výskumu záverom konštatovali, že hodnotenie návrhov zmien a možnej implementácie je kľúčové, aby programy a politiky mohli byť efektívne na dosahovanie zamýšľaných výsledkov.⁸

⁷ MACKOVÁ, Zuzana: Funkcie práva sociálneho zabezpečenia v Slovenskej republike na začiatku tretieho tisícročia. In: *Uskutočniteľnosť sociálnych práv v systémoch sociálnej bezpečnosti*. Plzeň: Aleš Čeněk, 2015, s. 133.

⁸ CAMILLETTI, Elena: Social Protection and Its Effects on Gender Equality: A Literature Review. Innocenti Working Paper 2020-06. Florence: UNICEF Office of Research – Innocenti, 2020. p.45.

Skončenie ekonomickej činnosti a účasť na nemocenskom poistení

Skončenie ekonomickej činnosti má okrem absencie príjmu aj dopad z hľadiska práva sociálneho zabezpečenia. Strata charakteru zamestnanca na účely sociálneho poistenia má za následok vylúčenie tejto fyzickej osoby z osobného rozsahu povinného sociálneho poistenia.⁹ Rovnako to platí aj pre samostatne zárobkovo činnú osobu, ak nespĺňa podmienky § 5 zákona č. 461/2003 Z. z. o sociálnom poistení (ďalej len „zákon o sociálnom poistení“).¹⁰ Vylúčenie z účasti na týchto sociálno-poistovacích právnych vzťahoch znamená pre fyzickú osobu okrem iného aj stratu nárokov na dávky nemocenského poistenia, ktorých poskytovanie je podmienené jednak sociálnymi udalosťami, ako je dočasná pracovná neschopnosť, potreba ošetrovania (starostlivosti) fyzickej osoby, tehotenstvo a materstvo, ale aj stratou príjmu za vykonanú prácu.

Jediné pozitívum skončenia účasti na povinnom nemocenskom poistení u zamestnankyni, ako aj u samostatne zárobkovo činnnej osoby, ak to možno takto nazvať, je skutočnosť, že zánikom účasti na povinnom nemocenskom poistení môže táto osoba byť zaradená do osobného rozsahu nemocenského poistenia, a to na báze dobrovoľnosti. To znamená, že sa môže sama rozhodnúť vstúpiť do systému nemocenského poistenia a platiť si poistné dobrovoľne. Výhodou dobrovoľného nemocenského poistenia je zachovanie si nároku na peňažné plnenia sociálneho poistenia, finančná istota v prípade nepriaznivej sociálnej situácie, dobrovoľnosť a možnosť ukončenia účasti na poistení, ako aj flexibilita, pričom osoba nie je viazaná ekonomickou činnosťou a môže si sama určiť rozsah svojej ochrany. Na druhej strane je dôležité zvážiť, či je schopná pravidelne platiť poistné. Zákon o sociálnom poistení vylučuje súbeh účasti na povinnom nemocenskom poistení a účasti na dobrovoľnom poistení, čo podľa nášho názoru je diskutabilné, nakoľko je v rozpore s princípom rovnosti pred zákonom a demotivačné pre osoby, ktoré by chceli mať vyššiu mieru zabezpečenia. Rovnako diskutabilné je aj podmienenie dobrovoľnej účasti na nemocenskom poistení dobrovoľnou účasťou na dôchodkovom poistení. Toto legislatívne podmienenie podľa nášho názoru znamená obmedzenie slobody jednotlivca, nakoľko dobrovoľné poistenie by malo byť založené na slobodnom rozhodnutí príslušnej fyzickej osoby. Ak zákonodarca podmieňuje účasť na dobrovoľnom nemocenskom poistení súbežnou účasťou na dobrovoľnom dôchodkovom poistení, podľa nášho názoru ide o neúčelné obmedzenie, nakoľko

⁹ Podľa § 20 ods.1 zákona č. 461/2003 Z. z. o sociálnom poistení povinné nemocenské poistenie, povinné dôchodkové poistenie a povinné poistenie v nezamestnanosti zamestnanca vzniká odo dňa vzniku právneho vzťahu, ktorým fyzická osoba získava postavenie zamestnanca a zaniká dňom zániku tohto právneho vzťahu.

¹⁰ Pre vznik a zánik povinného nemocenského poistenia a povinného dôchodkového poistenia samostatne zárobkovo činnnej osoby platí § 21 zákon a o sociálnom poistení.

každé z týchto poistení, t. j. nemocenské a dôchodkové, pokrýva iné rizikové situácie. Uvedená podmienenosť predstavuje aj zvýšené finančné zaťaženie poistenca, nakoľko viacerí záujemcovia o účasť na dobrovoľnom nemocenskom poistení (napr. ženy plánujúce tehotenstvo a materstvo) popri platení poistného na nemocenské poistenie sú povinné platiť poistné aj na dôchodkové poistenie, čo v podstatnej miere zvyšuje ich mesačné výdavky a pre niektoré okruhy osôb (napr. študentky, tehotné ženy, matky, nezamestnané osoby) je to neúnosné a odrádza ich to od účasti na dobrovoľnom nemocenskom poistení. Z uvedeného vyplýva, že táto legislatívna úprava predstavuje zníženie motivácie zapojiť sa do tohto systému a namiesto toho, aby zákonodarca motivoval fyzické osoby, a predovšetkým ženy, dobrovoľne sa poistiť, a tým zvýšiť počet osôb krytých nemocenským poistením, táto podmienka pôsobí demotivačne. Absencia neúčasti na dobrovoľnom nemocenskom poistení v mnohých prípadoch môže viesť k závislosti na vecnom rozsahu systému štátnej sociálnej podpory, prípadne systému sociálnej pomoci. Rovnako ide o nesúlad s účelom jednotlivých druhov sociálneho poistenia, nakoľko nemocenské poistenie a dôchodkové poistenie majú úplne rozdielny účel, rizikový profil a časový horizont. Kým nemocenské poistenie rieši krátkodobé výpadky príjmu, dôchodkové poistenie predstavuje riešenie dlhodobých záležitostí.

Podmienenie dobrovoľnej účasti na nemocenskom poistení súčasnou účasťou na dôchodkovom poistení nepovažujeme za efektívne a ani za spravodlivé. V praxi to znamená, že systém zbytočne komplikuje prístup k sociálnej ochrane pre fyzické osoby a v mnohých prípadoch práve pre ženy, ktoré by si radi platili poistné na nemocenské poistenie, no nie sú schopné alebo ochotné platiť súčasne aj poistné na dôchodkové poistenie. Viazanie týchto poistných vzťahov nie je logicky nevyhnutné a lepším riešením by bolo umožniť samostatnú účasť na dobrovoľnom poistení každého druhu.

Skončenie ekonomickej činnosti a jej dopad na vecný rozsah dôchodkového poistenia

„Nárok na dôchodok ovplyvňujú individuálne kariérne dráhy a podmienky na trhu práce, čo často vedie k rodovým rozdielom. Ženy čelia počas svojho pracovného života viacerým výzvam, ako je neskorý vstup na trh práce, rodové rozdiely v odmeňovaní, prerušovaná pracovná kariéra a predčasný odchod do dôchodku z dôvodu starostlivosti o rodinu, čo vedie k nižším dôchodkovým príjmom.“¹¹

¹¹ ABATEMARCO, Antonio - LAGOMARSINO, Elena, RUSSOLILLO, Maria: Gender Pension Gap in EU Countries: A Between-Group Inequality Approach. In: Risks, vol. 11(3), 63, 2023, pp. 1-2. https://ideas.repec.org/a/gam/jrisks/v11y2023i3p63-d1102469.html?utm_source=chatgpt.com

Skončenie ekonomickej činnosti, a teda aj skončenie sociálno-poistovacieho právneho vzťahu, môže negatívne ovplyvniť výšku dávok dôchodkového poistenia alebo u niektorých fyzických osôb môže mať negatívny dopad pre vznik nároku na starobný dôchodok, predčasný starobný dôchodok alebo invalidný dôchodok. Výška týchto dôchodkov je závislá aj od doby účasti na dôchodkovom poistení, pričom jej skončenie môže dobu poistenia podstatne skrátiť. Pre vznik nároku na dávkové plnenie, a to vo vzťahu na základné dôchodky a prostredníctvom nich aj na odvodené dôchodky, sa v rámci dôchodkového poistenia vyžaduje splnenie tzv. „čakacej doby“. Čakacia doba je určená časovým rozsahom účasti oprávnenej osoby v poistnom systéme, pričom platná právna úprava podmieňuje vznik nároku na dávkové plnenie v rámci dôchodkového poistenia minimálnym rozsahom poistnej účasti, a to bez ohľadu na to, či ide o účasť na povinnom poistení z titulu zamestnanca, samostatne zárobkovo činnnej osoby alebo z titulu dobrovoľnej účasti na dôchodkovom poistení. Dobrovoľnou účasťou na dôchodkovom poistení sa rozumie účasť za podmienok ustanovených v § 15 ods. 5 zákona o sociálnom poistení. Dobrovoľné dôchodkové poistenie predstavuje flexibilnú možnosť zabezpečenia si základnej dávky dôchodkového poistenia, a to jednak pre osoby, ktoré sú zároveň povinne dôchodkovo poistené, ako aj pre osoby mimo účasti na povinnom dôchodkovom poistení. V tejto súvislosti treba poukázať na skutočnosť, že účasť na dobrovoľnom dôchodkovom poistení, na rozdiel od dobrovoľnej účasti na nemocenskom poistení, zákonodarca nepodmieňuje dobrovoľnou účasťou na inom druhu sociálneho poistenia, čo treba hodnotiť pozitívne. Pozitívum treba vidieť hlavne v tom, že pri iných druhoch poistenia ide o poskytovanie dávok krátkodobejšieho charakteru a neprinášajú takú dlhodobú hodnotu ako účasť na dôchodkovom poistení.

Za určitých zákonom ustanovených podmienok sa do obdobia dôchodkového poistenia zahrnie aj obdobie, keď fyzická osoba sa priamo nepodieľa na financovaní dôchodkového systému¹², napr. pri riadnej starostlivosti o dieťa do šiestich rokov jeho veku alebo o dieťa s dlhodobou nepriaznivým zdravotným stavom do 18 rokov jeho veku, pričom vo väčšine prípadov túto starostlivosť zabezpečujú predovšetkým ženy - matky. Čakacia doba spolu s dovŕšením dôchodkového veku spolu s osobitnými podmienkami tvoria dávkovú schému konkrétnej základnej dávky dôchodkového poistenia.

Pokiaľ však ide o výšku dávky dôchodkového poistenia, táto závisí okrem iného aj od priemerného osobného mzdového bodu, ktorý sa viaže na vymeriavací základ zamestnanca. Za zamestnanca pri vyššie uvedenej starostlivosti platí poistné na dôchodkové poistenie štát, ak táto osoba nie je dôchodkovo poistená. Vymeriavací základ, z ktorého štát platí poistné na dôchodkové poistenie je mesačne vo výške 60 % priemerného mesačného zárobku platného v kalendárnom roku, ktorý dva roky

¹² § 15 ods.1 písm. c) – i) zákona o sociálnom poistení

predchádza kalendárnemu roku, za ktorý sa platí poistné. Dôsledkom plnenia tejto odvodovej povinnosti je pomerne nízka výška dôchodku, čo je jedným z dôvodov, že v ostatnom období je snaha o odstránenie diskriminácie rodičov, najmä matiek, ktorých starostlivosť o dieťa počas materskej, resp. rodičovskej dovolenky, negatívne ovplyvnila výšku dôchodku. Pripravuje sa legislatívna úprava, podľa ktorej by sa mali zohľadniť príjmy zamestnankyne pred materskou a rodičovskou dovolenkou a po jej skončení, a ich priemer bude vymeriavacím základom pre účely dôchodkového poistenia. Táto úprava by predstavovala významnú zmenu v prístupe štátu k rodičom, a predovšetkým k ženám počas čerpania materskej alebo rodičovskej dovolenky, a štát by symbolicky aj prakticky postavil starostlivosť o dieťa na roveň formy výkonu ekonomickej činnosti. Ide o pozitívny signál sociálnej politiky, ktorý uznáva neviditeľnú prácu žien (a v menšej miere aj mužov), ktorí kvôli rodičovstvu obetovali časť svojej ekonomickej aktivity. Ak bude implementovaný spravodlivo a efektívne, môže významne prispieť k dôchodkovej spravodlivosti a rovnosti medzi pohlaviami.

Peňažné plnenie v nezamestnanosti

V mnohých prípadoch po skončení pracovnoprávneho vzťahu alebo po skončení samostatnej zárobkovej činnosti sa fyzická osoba stáva nezamestnanou. Nezamestnanosť predstavuje socioekonomický jav, ktorý označuje stav, keď osoby schopné a ochotné vykonávať zárobkovú činnosť, nemôžu nájsť pracovné uplatnenie ako jeden z najbežnejších a najstabilnejších spôsobov získavania príjmu, pričom v modernej spoločnosti má zamestnanie nielen ekonomický, ale aj spoločenský a psychologický rozmer. Je to jeden z kľúčových ukazovateľov výkonnosti ekonomiky a má významné dôsledky, a to tak ako na jednotlivcov, tak aj na spoločnosť ako celok. Z jednotlivcov osobitne negatívny dopad má na ženy, tehotné ženy a osamelé ženy. V prípade skončenia ekonomickej činnosti, napr. straty zamestnania, je dôležitá otázka hmotného zabezpečenia jednotlivca a jeho rodiny v čase nezamestnanosti. Skončenie pracovného pomeru je obsahom ústavného práva na slobodný výkon povolania, zamestnania alebo inej zárobkovej činnosti. Prejav slobody platí nielen pre skončenie na základe dohody o skončení pracovného pomeru ako dvojstranného právneho úkonu, ale platí aj v prípadoch, keď pracovný pomer končí na základe jednostranného právneho úkonu, napr. výpovede, okamžitého skončenia pracovného pomeru, skončenia pracovného pomeru v skúšobnej dobe, a to buď zo strany zamestnanca alebo zamestnávateľa. Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov (ďalej len "Zákonník práce alebo ZP") prostredníctvom kogentnej úpravy spôsobov skončenia pracovného pomeru¹³ zabezpečuje

¹³ § 59 - § 80 zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov

zamestnancovi ochranu proti svojvoľnému prepúšťaniu zo zamestnania.¹⁴ Už pri založení pracovného pomeru na neurčitý čas sú si zmluvné strany vedomé toho, že nejde o nevypovedateľný právny vzťah.¹⁵

Vo väčšine prípadov sa fyzická osoba po skončení ekonomickej činnosti zaradí do evidencie uchádzačov o zamestnanie na príslušnom úrade práce, sociálnych vecí a rodiny a z titulu poistenia v nezamestnanosti jej patrí peňažné plnenie, a to netestovaná dávka - dávka v nezamestnanosti.

Podľa platnej právnej úpravy poistenec má nárok na dávku v nezamestnanosti, ak v posledných štyroch rokoch pred zaradením do evidencie nezamestnaných občanov hľadajúcich zamestnanie bol poistený v nezamestnanosti najmenej dva roky. V porovnaní s právnymi úpravami členských krajín Európskej únie ide o jednu z najtvrdšie formulovaných podmienok vzniku nároku na dávku v nezamestnanosti. V tejto súvislosti treba poukázať aj na určitú disproporciu medzi čakacou dobou a podpornou dobou pre poskytovanie dávky v nezamestnanosti, nakoľko podporná doba je vo väčšine prípadov šesť mesiacov. Legislatívna úprava hmotného zabezpečenia zamestnanca formou dávky v nezamestnanosti po skončení sociálno-poistovacieho právneho vzťahu je v porovnaní s legislatívnymi úpravami vo väčšine krajín Európskej únie menej priaznivá. Požadovaná dĺžka trvania poistenia, ako aj o doba poskytovania a výška tejto dávky, je na hranici Dohovoru MOP č. 102 o minimálnej norme sociálneho zabezpečenia, ktorý má v sociálnej sfére zásadný význam, nakoľko obsahuje celosvetovo dohodnuté minimálne normy vo všetkých odvetviach sociálneho zabezpečenia: liečebná starostlivosť, nemocenské, podpora v nezamestnanosti, starobný dôchodok, dávky pri pracovných úrazoch a chorobách z povolania, rodinné dávky, dávky v materstve, invalidný dôchodok a dávky poskytované pozostalým¹⁶.

Sme toho názoru, že vzhľadom na ostatné legislatívne úpravy v nemocenskom poistení, napr. zavedenie tehotenského¹⁷, úprava ochrannnej lehoty u tehotnej poistenkyni, je na zváženie legislatívne upraviť dávku v nezamestnanosti, špecificky pre tehotné ženy po skončení zárobkovej činnosti, a to z dôvodu vyšších životných nákladov počas tehotenstva - upraviť percentuálnu výšku dávky zo štandardných 50 % napr. na 70 %, predĺžiť obdobie poberania dávky zo 6 mesiacov na 9 mesiacov,

¹⁴ TREĽOVÁ, Silvia: Základy pracovného práva pre manažérov. - 1. vyd. - Brno : Tribun EU, 2019. s. 69.

¹⁵ BARANCOVÁ, Helena. a kol.: Zákoník práce. Komentár. 3. vydanie. Bratislava: C. H. Beck, 2022, s. 678.

¹⁶ GABRIELOVÁ, Jana: Medzinárodné dimenzie ľudských práv a sociálnej práce. In: Humanum (Międzynarodowe Studia SpołecznoHumanistyczne). Nr 9(2)/2012, s. 93.

¹⁷ Poskytovanie tehotenského sa nevylučuje napr. popri príjmu zo zárobkovej činnosti, podnikaní, poberaní materského, nemocenského, ošetrovného, rodičovského príspevku, príspevku na starostlivosť o nezaopatrené dieťa.

prípadne určiť minimálnu výšku dávky v nezamestnanosti bez ohľadu na predchádzajúci príjem¹⁸.

Domnievame sa, že existuje viacero dôvodov, prečo tento návrh je odôvodnený. Jedným z dôvodov je skutočnosť, že tehotné ženy čelia vyšším výdavkom súvisiacim so zdravotnou starostlivosťou, výživou, liekmi, predpôrodnými vyšetreniami, prípravou na pôrod, a pod. Platná suma dávky v nezamestnanosti nemusí vždy pokrývať tieto náklady. Rovnako platí, že tehotné ženy majú objektívne zníženú schopnosť zamestnať sa, či už kvôli fyzickým obmedzeniam, prípadne aj diskriminácii zo strany zamestnávateľov, pričom doba nezamestnanosti môže byť dlhšia, a to bez úmyslu tejto ženy.

Ochranná lehota

Ochrana tehotných žien pri skončení ekonomickej činnosti je zabezpečená viacerými právnymi nástrojmi, ktoré majú odlišné účely a pôsobnosti. V rámci práva sociálneho zabezpečenia je to ochranná lehota, avšak rovnako významný je nástroj v rámci pracovného práva - ochranná doba. Ide o pojmy rôznej povahy, pričom ochranná lehota reflektuje zvýšenú ochranu tehotných žien a umožňuje im získať nárok na materské, resp. ostatné dávky nemocenského poistenia (s výnimkou vyrovnávacej dávky), a to aj v prípade skončenia ekonomickej činnosti, t. j. v prípade skončenia účasti na nemocenskom poistení.

Pri skončení pracovného pomeru, a teda aj pri skončení poistného vzťahu nemocenského poistenia, má osobitný význam inštitút ochrannej lehoty, s ktorým sa však nestretávame vo všetkých štátoch EÚ. Ochranná lehota v nemocenskom poistení predstavuje právny nástroj, ktorým sa zabezpečuje existencia nároku na dávky nemocenského poistenia aj po zániku účasti na tomto poistení. V tejto súvislosti treba poznamenať, že v zmysle platnej právne úpravy v rámci ochrannej lehoty, pri splnení zákonom ustanovených podmienok, vzniká nárok na všetky dávky nemocenského poistenia (nemocenské, ošetrovné, tehotenské, materské) s výnimkou vyrovnávacej dávky, na rozdiel napr. od českej právnej úpravy, podľa ktorej v ochrannej lehote vzniká nárok iba na nemocenské a peňažnú pomoc v materstve. Existencia ochrannej lehoty síce potláča poistný systém, ale za pozitívum treba považovať skutočnosť, že predstavuje určitú kompenzáciu účasti na nemocenskom poistení, čím zmierňuje negatívny dopad neúčasti na týchto poistných vzťahoch.

¹⁸ V rámci dôchodkového poistenia je zavedený minimálny dôchodok, ktorým sa zabezpečuje, že fyzické osoby s nízkymi príjmami počas života (napr. z dôvodu starostlivosti o deti, choroby, alebo výkonu nízko platených prác) nebudú v starobe úplne bez prostriedkov a je prostriedkom proti chudobe seniorov. Suma starobného dôchodku a suma invalidného dôchodku vyplácaného po dovŕšení dôchodkového veku sa zvýši na sumu minimálneho dôchodku.

Ochranná lehota v nemocenskom poistení plní dôležitú funkciu pri zabezpečení sociálnych práv poistencov v období medzi stratou poistenia a možnosťou jeho obnovenia. Dĺžka ochrannej lehoty by mala byť zvolená s ohľadom na spravodlivosť, udržateľnosť systému a minimalizáciu rizika zneužívania. Osobitné zvýhodnenie pre tehotné ženy poukazuje na hodnotové smerovanie systému sociálneho zabezpečenia – k ochrane zraniteľných skupín. Z týchto dôvodov možno konštatovať, že dĺžka ochrannej lehoty je vo väčšine prípadov primeraná, vecne opodstatnená a v súlade s cieľmi nemocenského poistenia. Ochrannú lehotu možno chápať aj ako predĺženie účasti na nemocenskom poistení aj po jej zániku, ak sociálna udalosť nastane v zákone ustanovenej lehote. „Ochranná lehota tak v istom zmysle „predlžuje“ účinky nemocenského poistenia, nakoľko toto by inak už danú osobu nekrylo“.¹⁹

Niekoľko desiatok rokov dĺžka ochrannej lehoty bola 42 kalendárnych dní a v prípade, ak poistenkyňa v čase skončenia poistného vzťahu bola tehotná, jej plynula ochranná lehota šesť mesiacov. Legislatívnou úpravou sa podstatne znížila ochranná lehota zo 42 na 7 kalendárnych dní, čím sa síce znížil priestor na špekulatívne čerpanie dávok nemocenského poistenia, zvýšila sa motivácia poistencov zostať v aktívnej účasti na nemocenskom poistení, na druhej strane to znamená ohrozenie zraniteľných skupín a určite to má negatívny dopad na hmotné zabezpečenie fyzickej osoby pri náhlych nepriaznivých sociálnych situáciách po skončení poistného vzťahu. Na druhej strane, ak nemocenské poistenie poistenky zaniklo v období tehotenstva, ochranná lehota sa predĺžila zo 6 mesiacov na 8 mesiacov.

Ochranná lehota plyní aj pri prerušení povinného nemocenského poistenia z dôvodov uvedených v § 26 zákona o sociálnom poistení, nakoľko vznik prerušenia povinného nemocenského poistenia sa posudzuje rovnako ako zánik povinného nemocenského poistenia. Jedným z dôvodov prerušenia tohto poistenia je u zamestnankyne aj čerpanie rodičovskej dovolenky a u samostatne zárobkovo činnnej osoby pobranie rodičovského príspevku.

S účinnosťou od 1. júna 2022 nastala v rámci legislatívnej úpravy ochrannej lehoty pozitívna zmena, nakoľko poistenkyňa, ktorej nemocenské poistenie zaniklo v období 42 týždňov pred očakávaným dňom pôrodu prvýkrát určeným lekárom, plyní ochranná lehota osem mesiacov. Rovnaká dĺžka ochrannej lehoty, t. j. 8 mesiacov sa vzťahuje aj na ženy, ktoré otehotneli v období 180 dní od zániku nemocenského poistenia. Takýmto ženám, ktorým zanikne nemocenské poistenie, napr. z dôvodu skončenia ekonomickej činnosti, začne plynúť osem mesačná ochranná lehota od začiatku 40. týždňa pred očakávaným dňom pôrodu určeným lekárom prvýkrát. Táto legislatívna úprava má priaznivé dopady v prípade, ak účasť na nemocenskom poistení zanikla žene ešte pred otehotnením, čím tieto ženy majú možnosť čerpať

¹⁹ KOLDINSKÁ, K. a kol. Právo sociálneho zabezpečení. 1. vydání. Praha: C.H.Beck, 2022, s. 191.

dávky nemocenského poistenia aj v prípade, že im účasť na nemocenskom poistení zanikla pred tehotenstvom, čo má určite pozitívny vplyv na ich sociálne istoty a v mnohých prípadoch aj na predchádzanie riziku chudoby a sociálneho vylúčenia.

Zmena sa dotkla aj možnosti uplatniť si nárok na materské v rozmedzí 8 – 6 týždňov pred očakávaným dňom pôrodu. Do 31. mája 2022 si žena mohla uplatniť nárok z ochrannnej lehoty iba 6 týždňov pred očakávaným dňom pôrodu. Toto predĺženie možnosti uplatnenia si nároku na materské hodnotíme pozitívne, nakoľko tretí trimester tehotenstva, do ktorého spadá obdobie 6–8 týždňov pred pôrodom, je fyzicky najnáročnejší pre ženu a tiež odborné odporúčania (napr. WHO alebo ACOG – American College of Obstetricians and Gynecologists) zdôrazňujú potrebu zníženia stresu a fyzickej námahy v pokročilom štádiu tehotenstva, nakoľko pracovná záťaž môže prispieť k predčasnému pôrodu a iným komplikáciám.

V súvislosti so slovným spojením ochranná lehota je diskutabilné znenie § 34 ods. 2 zákona o sociálnom poistení, podľa ktorého „Zamestnancovi vzniká nárok na nemocenské od prvého dňa dočasnej pracovnej neschopnosti, ak dočasná pracovná neschopnosť vznikla v ochrannnej lehote“. V tomto prípade už fyzická osoba nemá postavenie zamestnanca a ide vlastne o ex-zamestnanca, resp. ex-poistenca. „Ex-poistenec má nárok na nemocenské od prvého dňa dočasnej pracovnej neschopnosti, ktorá mu vznikla počas plynutia ochrannnej lehoty.“²⁰

Ochranná doba

Ochranná doba na rozdiel od ochrannnej lehoty nepredstavuje časový priestor po skončení pracovného pomeru, ale ide o dobu trvania pracovného pomeru, počas ktorého je zamestnankyňa chránená pred výpoveďou zo strany zamestnávateľa. Aj napriek tomu, že oba inštitúty sledujú sociálnu ochranu ženy v zraniteľnom období, ich účel, trvanie a právne dôsledky sú rozdielne. Prechod medzi týmito dvoma režimami je spojený s právnou diskontinuitou – t. j. zánik pracovného pomeru automaticky ukončuje ochranu podľa Zákonníka práce, ale otvára sa ochranná lehota podľa zákona o sociálnom poistení, ktorá umožňuje pokračovanie v ochrane tehotnej ženy aspoň z hľadiska vecného rozsahu nemocenského poistenia.

Pracovnoprávne predpisy SR poskytujú zamestnancom viaceré formy ochrany pred skončením pracovného pomeru zo strany zamestnávateľa. Jednou z najvýznamnejších foriem ochrany je zákaz výpovede v tzv. ochrannnej dobe podľa § 64 ZP²¹. Aj keď môže ísť o opodstatnenosť výpovede, pri určitých sociálnych situáciách je skončenie pracovného pomeru v rozpore so spoločenským záujmom. Preto Zákonník práce v ochrannnej dobe chráni zamestnankyňu pred jednostranným skončením pracovného pomeru zo strany zamestnávateľa. Zákaz výpovede sa

²⁰ LACKO, M.: Sociálnopoistovacie právne vzťahy. Praha: Leges, 2015, s. 110.

²¹ Bližšie pozri: DOLOBÁČ, Marcel a kol.: Zákonník práce – Veľký komentár. Eurokódex, 2023, s. 422.

vzťahuje na viaceré situácie, medzi iným aj na dobu, keď je zamestnankyňa tehotná a „ Vzhľadom na ďalší okruh zákazu výpovede ide o prípad, keď je zamestnankyňa tehotná, ale ešte nie je na materskej dovolenke. Pojem tehotná zamestnankyňa vymedzuje v § 40 ods. 6 ZP. Podľa judikatúry súdu (R 74/1966) „rozviazanie pracovného pomeru výpoveďou v dobe, kedy pracovníčka je tehotná, je právne neúčinné, a to bez ohľadu na to, či podnik o tehotenstve vedel“. Z uvedeného vyplýva, že ochranná doba plynie v prípade, ak zamestnankyňa je tehotná, a to bez ohľadu na to, či zamestnávateľ o tejto skutočnosti je alebo nie je informovaný, prípadne či samotná zamestnankyňa vie o tehotenstve. Zamestnankyňa je ďalej chránená okamihom nástupu na materskú dovolenku, rodičovskú dovolenku alebo keď sa osamelá zamestnankyňa stará o dieťa mladšie ako tri roky. „Tehotenstvo, pôrod a materstvo patrí medzi dôležité sociálne udalosti, pri ktorých žena potrebuje intenzívnu pomoc spoločnosti. Je potrebné jej zabezpečiť predovšetkým lekársku starostlivosť, pracovné voľno a hmotné zabezpečenie počas tohto voľna.“²² V rámci aplikačnej praxe vznikajú otázky, či zamestnankyňa je po návrate z materskej či rodičovskej dovolenky dostatočne chránená pred výpoveďou a či nie je na zváženie myšlienka legislatívne predĺžiť túto ochrannú dobu. Pri zákaze výpovede v ochrannej dobe platia určité výnimky, ktoré podľa nášho názoru sú z právneho, ako aj praktického hľadiska, opodstatnené. Po skončení materskej alebo rodičovskej dovolenky sa zamestnankyňa vracia do bežného pracovného režimu, čím ochranná doba zaniká a zamestnávateľ môže, samozrejme za predpokladu, že sú splnené zákonné podmienky, s ňou skončiť pracovný pomer výpoveďou. Práve tento moment návratu do zamestnania predstavuje rizikovú zónu, najmä z hľadiska zosúladenia pracovného a rodinného života, ako aj možného diskriminačného konania zamestnávateľa. Návrat z materskej či rodičovskej dovolenky je pre zamestnankyňu často náročný, nakoľko po niekoľkých mesiacoch až rokoch mimo pracovného prostredia musí opätovne zvládnuť pracovné tempo, obnoviť zručnosti a zladíť pracovné povinnosti so starostlivosťou o dieťa. Predĺženie ochrannej doby by umožnilo aspoň minimálny časový priestor na túto adaptáciu bez rizika výpovede. Hoci Zákoník práce a antidiskriminačný zákon (zákon č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov) zakazujú diskrimináciu z dôvodu materstva alebo starostlivosti o dieťa, v praxi sa často vyskytujú prípady, keď je výpoveď zamestnankyni podaná krátko po návrate z materskej alebo rodičovskej dovolenky, a to pod zámienkou organizačných dôvodov. Ochrana pred výpoveďou po určitú dobu po návrate by minimalizovala možnosť takéhoto konania. Predĺženie ochrannej doby by mohlo predstavovať pozitívne opatrenie v zmysle § 8a

²² BĚLINA, Miroslav a kol.: Pracovní právo. 6. doplněné a podstatně přepracované vydání. Praha: C. H. Beck, 2014, s. 268.

antidiskriminačného zákona, ktoré má za cieľ vyrovnať znevýhodnenie určitých skupín, v tomto prípade predovšetkým žien – matiek. Najpriamejším spôsobom ako dosiahnuť túto zmenu by bolo novelizovať Zákonník práce tak, že by sa ochranná doba predĺžila na určitý čas po skončení materskej/rodičovskej dovolenky – napr. 3 až 6 mesiacov, čím by sa predĺžila ochrana aj na obdobie tzv. „postnatálnej reintegrácie“. Ďalšou možnosťou je zakotvenie predĺženia ochrannej doby do kolektívnej zmluvy alebo možnosť riešiť danú problematiku v rámci vnútropodnikových normatívnych právnych aktov.

Uvedomujeme si, že problematika predĺženia ochrannej doby po skončení materskej a rodičovskej dovolenky nie je jednoduchá – ide o udržanie rovnováhy medzi právom na ochranu na strane zamestnankyne a legitímnym záujmom zamestnávateľa na flexibilnom rozhodovaní. Prípadné predĺženie ochrannej doby môže prispieť k lepšiemu zosúladieniu rodinného a pracovného života, ako aj k zníženiu diskriminácie, avšak vyžaduje dôkladnú právnu a spoločenskú diskusiu s cieľom predísť negatívnym dopadom na pracovný trh. Z pohľadu rovnosti príležitostí a ochrany zraniteľných skupín je mierne predĺženie tejto ochrany opodstatnené. Avšak pozitívne hodnotíme zistenie u nemeckých malých a stredných firiem, že dlhšia absencia z dôvodu čerpania rodičovskej dovolenky nemá trvalý vplyv na firmy. Z dlhodobého hľadiska neboli vo výskume zistené žiadne účinky na zamestnanosť alebo zatvorenie firiem.²³

Digitalizácia

Digitalizácia okrem iného predstavuje aj zásadný nástroj na zefektívnenie poskytovania služieb občanom. Osobitný význam nadobúda v oblasti uplatňovania nárokov v súvislosti s tehotenstvom a materstvom, a to jednak z pohľadu administratívneho, ale aj sociálneho, a vzhľadom na danú problematiku aj z pohľadu zdravotného. V tomto smere treba digitalizáciu chápať ako nevyhnutný a legitímny krok v kontexte zvyšovania dostupnosti, efektívnosti a spravodlivosti sociálnych služieb pre ženy v období tehotenstva a materstva. Digitalizácia procesov pri uplatňovaní nárokov v tehotenstve a materstve je nielen opodstatnená, ale aj prakticky odôvodniteľná z viacerých hľadísk. Skúsenosti z aplikačnej praxe ukazujú, že digitalizáciou sa skracuje časový priestor, ako aj náklady na spracovanie žiadostí, nakoľko manuálne spracovanie dokumentov je spojené s vyššou pravdepodobnosťou chýb, duplicitného zadávania údajov a predlžovania lehoty vybavenia. V prípade tehotných žien a matiek, ktoré často čelia fyzickému diskomfortu a zvýšenej miere stresu, únave a v neposlednom rade aj zdravotným obmedzeniam, je minimalizácia administratívnej záťaže zásadná z medicínskeho ako aj zo sociálneho hľadiska a

²³ HUEBENER, Mathias - JESSEN, Jonas - KUEHNLE, Daniel - OBERFICHTNER, Michael. Parental Leave, Worker Substitutability and Firms' Employment. In: The Economic Journal, Volume 135, Issue 669, July 2025, p. 1492, <https://doi.org/10.1093/ej/ueae114>

redukcia administratívneho zaťaženia je významným zlepšením prístupu k zákonným nárokom.

Jedným z hlavných benefitov digitalizácie je zabezpečenie rovnosti v prístupe k službám, nakoľko elektronická forma podávania žiadostí predstavuje nástroj na prekonanie geografických a sociálno-ekonomických bariér, čo umožňuje určitým skupinám (aj marginalizovaným) efektívnejšie uplatniť svoje práva bez potreby osobnej účasti, čo je osobitne dôležité v čase tehotenstva alebo krátko po pôrode.

Digitálne informačné systémy umožňujú prepojenie medzi zdravotníckymi zariadeniami, Sociálnou poisťovňou a ďalšími inštitúciami, čím sa eliminuje potreba viacerých potvrdení a manuálnych vstupov. Od 1. júna 2022 funguje plne digitalizovaný proces len pri potvrdzovaní dočasnej pracovnej neschopnosti. V ostatnom období je zo strany MPSVaR SR snaha rozšíriť digitalizáciu v rámci sociálno-poisťovacích právnych vzťahov, a to novelou zákona o sociálnom poistení. V rámci tejto novely by dávky v tehotenstve a materstve boli poskytované automaticky, teda bez písomnej žiadosti oprávnenej osoby (tzv. „proaktívne dávky“). Digitalizáciu treba chápať ako nevyhnutný a legitímny krok v kontexte zvyšovania dostupnosti, efektívnosti a spravodlivosti sociálnych služieb pre ženy v období tehotenstva a materstva.

Záver

Koniec ekonomickej činnosti žien predstavuje významný faktor ovplyvňujúci udržateľnosť a spravodlivosť sociálneho a zdravotného poisťovacieho systému. Výstup z trhu práce zo zdravotných, rodinných alebo sociálnych dôvodov vedie nielen k poklesu individuálnych príjmov žien a ich rodín, ale zároveň k zníženiu ich odvodovej účasti v sociálno-poisťovacom systéme. Tento jav má dlhodobé dôsledky, a to nielen na aktuálne financovanie tohto systému, ale aj na zabezpečenie týchto osôb predovšetkým z hľadiska vecného rozsahu nemocenského a dôchodkového poistenia. Domnievame sa, že súčasný poisťovací systém, aj napriek viacerým pozitívam, často nedostatočne reflektuje špecifické životné situácie žien, vedie k oslabeniu sociálnej ochrany, čo môže viesť k ich ekonomickej marginalizácii. Systémové nastavenie by preto malo zahŕňať prvky, ktoré tieto skutočnosti zohľadnia, napríklad formou započítania neplatenej starostlivej práce, flexibilnejších podmienok poistenia alebo stimulácií na návrat žien do pracovného života. A práve v oblasti práva sociálneho zabezpečenia je žiaduce prijímať legislatívne opatrenia smerujúce k zmierneniu negatívnych dôsledkov skončenia ekonomickej činnosti žien.

Navrhované legislatívne úpravy možno chápať ako vyjadrenie sociálnej solidarity voči zraniteľnej skupine obyvateľstva, ktorou sú ženy, matky a predovšetkým tehotné ženy. Zabezpečenie dôstojných podmienok pre tehotné ženy je podporou

demografického rastu a dávka v nezamestnanosti môže byť súčasťou prorodinnej politiky. Samozrejme pri týchto legislatívnych opatreniach je kľúčové nastavenie jasných pravidiel a podmienok, ktoré minimalizujú riziko zneužitia a zároveň chránia ženy v tomto citlivom období.

Zoznam použitej literatúry

1. ABATEMARCO, Antonio - LAGOMARSINO, Elena, RUSSOLILLO, Maria: Gender Pension Gap in EU Countries: A Between-Group Inequality Approach. In: Risks, vol. 11(3), 63, 2023, 15 pp. [online]. [Published: 20 March 2023]. https://ideas.repec.org/a/gam/jrisks/v11y2023i3p63-d1102469.html?utm_source=chatgpt.com
2. BARANCOVÁ, Helena a kol.: Zákoník práce. Komentár. 3. vydanie. Bratislava: C. H. Beck, 2022, 1624 s. EAN: 9788082320247.
3. BERTAY, Ata Can, DORDEVIC, Ljubica, SEVER, Can: Gender Inequality and Economic Growth: Evidence from Industry-Level Data. IMF Working Paper No. 20/119. Singapore: International Monetary Fund. 2020. 42 pp. <https://www.imf.org/en/Publications/WP/Issues/2020/07/03/Gender-Inequality-and-Economic-Growth-Evidence-from-Industry-Level-Data-49478>.
4. BĚLINA, Miroslav a kol.: Pracovní právo. 6.doplňené a podstatně přepracované vydání. Praha: C. H. Beck, 2014, 496 s. EAN: 9788074002830.
5. CAMILLETTI, Elena: Social Protection and Its Effects on Gender Equality: A Literature Review. Innocenti Working Paper 2020-06. Florence: UNICEF Office of Research – Innocenti, 2020.
6. Dohovor č. 102 z roku 1952 o minimálnych normách v sociálnom zabezpečení, ratifikovaný a vyhlásený pod č. 461/1991 Zb.
7. DOLOBÁČ, Marcel a kol.: Zákoník práce – Veľký komentár. Eurokódex, 2023, 915 s. ISBN 9788081551185.
8. GABRIELOVÁ, Jana: Medzinárodné dimenzie ľudských práv a sociálnej práce. In: Humanum (Międzynarodowe Studia SpołecznoHumanistyczne). Nr 9(2)/2012, s. 89 – 105. ISSN 1898-843.
9. HUEBENER, Mathias - JESSEN, Jonas - KUEHNLE, Daniel - OBERFICHTNER, Michael. Parental Leave, Worker Substitutability and Firms' Employment. In: The Economic Journal, Volume 135, Issue 669, July 2025, Pages 1467–1495, <https://doi.org/10.1093/ej/ueae114>
10. CHUARD, Caroline: Negative effects of long parental leave on maternal health In: Journal of Health Economics, 2023, 24 pp. [Negative effects of long parental leave on maternal health: Evidence from a substantial policy change in Austria](#)
11. JØRGENSEN, Thomas Høgholm – SØGAARD, Jakob Egholt: The division of parental leave: Empirical evidence and policy design. In Journal of Public

Economics, 2024, 19 pp. [The division of parental leave: Empirical evidence and policy design](#)

12. KOCHHAR, Kalpana - JAIN-CHANDRA, Sonali – NEWIAK, Monique: Women, Work, and Economic Growth: Leveling the Playing Field. Washington, DC: International Monetary Fund. 2017.
https://www.google.sk/books/edition/Excerpt_Women_Work_and_Economic_Growth/KVoZEAAAQBAJ?hl=sk&gbpv=1&dq=inauthor:%22Ms.Kalpana+Kochhar%22&printsec=frontcover
13. KOLDINSKÁ, Kristína. a kol.: Právo sociálneho zabezpečení. 1. vydání. Praha: C. H. Beck, 2022, 481 s. ISBN: 978-80-7400-902-0.
14. LACKO, M.: Sociálnopoistovacie právne vzťahy. Praha: Leges, 2015, s. 110.
15. MACKOVÁ, Zuzana: Funkcie práva sociálneho zabezpečenia v Slovenskej republike na začiatku tretieho tisícročia. In: Uskutočniteľnosť sociálnych práv v systémoch sociálnej bezpečnosti. Plzeň: Aleš Čeněk, 2015, 420 s. ISBN 9788081730160.
16. TREĽOVÁ, Silvia: Základy pracovného práva pre manažérov. - 1. vyd. - Brno : Tribun EU, 2019, 90 s. ISBN 978-80-263-1464-6.
17. Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov. [online]. Dostupné na: <https://www.zakonypreludi.sk/zz/2001-311/znenie-20250715#cast2>.
18. Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov. [online]. Dostupné na: <https://www.zakonypreludi.sk/zz/2003-461>.
19. Zákon č. 365/2004 Z. z. o rovnakom zaobchádzaní v niektorých oblastiach a o ochrane pred diskrimináciou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. [online]. Dostupné na: <https://www.zakonypreludi.sk/zz/2004-365>.

Kontaktné údaje

doc. JUDr. Ján Matlák, CSc.

jan.matlak@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta

doc. JUDr. PhDr. Silvia Treľová, PhD.

silvia.trelova@fm.uniba.sk

Univerzita Komenského v Bratislave, Fakulta managementu

PRÁVO NA ODPOJENIE – OCHRANA ZAMESTNANCA PRED DIGITÁLNYM VYHORENÍM¹

THE RIGHT TO DISCONNECT – PROTECTING EMPLOYEES FROM DIGITAL BURNOUT

Lenka Freel², Soňa Kašická³

Abstrakt: Rozvoj informačných a komunikačných technológií zásadne transformoval spôsob výkonu práce, najmä v súvislosti s rozšírením domácej práce a telepráce. Flexibilita, ktorú tieto formy umožňujú, síce prispieva k zosúladieniu pracovného a súkromného života, avšak prináša aj zvýšené riziká spojené s permanentnou dostupnosťou a digitálnym preťažením. Novela Zákonníka práce účinná od 1. marca 2021 zaviedla právo na odpojenie pre zamestnancov pracujúcich na diaľku. Príspevok analyzuje právne a praktické aspekty tohto inštitútu, jeho vzťah k úprave pracovného času a význam pre ochranu zdravia, súkromia a odpočinku. Zároveň sa venuje otázke, či by malo byť právo na odpojenie rozšírené aj na zamestnancov pracujúcich na pracovisku. Pozornosť je venovaná aj komparatívnemu pohľadu na právnu úpravu vo vybraných členských štátoch Európskej únie a diskusii o jeho zakotvení na európskej úrovni. Právo na odpojenie je prezentované ako účinný a moderný právny nástroj prevencie digitálneho vyhorenia a ako konkrétny prejav základného práva na odpočinok zamestnanca podľa práva Európskej únie.

Kľúčové slová: právo na odpojenie, telepráca, domácka práca, pracovný čas, digitálne vyhorenie

Abstract: The rapid development of information and communication technologies has fundamentally reshaped the performance of work, particularly through the expansion of telework and home-based work. While these flexible forms can support a better work-life balance, they also bring new psychosocial risks linked to constant availability and digital overload. The Slovak Labour Code, amended with effect from 1 March 2021, introduced the

¹ Príspevok bol spracovaný pod záštitou projektu VEGA č. 1/0677/24 s názvom „Ženy v kríze“.

² Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta, Univerzita Komenského v Bratislave

³ Katedra pracovného práva a práva sociálneho zabezpečenia, Právnická fakulta, Univerzita Komenského v Bratislave

right to disconnect for employees working remotely. This paper examines the legal and practical aspects of this right, its relationship to working time regulation, and its significance for protecting employees' health, privacy, and rest periods. It also addresses the question of whether the right to disconnect should be extended to employees working on-site, given the increasing use of digital tools across all work environments. Comparative insights from selected European Union Member States are presented, together with reflections on the potential need for a harmonised European legal framework. The right to disconnect is presented as an effective and modern legal tool for preventing digital burnout and as a concrete manifestation of the employee's fundamental right to rest under European Union law.

Key words: right to disconnect, telework, home-based work, working time, digital burnout

Úvod

Informačno-komunikačné technológie výrazne transformovali charakter výkonu práce, najmä prostredníctvom digitalizácie pracovných procesov a možnosti pracovať nezávisle od konkrétneho miesta a času. Pri vhodne nastavenom používaní môžu tieto digitálne nástroje prispievať k zlepšeniu rovnováhy medzi pracovným a súkromným životom zamestnancov, keďže umožňujú flexibilitu a autonómiu pri organizovaní pracovného času. Zároveň však využívanie digitálnych technológií na pracovné účely prináša aj viaceré negatívne dôsledky. Medzi najvýraznejšie patrí zvyšovanie intenzity práce a postupné stieranie hraníc medzi pracovným a voľným časom. Neustála dostupnosť a očakávania späté s okamžitou reakciou môžu viesť k tlaku vykonávať pracovné povinnosti aj mimo štandardného pracovného času. Tento fenomén môže mať nepriaznivý vplyv na fyzické i duševné zdravie zamestnancov a prispievať k nárastu psychosociálnych rizík. Medzi časté dôsledky patrí napríklad chronický stres, úzkosť, depresívne symptómy, poruchy spánku, syndróm vyhorenia či technologický stres („technostress“). Dlhodobé pôsobenie týchto faktorov môže výrazne znížiť subjektívnu pohodu jednotlivcov a nepriaznivo ovplyvniť ich pracovný výkon a motiváciu.

Zákonom č. 76/2021 Z. z., ktorým sa mení a dopĺňa zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony bola novelizovaná a zmodernizovaná domácka práca a telepráca a to s účinnosťou od 1.3.2021, pričom do Zákonníka práce bolo pridané aj právo na odpojenie, ale iba vo vzťahu k domáckej práci a telepráci.

Domácka práca a telepráca

Právna úprava telepráce a domácej práce v Slovenskej republike je založená na medzinárodnej dokumentácii a bola významne ovplyvnená mnohými domácimi legislatívami v znení neskorších predpisov, konkrétne Rámcovou dohodou európskych sociálnych partnerov o telepráci z roku 2002 a Dohovorom Medzinárodnej organizácie práce č. 177 o domácej práci z roku 1996. Keďže rámcová dohoda nebola premenená na záväzné sekundárne právo EÚ, bola dôležitým prvkom tzv. mäkkého práva, ktoré bolo navrhnuté s cieľom uviesť do praxe kolektívne vyjednávanie s národným sociálnym dialógom. Hoci Rámcová dohoda nebola začlenená do sekundárneho práva EÚ ako záväzné právo, bola vyvinutá ako podstatný nástroj mäkkého práva, ktorý bol do veľkej miery založený na procese kolektívneho vyjednávania a sociálnej konzultácie na národnej úrovni. Slovenská republika prispela čiastočne začlenením ustanovení o domácej práci a telepráci do § 52 Zákonníka práce. Podľa Rámцovej dohody sa telepráca vzťahuje na prácu, ktorú by zamestnanec mohol vykonávať na pracovisku zamestnávateľa, ale ktorú môže pravidelne vykonávať mimo tohto fyzického pracoviska, zvyčajne z domu. Pravidelnosť neznamena plný výkon týždenne – môže to byť aj kolektívne dohodnutý čiastočný režim (t.j. 1 alebo 2 dni v týždni). Kľúčovým kritériom je opakovateľnosť a predvídateľnosť pracovného výkonu mimo pracoviska. Tento štandard tiež umožňuje rozlíšiť rozdiel medzi domácou prácou/telepracou a príležitostnou prácou z domu, často nazývanou home office. Zatiaľ čo home office nie je v technickom jazyku Zákonníka práce, je často praktizovaný v súvislosti s flexibilnými alebo neformálnymi politikami práce z domu, ktoré postrádajú pravidelné pracovné prvky. Preto je právna úprava Slovenskej republiky založená predovšetkým na konceptoch domácej práce a telepráce, v ktorých je norma pracovného výkonu mimo pracoviska zamestnávateľa, ktorá určuje ich právny režim a povinnosť zamestnávateľa. Treba tiež zohľadniť technologický rozmer pracovného výkonu. Telepráca nie je len o používaní informačných technológií ako nástroja pre prácu zamestnanca, ale o neustálom diaľkovom spojení medzi zamestnancom a zamestnávateľom, alebo dokonca klientom – obojsmerný tok informácií. Keď zamestnanec používa technológiu len na vykonávanie svojich nezávislých úloh (napr. kreslenie na tablete offline), ide skôr o domácu prácu než o teleprácu v zmysle špecifikovanom rámcovou dohodou. V skutočnosti sa zdá, že mnohí zamestnávatelia vybavujú zamestnancov nástrojmi často spojenými s telepracou (notebooky, prístup k firemným systémom), pričom považujú pracovný výkon za príležitostný. To zamieňa rozdiel medzi typmi domácej práce, s dôsledkami pre pracovný status zamestnanca, najmä pokiaľ ide o povinnosť zamestnávateľa podľa § 52 Zákonníka práce – napríklad pokiaľ ide o technické vybavenie, ochranu zdravia na pracovisku alebo náhradu nákladov spojených s prácou z domu. Ak existuje rozdiel v dostupnosti režimu domácej práce pre rôznych

zamestnancov, ani rovnaké zaobchádzanie nesmie byť prehliadané – to znamená, že pracovné podmienky domácej práce a telepráce by nemali zamestnanca znevýhodňovať v porovnaní s porovnateľným zamestnancom pre rovnakú prácu na pracovisku. Ide však primárne o otázku organizácie práce a pracovného času, nie o diskrimináciu v pravom zmysle slova. Základným princípom zakotveným v Rámcovej dohode európskych sociálnych partnerov o telepráci z roku 2002 je, že telepráca musí byť založená na dohode medzi zamestnávateľom a zamestnancom. Tento princíp sa vzťahuje aj na režim domácej práce, v tom zmysle, že oba druhy práce sa vykonávajú mimo pracoviska a ich výkon nemôže byť jednostranne uložený pracovníkovi. Medzitým platí aj to, že zamestnanec nemôže zvoliť miesto práce bez súhlasu zamestnávateľa, podľa vlastného uváženia vykonávať prácu zo svojho miesta trvalého pobytu. Miesto práce je ústredným prvkom pracovnej zmluvy. Aj pre prácu z domu a teleprácu je potom potrebné dohodnúť sa na mieste práce (v pracovnej zmluve alebo jej dodatku). V skutočnosti to znamená, že práca z domu musí mať právny základ podľa princípu konsenzu a inými spôsobmi zamestnanec nemá „jednostranné právo pracovať z domu ako súčasť zamestnania“ zo svojej existujúcej zmluvy. Osobitný režim domácej práce v kontexte telepráce je tiež úzko spojený so štruktúrou pracovného času. Strany pracovného vzťahu by mohli prijať jeden z rôznych modelov stanovených Zákonníkom práce, vrátane rovnomerne rozloženého pracovného času podľa § 86, flexibilného pracovného času podľa § 88, alebo jedného z nerovnomerne rozloženého pracovného času podľa § 87. Na druhej strane môžu tiež vytvoriť celý scenár „samostatného plánovania“ pracovného času zamestnancom, keďže povaha práce umožňuje vykonávanie úloh bez ich vykonávania v skutočnom termíne. V prípade, že pracovný čas je organizovaný zamestnávateľom podľa uvedených ustanovení (§ 86, § 87 alebo § 88), nie je možné uplatniť výnimky podľa § 52 ods. 7 Zákonníka práce, ktoré sa viažu na špecifický režim samostatného rozvrhovania času zamestnancom. Napríklad pri pružnom pracovnom čase (§ 88) síce zamestnanec rozhoduje o začatí a ukončení pracovnej doby v rámci určeného časového rámca, avšak zamestnávateľ stále definuje hranice výkonu práce a podmienky jej organizácie. Naopak, ak sa zamestnávateľ výslovne dohodne so zamestnancom, že rozvrhnutie pracovného času bude plne ponechané na zamestnanca (nebude určovať žiadne časové rámce výkonu práce, napr. konkrétne dni v týždni či minimálne a maximálne denné úseky výkonu práce), vzniká priestor pre aplikáciu výnimiek uvedených v § 52 ods. 7 Zákonníka práce. Tieto výnimky zahŕňajú najmä to, že na samostatne rozvrhnutú domácku prácu/teleprácu sa nevzťahujú ustanovenia o rozvrhnutí pracovného času a o minimálnom dennom a týždennom odpočinku a zamestnanec nemá nárok na niektoré príspevky (napr. náhradu mzdy pri osobných prekážkach či mzdové zvýhodnenia za prácu nadčas, nočnú prácu a sťažený výkon práce), pokiaľ sa so zamestnávateľom nedohodne inak. Pod týmto režimom je zamestnanec konečným rozhodovateľom o počte pracovných

dní, prestávkach, odpočinku a návštevách lekára – najdôležitejší prvok organizačného posunu od rozhodovania zamestnaneckých manažérskych zručností od zamestnávateľa. Preto „samostatné plánovanie“ pracovného času nie je základnou charakteristikou domácej práce alebo telepráce, ale skôr alternatívou, ktorú musia strany výslovne dohodnúť v súlade so špecifickou povahou pracovného vzťahu. Len preto, že zamestnanec pracuje z domu, mu automaticky nepatrí právo nezávisle určovať pracovný rozvrh. Takéto právo je len odvodené od strany dohody, ktorá existuje v zmluve.

Napokon, novela Zákonníka práce zaviedla do § 52 aj ustanovenie o tzv. práve na odpojenie. Podľa § 52 ods. 10 Zákonníka práce má zamestnanec vykonávajúci domáčku prácu alebo teleprácu právo počas nepretržitého denného odpočinku a nepretržitého odpočinku v týždni – ak mu nie je v tomto čase nariadená alebo dohodnutá pracovná pohotovosť či práca nadčas – ako aj počas čerpania dovolenky, počas sviatku, keď práca odpadla, a počas prekážok v práci, nepoužívať pracovné prostriedky slúžiace na výkon domáckej práce alebo telepráce. Zamestnávateľ nesmie posudzovať ako nesplnenie povinnosti, ak zamestnanec odmietne vykonať prácu alebo splniť pokyn v tomto čase. Uvedené ustanovenie teda legislatívne garantuje právo zamestnanca odpojiť sa mimo pracovného času, čo je významné z hľadiska prevencie nadmerného zaťažovania zamestnancov pracujúcich z domu.

Právo na odpojenie

Uplatňovanie domáckej práce a telepráce v aplikačnej praxi prináša popri nesporných výhodách aj viaceré riziká, ktoré sa prejavujú najmä na strane zamestnanca. Rýchly technologický pokrok a rozvoj informačno-komunikačných nástrojov síce umožnili efektívnejší výkon práce mimo tradičných priestorov zamestnávateľa a zároveň vytvorili predpoklady pre lepšie zosúladenie pracovného a rodinného života, no tento vývoj zároveň otvára otázky súvisiace s ochranou súkromia a práva na odpočinok zamestnancov pracujúcich na diaľku.⁴

Jedným z najvýraznejších negatívnych dôsledkov mobilnej práce je stála osobná disponibilita zamestnanca, ktorá v praxi často vedie k narušeniu hranice medzi pracovným a nepracovným časom. Tento jav je dôsledkom implicitného alebo explicitného tlaku na nepretržitú dostupnosť, čo zamestnanca núti byť v pohotovosti aj mimo dohodnutého pracovného času.⁵ V dôsledku toho môže dochádzať k

⁴ Porov. MESSENGER, J., VARGAS LLAVE, Ó., GSCHWIND, L., BOEHMER, S., VERMEYLEN, G. A WILKENS, M. *Working anytime, anywhere: The effects on the world of work*, Luxembourg: Publications Office of the European Union, 2017, s. 25–33.

⁵ V praxi ide často o tzv. „technostres“ – formu stresu vyvolanú nadmernou prácou s digitálnymi technológiami. Pozri Tarafdar, M. – Cooper, C. L. – Stich, J.-F.: *The technostress trifecta – technoeustress, techno distress and design*, in: *Information Systems Journal*, 29(1), 2019, s. 6–42.

digitálnemu preťaženiu, psychickému vyčerpaniu či až k vyhoreniu, čo výrazne znižuje kvalitu pracovného aj osobného života. Zamestnanci vykonávajúci domácku prácu alebo teleprácu preto čelia osobitným psychosociálnym rizikám, medzi ktoré patrí najmä strata kontroly nad vlastným časom, oslabenie oddychových režimov a nárast stresu z permanentnej dostupnosti.⁶

V reakcii na tieto výzvy sa na európskej úrovni začína čoraz viac uplatňovať koncept tzv. práva na odpojenie (right to disconnect), ktoré má za cieľ výslovne priznať zamestnancovi právo neprijímať pracovné pokyny alebo komunikáciu mimo dohodnutého pracovného času. Právo na odpojenie bolo legislatívne zavedené vo Francúzsku už v roku 2016, pričom v rôznych formách ho implementovali aj ďalšie členské štáty ako Belgicko, Taliansko či Írsko.⁷ Na úrovni EÚ Európsky parlament v roku 2021 vyzval Komisiu na predloženie návrhu smernice upravujúcej toto právo, k čomu však doposiaľ nedošlo.⁸ Jednotlivé členské štáty majú respektíve nemajú právnu úpravu práva na odpojenie vo svojich právnych poriadkoch, pričom daná rozličnosť právnej úpravy v praxi neposkytuje zamestnancom rovnakú mieru ochrany a spôsobuje rôzne negatívne následky. Z právneho hľadiska nemožno opomenúť, že právo na odpojenie by mohlo byť chápané ako konkrétna realizácia práva na odpočinok, ktoré je garantované už v článku 31 ods. 2 Charty základných práv EÚ a v smernici 2003/88/ES o organizácii pracovného času. V tejto súvislosti sa začína diskutovať o potrebe zmeny paradigmy v chápaní pracovného času v digitálnom veku, v ktorom tradičné vymedzenie začiatku a konca pracovnej doby prestáva byť postačujúce na ochranu zamestnanca.

Právo na odpojenie je významnou súčasťou stratégie Európskej únie v oblasti bezpečnosti a ochrany zdravia pri práci na obdobie 2021–2027, ktorá osobitne zdôrazňuje potrebu jeho zabezpečenia ako jedného z kľúčových prvkov ochrany zamestnancov v digitálnom pracovnom prostredí. Tento dokument zdôrazňuje potrebu implementácie adekvátnych opatrení na ochranu zamestnancov vykonávajúcich prácu na diaľku alebo využívajúcich digitálne nástroje. Rámec stratégie kladie dôraz na výskum psychologických rizík spojených s digitálnymi a diaľkovými pracovnými prostrediami a podporuje vytvorenie minimálnych

⁶AGALLIU, P., IBRAHIMI, S. The right to disconnect and techno-stress in home-working: A comparative legal and psychological analysis in the European union and the Western Balkans. In: *Edelweiss Applied Science and Technology*, 9(6), .(2025). 79–80. <https://doi.org/10.55214/25768484.v9i6.7756>

⁷ Francúzsky zákon č. 2016–1088 z 8. augusta 2016 o práci, modernizácii sociálneho dialógu a zabezpečení kariér. Belgicko uzákonilo povinnosť prerokovať pravidlá o odpájaní vo firmách s viac ako 20 zamestnancami (zákon z 3. októbra 2022). Írsko vydalo *Code of Practice on the Right to Disconnect* (Workplace Relations Commission, 2021).

⁸ European Parliament resolution of 21 January 2021 with recommendations to the Commission on the right to disconnect (2019/2181(INL)). Dostupné na : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_456_R_0016

štandardov a podmienok, ktoré zabezpečia právo pracovníkov na odpojenie sa od pracovných aktivít mimo bežných pracovných hodín.⁹

Novela Zákonníka práce priniesla nie len úpravu podmienok domáckej práce a telepráce, ale predstavila v Zákonníku práce nový inštitút – právo na odpojenie. Konkrétne §52 ods. 10 Zákonníka práce ustanovuje, že zamestnanec vykonávajúci domácku prácu alebo teleprácu má právo počas jeho nepretržitého denného odpočinku a nepretržitého odpočinku v týždni, ak mu nie je v tomto čase nariadená alebo s ním dohodnutá pracovná pohotovosť alebo práca nadčas, počas čerpania dovolenky, sviatku, pre ktorý práca odpadla, a prekážky v práci nepoužívať pracovné prostriedky slúžiace na výkon domáckej práce alebo telepráce. Zamestnávateľ nesmie posudzovať ako nesplnenie povinnosti, ak zamestnanec odmietne vykonať prácu alebo splniť pokyn v čase podľa predchádzajúcej vety.

Ak zamestnávateľ nevyžaduje nepretržitú osobnú disponibilitu od zamestnancov, ktorí vykonávajú prácu na pracovisku, nemožno túto povinnosť jednostranne preniesť na zamestnancov vykonávajúcich domácku prácu alebo teleprácu. Uplatňovanie takejto asymetrickej požiadavky by mohlo byť kvalifikované ako diskriminácia v zmysle zásady rovnakého zaobchádzania podľa § 13 Zákonníka práce a súvisiacej antidiskriminačnej legislatívy. Z tohto dôvodu odmietnutie vykonávať prácu mimo dohodnutého pracovného času, najmä pri výkone domáckej práce alebo telepráce, nemôže byť považované za porušenie pracovnej disciplíny, pokiaľ nejde o situáciu, ktorá by napĺňala znaky mimoriadnej potreby zo strany zamestnávateľa. Výkon práce mimo pracovného času je prípustný iba za predpokladu, že sú splnené podmienky ustanovené pre prácu nadčas podľa § 97 Zákonníka práce, pričom zamestnancovi patrí príslušné mzdové zvýhodnenie. Výnimočne môže byť požiadavka na pripojenie zamestnanca legitímna v prípade, že je preukázané, že neodkladné pripojenie zamestnanca je nevyhnutné na zabránenie vzniku bezprostrednej a závažnej ujmy zamestnávateľovi, pričom aj v takom prípade musí ísť o časovo ohraničený a výnimočný zásah. Za týchto okolností je vhodné, aby výkon takejto práce bol riadne evidovaný ako nadčasová práca so všetkými z toho vyplývajúcimi právnymi a mzdovými dôsledkami.

Pozitíva a negatíva práva na odpojenie

Právo na odpojenie v kontexte výkonu domáckej práce a telepráce so sebou môže prinášať isté výhody a nevýhody pre zamestnanca aj zamestnávateľa, pričom jeho

⁹ YAROSHENKO, OLEG M., ANATOLII P. GETMAN, VLADYSLAV S. TKACHENKO, OLEG L. MUSIIENKO, MARIYAP. PETROVA. Legal and Policy Dimensions of Using Digital Technologies to Monitor and Manage Working Time in the EU. In: *Információs Társadalom XXIV, no. 4 (2024): 71–72.* <https://dx.doi.org/10.22503/infatars.XXIV.2024.4.4>

najväčší význam a prínos sa osobitne prejavujú na strane zamestnanca.¹⁰ Z pohľadu zamestnanca právo na odpojenie znamená legitímne očakávanie, že mimo dohodnutého pracovného času nie je povinný reagovať na pracovné podnety, najmä vo forme e-mailovej, telefonической alebo inej elektronickej komunikácie.¹¹

Takýto prístup zamestnancovi umožňuje účinne oddeliť pracovný čas od času určeného na regeneráciu, čím podporuje tzv. mentálny a digitálny detox. Vďaka tomu možno účinne zmierniť negatívne dopady technostresu, keďže zamestnancom sa poskytuje väčšia miera autonómie pri stanovovaní jasných hraníc medzi pracovným a súkromným životom. Takto oddýchnutý zamestnanec je následne schopný vykonávať prácu so zvýšenou koncentráciou a efektivitou, čo má nepriamy pozitívny dopad aj na zamestnávateľa v podobe vyššej produktivity.¹²

Zamestnávateľ, aj napriek určitej strate bezprostrednej dostupnosti zamestnanca v mimopracovnom čase získava výhodu v podobe duševne stabilnejšieho a menej vyčerpaného pracovného kolektívu. Právo na odpojenie tak znižuje psychickú záťaž pracovníkov a eliminuje riziko vyhorenia, čím sa posilňuje kultúra dôvery a právnej istoty na pracovisku.

Negatívne dôsledky uplatňovania práva na odpojenie sa v prevažnej miere prejavujú na strane zamestnávateľa. Z pohľadu zamestnávateľa dochádza predovšetkým k zníženiu flexibility v organizácii práce, najmä pokiaľ ide o dostupnosť zamestnanca mimo jeho riadneho pracovného času. Tento aspekt môže byť problematický najmä v rámci medzinárodnej spolupráce kde sa pracovné požiadavky neraz viažu na rozdielne časové pásma. Uvedený problém je však možné čiastočne riešiť prostredníctvom inštitútu pracovnej pohotovosti, za ktorú zamestnancovi prináleží náhrada.

Ďalšou nevýhodou je zvýšená administratívna záťaž, ktorá spočíva v povinnosti zamestnávateľa jednoznačne stanoviť pravidlá a podmienky, za ktorých zamestnanci nie sú povinní reagovať na elektronickej komunikáciu mimo pracovného času. Zamestnávateľ by musel v rámci interných predpisov či kolektívnej zmluvy zabezpečiť aby bolo právo na odpojenie uplatňované v súlade so zásadou rovnakého zaobchádzania čím sa zároveň predchádza riziku diskriminácie. V tejto súvislosti

¹⁰ BARANCOVÁ, H. § 52 [Domácka práca a telepráca]. In: BARANCOVÁ, H. a kol. *Zákonník práce*. 3. vydanie. Bratislava: C. H. Beck, 2022, s. 588

¹¹ LADIVEROVÁ, E., NEVICKÁ, D.: Práca z domu a domácka práca, IN: Bratislavské právnické fórum - Realizácia sociálnych práv v období pandémie / Michaela Durec Kahounová, Silvia Senková, Magdaléna Mydliarová, Tibor Hlinka, Andrea Szakács, (zost.). Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2021 s.85. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2021/Zbornik_BPF_2_021_sekcia_10_Pracovne_pravo_a_pravo_socialneho_zabezpecenia_FINAL.pdf

¹² ALKANDARI, A., BAROUN, A., ALBOLOUSHI, B. (2025). The right to disconnect: Job demands, burnout, and well-being among female teachers and regulatory policy context [Special issue]. In: *Journal of Governance & Regulation*, 14(2), (2025). 300-301. <https://doi.org/10.22495/jgrv14i2siart8>

predstavuje pre zamestnanca aj zamestnávateľa kľúčový aspekt jednoznačné a zrozumiteľné vymedzenie hraníc výkonu pracovnej činnosti a uplatňovania práva na odpojenie. Osobitne dôležité je precízne určiť výnimky z tohto práva, najmä situácie, ktoré si vyžadujú bezodkladné konanie, ako napríklad havarijné poruchy, na ktoré sa právo na odpojenie nebude vzťahovať. Presné a transparentné zakotvenie týchto výnimiek v interných predpisoch zamestnávateľa môže významne prispieť k predchádzaniu potenciálnym pracovnoprávnym dôsledkom pre zamestnanca, najmä v prípadoch, keď by jeho nereagovanie na mimoriadnu situáciu mohlo byť vyhodnotené ako porušenie pracovnej disciplíny (napr. ak by mohlo zamestnávateľovi privodiť závažnú škodu).¹³ V závislosti od konkrétnych okolností môže takéto konanie zamestnanca viesť k ukončeniu pracovného pomeru výpoveďou podľa § 63 ods. 6 Zákonníka práce, alebo v prípade závažného porušenia pracovnej disciplíny aj k jeho okamžitému skončeniu podľa § 68 ods. 1 písm. b) Zákonníka práce.

Zamestnanci môžu čeliť aj negatívnym dôsledkom zavedenia práva na odpojenie. Ide najmä o prípad keď určitá časť zamestnancov z vlastnej iniciatívy komunikuje so zamestnávateľom aj mimo pracovného času, často z obavy o udržanie svojho pracovného miesta alebo z dôvodu domnienky, že takéto správanie bude zamestnávateľom pozitívne hodnotené v rámci mzdového ohodnotenia.¹⁴ Týmto spôsobom však vzniká nepriamy tlak na ostatných zamestnancov, ktorí sa rozhodnú právo na odpojenie reálne uplatňovať čím môže dôjsť k narušeniu rovnosti medzi zamestnancami a k oslabeniu účelu práva na odpojenie práva.

Právo na odpojenie predstavuje právny nástroj, ktorý vhodným spôsobom vyvažuje legitímne záujmy oboch strán pracovnoprávneho vzťahu. Jeho správna aplikácia si však vyžaduje nielen legislatívne ukotvenie, ale aj kultivovanú pracovnú kultúru rešpektujúcu hranice pracovného času aj v prostredí flexibilných foriem práce.

Pri výhodách a nevýhodách sa naskytá aj otázka, či by sa právo na odpojenie nemohlo primerane uplatniť aj vo vzťahu k zamestnancom, ktorí nevykonávajú prácu prostredníctvom domáckej práce alebo telepráce. V kontexte súčasnej technologickej vyspelosti a digitalizácie pracovného prostredia by sa právo na odpojenie nemalo obmedzovať výlučne na zamestnancov vykonávajúcich prácu formou domáckej práce alebo telepráce. Väčšina zamestnancov dnes využíva

¹³ BARANCOVÁ, H.: Nová právna úprava domáckej práce a telepráce .In: *Právny obzor*, 105, 2022, č. 1, s. 15. <https://doi.org/10.31577/pravnyobzor.2022.1.01>

¹⁴ LAZAR, O. Taking it home with you: work, free time, and domination. In: *Critical review of international social and political philosophy*. (2025) . DOI: 10.1080/13698230.2025.2546288. Dostupné na: https://www.tandfonline.com/doi/epdf/10.1080/13698230.2025.2546288?src=getft&utm_source=scopus&getft_integrator=scopus . s. 14

digitálne nástroje pri výkone práce aj keď pracuje priamo na pracovisku.¹⁵ Navyše, mnohí z týchto zamestnancov si, či už z vlastnej iniciatívy alebo na podnet zamestnávateľa prenášajú pracovné povinnosti do svojho súkromného priestoru. Preto sa často vyskytujú situácie, keď zamestnávateľ kontaktuje zamestnanca po skončení pracovnej doby v súvislosti s tzv. „naliehavou“ pracovnou úlohou, ktorá však v mnohých prípadoch nemá charakter mimoriadnej udalosti alebo ohrozenia života či zdravia, ale je urgentná najmä z pohľadu ekonomických záujmov zamestnávateľa. Zamestnanec v takýchto prípadoch často opätovne nastupuje do výkonu práce mimo určeného pracovného času, čím dochádza k narušeniu jeho práva na nepretržitý odpočinok, ako aj k obmedzeniu práva na súkromie a odpočinok. Z hľadiska rovnakého zaobchádzania možno preto argumentovať, že právo na odpojenie by malo byť priznané všetkým zamestnancom, pri ktorých to povaha práce a organizačné podmienky umožňujú, a to bez ohľadu na to, či vykonávajú prácu na diaľku alebo na pracovisku. Takéto rozhodnutie by mohlo významne prispieť k zníženiu rizika syndrómu vyhorenia, k podpore duševného zdravia zamestnancov a k celkovému zlepšeniu pracovnej kultúry.

Problematickým však zostáva fakt, že nie všetci zamestnanci majú objektívnu možnosť odpojiť sa, najmä v povolaniach s vysokou mierou nepredvídateľnosti, alebo kde pracovné procesy vyžadujú nepretržitý dohľad či zásah. Rovnako môže byť pri flexibilnom pracovnom čase zložitým jednoznačne určiť, kedy zamestnanec vykonáva prácu a kedy je mimo pracovného času. Napriek týmto výzvam možno konštatovať, že rozšírenie uplatnenia práva na odpojenie aj na bežných zamestnancov, ktorí nevykonávajú prácu z domu by mohlo mať pozitívny vplyv nielen na ich pracovnú pohodu a psychické nastavenie, ale aj na celkovú rovnováhu medzi pracovným a súkromným životom.

Záver

Právo na odpojenie predstavuje moderný právny inštitút, ktorý reflektuje výzvy digitalizácie pracovného prostredia a rastúce požiadavky na ochranu duševného zdravia zamestnancov. Z hľadiska jeho aplikačného rozsahu ide o nástroj, ktorý by mal byť systematicky rozvíjaný a rozširovaný aj mimo rámca domáckej práce a telepráce. Skúsenosti viacerých členských štátov EÚ ukazujú, že právo na odpojenie má potenciál významne prispieť k posilneniu rovnováhy medzi pracovným a

¹⁵ SÍPOS, Á. Právo na digitálny detox - regulácia pracovného času a súkromia zamestnanca, In: *Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia* / Nikola Bezáková, Ádám Sípos, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. s. 194. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2023/BPF_2023_prac_ovne_pravo_.pdf

súkromným životom, k prevencii syndrómu vyhorenia a k zlepšeniu celkovej pracovnej pohody zamestnancov.

Slovenská právna úprava predstavuje prvý krok správnym smerom, avšak jej aktuálne obmedzený rozsah poukazuje na potrebu ďalšej legislatívnej a aplikačnej diskusie. Dôležitá je aj aktívna úloha zamestnávateľov pri vytváraní zrozumiteľných pravidiel a transparentných mechanizmov uplatňovania tohto práva, vrátane nastavenia výnimiek a zabezpečenia rovnakého zaobchádzania medzi zamestnancami.

Do budúcnosti bude nevyhnutné uvažovať o rozšírení práva na odpojenie na širší okruh zamestnancov a o jeho zakotvení v rámci celoeurópskej právnej úpravy, aby bola zabezpečená jednotná úroveň ochrany pre všetkých pracovníkov v digitálnom veku. Skutočná účinnosť tohto práva však závisí nielen od právnych predpisov, ale aj od kultúry práce, ktorá rešpektuje hranice medzi pracovným a osobným priestorom každého jednotlivca.

Zoznam použitej literatúry

1. ALKANDARI, A., BAROUN, A., & ALBOLOUSHI, B., The right to disconnect: Job demands, burnout, and well-being among female teachers and regulatory policy context [Special issue]. In: *Journal of Governance & Regulation*, 14(2), (2025). 299–309. <https://doi.org/10.22495/jgrv14i2siart8>
2. AGALLIU, P., IBRAHIMI, S. The right to disconnect and techno-stress in home-working: A comparative legal and psychological analysis in the European union and the Western Balkans. In: *Edelweiss Applied Science and Technology*, 9(6), (2025). 79–94. <https://doi.org/10.55214/25768484.v9i6.7756>
3. BARANCOVÁ, H.: Nová právna úprava domáckej práce a telepráce . In: *Právny obzor*, 105, 2022, č. 1, s. 3 – 18. <https://doi.org/10.31577/pravnyobzor.2022.1.01>
4. BARANCOVÁ, H. § 52 [Domácka práca a telepráca]. In: BARANCOVÁ, H. a kol. *Zákonník práce*. 3. vydanie. Bratislava: C. H. Beck, 2022, s. 576 - 591
5. BENKO, M. – MORAVČÍKOVÁ, K. – PIROŠÍKOVÁ, M.: *Pracovné právo*. C. H. Beck, Bratislava, 2022, s. 203–206.
6. Dohovor Medzinárodná organizácia práce č. 177 o práci doma z roku 1996
7. MESSENGER, J., VARGAS LLAVE, Ó., GSCHWIND, L., BOEHMER, S., VERMEYLEN, G. A WILKENS, M. *Working anytime, anywhere: The effects on the world of work*, Luxembourg: Publications Office of the European Union, 2017, s. 25–33.
8. European Parliament resolution of 21 January 2021 with recommendations to the Commission on the right to disconnect (2019/2181(INL)). Dostupné na : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_456_R_0016

9. LADIVEROVÁ, E., NEVICKÁ, D.: Práca z domu a domácka práca, IN: *Bratislavské právnické fórum - Realizácia sociálnych práv v období pandémie* / Michaela Durec Kahounová , Silvia Senková , Magdaléna Mydliarová , Tibor Hlinka, Andrea Szakács, (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2021 s. 83-87 Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2021/Zbornik_BPF_2021_sekcia_10_Pracovne_pravo_a_pravo_socialneho_zabezpecenia_FINAL.pdf
10. LAZAR, O. Taking it home with you: work, free time, and domination. In: *Critical review of international social and political philosophy*. 2025 . DOI: 10.1080/13698230.2025.2546288. Dostupné na: https://www.tandfonline.com/doi/epdf/10.1080/13698230.2025.2546288?src=get_ft&utm_source=scopus&getft_integrator=scopus . s. 14
11. Rámcová dohoda o telepráci bola uzatvorená medzi UNICE/UEAPME, CEEP a ETUC dňa 16. júla 2002
12. SÍPOS, Á. Právo na digitálny detox - regulácia pracovného času a súkromia zamestnanca, In: *Bratislavské právnické fórum 2023 : technologické a etické výzvy pre pracovné právo a právo sociálneho zabezpečenia* / Nikola Bezáková, Ádám Sípos, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2023. 187-197 s. ISBN 978-80-7160-698-7. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2023/BPF_2023_pracovne_pravo .pdf
13. ŠVEC, M.- TOMAN, J. a kol. Zákoník práce. Zákon o kolektívnom vyjednávaní. Komentár. Zväzok 1. 2, doplnené a prepracované vydanie Bratislava.: Wolters Kluwer, 2023, s. 2776
14. TARAFDAR, M. – COOPER, C. L. – STICH, J.-F.: The technostress trifecta – techno eustress, techno distress and design, In: *Information Systems Journal*, 29(1), 2019, s. 6–42.
15. YAROSHENKO, OLEG M., ANATOLII P. GETMAN, VLADYSLAV S. TKACHENKO, OLEG L. MUSIIENKO, MARIYAP. PETROVA. Legal and Policy Dimensions of Using Digital Technologies to Monitor and Manage Working Time in the EU. In: *Információs Társadalom XXIV*, no. 4 (2024): 62–78. <https://dx.doi.org/10.22503/inftars.XXIV.2024.4.4>
16. Zákona č. 311/2001 Z. z. Zákoník práce v znení neskorších predpisov

Kontaktné údaje

doc. JUDr. Lenka Freel, PhD.
lenka.freel@flaw.uniba.sk

Univerzita Komenského v Bratislave
Právnická fakulta
Katedra pracovného práva a práva sociálneho zabezpečenia

Mgr. Soňa Kašická
sona.kasicka@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta
Katedra pracovného práva a práva sociálneho zabezpečenia

HUMAN ENHANCEMENT, ROBOTICS AND AI: THE CONSEQUENCES FOR THE LABOUR MARKET

Massimiliano Delfino¹

Abstract: This paper analyses the implications of human enhancement for labour law and the labour market, with a particular focus on disability, occupational health and safety, and the impact of artificial intelligence. The aim is to examine how technological, pharmacological, and biotechnological interventions, designed to increase human capacities, interact with existing legal frameworks and reshape the boundaries between therapy and enhancement. The methodology is based on a legal analysis of national and European provisions, including references to constitutional principles and statutory provisions, combined with case studies of emerging technologies such as exoskeletons and cognitive enhancement tools. The main findings suggest that human enhancement may influence the legal definition of disability, impact access to welfare and social security systems, and introduce new risks in the workplace that current health and safety regulations only partially address. This paper also identifies challenges associated with robotics and artificial intelligence and examines the ethical and legal issues raised by cognitive enhancement in the context of employment relations. The contribution lies in outlining possible regulatory directions and highlighting the role of social partners in ensuring that human enhancement develops consistently with labour law principles.

Key words: human enhancement, labour law, disability, exoskeletons, artificial intelligence.

The meaning of human enhancement

It is appropriate to begin with the defining profiles. Human enhancement refers to any intentional modification of the human body, not intending to make disabled or sick people able-bodied or healthy, but to make healthy people better than those in good health and disabled people not only normal, but beyond normal. In other words, it is about raising the threshold of what is considered 'normality' in humans². Perhaps, a more pragmatic approach is to disregard a general definition of human

¹ Faculty of Law, University of Naples Federico II, Naples, Italy

² GREELY, Henry T.: *Remarks on Human Biological Enhancement*. In: 56 *Kansas Law Review*, 2008, p. 1139-1140.

enhancement and refer instead to three core topics or, rather, three areas of investigation:

1. "enhancement through the implantation of technological devices in the human body", known as *Empowerment*;
2. the "enhancement achievable through pharmacological or biotechnological interventions capable of altering a person's cognitive abilities", known as *Cognitive Enhancement*;
3. enhancement passed on to future generations by altering the genetic makeup.

The last of these areas is the most futuristic but probably also the furthest removed from labour law, since it is not yet possible to 'design' individuals who genetically possess the physical or intellectual qualities suited to this or that type of work, not least because such practices are at high risk of being considered unlawful, as demonstrated by a key provision of the Charter of Fundamental Rights of the European Union, Article 3(2), which establishes the 'prohibition of eugenics practices, in particular those aimed at the selection of persons', including for employment purposes.

Another point that should be made clear right away is that artificial intelligence does not necessarily play a significant role in human enhancement. It has no role at all in the second and third areas mentioned above, since neither pharmacological nor biotechnological techniques nor hereditary enhancement are based on AI.

This refers to physical *empowerment*, which can also be achieved through devices that use AI. However, I will return to this shortly.

More Able vs. Differently Abled at Work?

As can be seen, the division by field of investigation allows the issue of disability to be included within each of the categories.

An essential aspect of the debate on enhancement is determining whether a particular technology can restore or improve a human function.

It is not easy to draw the line between restoration and enhancement.

Firstly, it should be noted that most restoration technologies are ambivalent, as they can also be applied for enhancement purposes. Secondly, these technologies were initially developed precisely for therapeutic purposes.

Having clarified that eugenics will not be addressed, the first and second thematic areas require us to consider various aspects, starting with the very notion of disability, which the use of empowerment or enhancement techniques could alter. Consider, for example, the concept contained in Article 3(1) of Law No. 104/1992, which refers to a person 'who has a physical, mental or sensory impairment, whether stable or progressive, which causes difficulties in learning, relating to others or integrating into

the workplace and which leads to social disadvantage or marginalisation' or, again, to persons with severe disabilities, as provided for in Article 3(3) of the same law, according to which 'if the impairment, whether single or multiple, has reduced personal autonomy, in relation to age, to such an extent that permanent, continuous and comprehensive assistance is required in the individual's personal or relational sphere, the situation is considered to be serious'.

It is also helpful to recall the general concept of disability contained in Article 1 of Law No. 68/1999 (Provisions for the right to work of persons with disabilities), a measure aimed at the inclusion and integration into the workplace of a group of persons that partly coincides with that indicated in Law No. 104/1992³.

The issue is also evident in the field of social security protection, where the condition of disability, known as pensionable disability, occurs if the worker has a 'working capacity, in occupations suited to his or her aptitudes, ... permanently reduced to less than one third due to physical or mental infirmity or defect'⁴.

Furthermore, "for the purposes of obtaining pension rights under compulsory disability insurance ..., an insured person ... who, due to physical or mental illness or disability, is absolutely and permanently unable to perform any work activity" is considered disabled⁵.

Similar considerations could be made for welfare protection recognised through civil disability and civil incapacity⁶.

³ 5 'a) ... persons of working age with physical, mental or sensory impairments and ... persons with intellectual disabilities, resulting in a reduction in working capacity of more than 45%, as ascertained by the competent commissions for the recognition of civil disability in accordance with indicative table of disability percentages for impairments and disabling diseases approved, pursuant to Article 2 of Legislative Decree No. 509 of 23 November 1988, by the Ministry of Health based on the international classification of impairments developed by the World Health Organisation...;

b) ... persons with a degree of disability exceeding 33%, as ascertained by the National Institute for Insurance against Accidents at Work and Occupational Diseases (INAIL) ...;

c) ... blind or deaf-mute persons, as referred to in Laws No. 382 of 27 May 1970, as amended, and No. 381 of 26 May 1970, as amended;

d) ... persons disabled as a result of war, civilian war invalids and persons disabled as a result of service with impairments classified in categories 1 to 8 as referred to in the tables attached to the consolidated text of the regulations on war pensions, approved by Presidential Decree No. 915 of 23 December 1978, as amended.

⁴ Art. 1, paragraph 1, Law No. 222/1984 (italics added by the author).

⁵ Art. 2, paragraph 1, Law No. 222/1984 (italics added by the author).

⁶ According to Article 2, paragraph 1, Law No. 118/1971, "citizens with congenital or acquired impairments, including progressive ones, are considered disabled and incapacitated, including those with mental disorders due to organic or metabolic oligophrenia, mental deficiencies resulting from sensory and functional defects that have suffered a permanent reduction in working capacity of not less than one third or, if under the age of 18, who have persistent difficulties in performing the tasks

Human enhancement techniques (using technological and pharmacological devices) are increasingly able to affect individuals' working capacity, both physically and cognitively, so that they can recover at least part of *the deficits* on which the recognition of social security and welfare benefits and the benefits deriving from Law No. 104/1992 are based.

Of course, there are various problems, starting with the high costs of these technologies, which, if they were to decrease, would make their use more affordable. In particular, the use of these technologies could enable the partial recovery of specific disabilities, thereby reducing the need for regulatory benefits, welfare, and social security protections.

While the former (e.g., paid leave under Law No. 104/1992) are at least partially borne by employers, the latter are borne by the public; thus, in the long run, it may be more cost-effective for the State to invest in human development and promote the use of new technologies.

Of course, it remains the case that it is not possible to force disabled workers and citizens to use this equipment, but the more advanced and easier-to-use it is, the more likely it is to be accepted by those concerned. This also applies to the most advanced pharmacological and biotechnological devices that may be able to improve certain types of disability, such as cognitive disabilities. This is also crucial from the labour market perspective, which is the topic of this session.

Empowerment: the challenges of robotics

Among the many non-cognitive human enhancement mechanisms, those most closely related to artificial intelligence are undoubtedly exoskeletons, as they frequently utilise robotic technology that could leverage AI⁷.

It should be clarified immediately that exoskeletons are wearable devices but not wearable devices in the sense of the term used in the so-called Internet of Things, i.e. 'devices that, using software applications and sensors, are used for monitoring, localisation and measurement purposes'⁸.

Therefore, the difference lies in the purpose of the devices, which, in the case of exoskeletons, is to augment human capabilities. This purpose is not irrelevant to labour law, as the legal issues to be addressed depend on it. Wearable devices mainly raise issues of privacy and protection of the worker's consent, while for exoskeletons,

and functions appropriate to their age." "Civilian amputees and invalids over the age of 18 who, following a medical examination, are found *to be totally unable to work*, are granted a disability pension by the State and administered by the Ministry of the Interior" (Article 12, Law No. 118/1971).

⁷ On this point, see FIATA, Emanuela: *Robotica e Lavoro*, in M. Biasi (ed.), *Diritto del lavoro e intelligenza artificiale*, Milan, 2024. p.611.

⁸ BRINO, Vania: *Wearable devices*, in S. BORELLI et al, *Lavoro e tecnologie. Dizionario del diritto del Lavoro che cambia*, Turin, 2022. p. 223.

the problems go far beyond.

To better define the characteristics of exoskeletons, it is necessary to understand what is meant by 'robot' and 'robotic device', since, as mentioned above, this type of technology often forms the basis of exoskeletons. A robot is a programmable mechanism with two or more axes that has a certain degree of autonomy, which moves within its environment to perform specific tasks. It consists of a control system and an interface with that system. A robotic device is a mechanism that exhibits the characteristics of a robot but lacks programmable axes or any degree of autonomy. In this context, it is not possible to address all the issues concerning human empowerment through robotics; therefore, I have chosen to focus on the most pressing one, namely, work performance and workplace safety⁹.

Exoskeletons can be classified as active or passive. The former use actuators (mechanical drive components) to support human movements, and most of them utilise electric motors, although there are examples of pneumatic actuation¹⁰. A computer programme based on sensor information controls the action of the actuators during operation.

Passive exoskeletons, on the other hand, use the force generated by elastic bands, shock absorbers or other materials to support human movement. The user's movements generate the energy stored in the exoskeleton.¹¹

Additionally, forces are redistributed to protect specific areas of the body. The change in user performance does not result from additional physical strength, but from the ability to maintain fatigued positions for a longer period.

Starting with safety, for workers who wear professional exoskeletons (both active and passive), various risk scenarios can be imagined in relation to their prolonged use. In this regard, the French *Institut National de Recherche et de Sécurité* has identified new risk factors associated with the workplace resulting from the use of exoskeletons¹².

⁹ For information on occupational safety profiles, see MARASSI, Stefania: *Intelligenza artificiale e sicurezza sul lavoro*, in M. Biasi, op. cit., 207.

¹⁰ AIDA, Takamitsu – NOZAKI, Hirokazu – KOBAYASHI, Hiroshi: Development of a muscle suit and application to factory labourers. Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation, IEEE, 9–12 August 2009, Changchun, China. p. 1027–1032; INOSE, Hiroshi – MOHRI, S. – ARAKAWA H. – OKUI, M. – KOIDE, K. –YAMADA, Y. –KIKUTANI, I. – NAKAMURA, T.: Semi-endoskeleton-type waist assist ABwear suit equipped with compressive force reduction mechanism. Proceedings 2017 IEEE International Conference on Robotics and Automation (ICRA) Singapore, 29 May–3 June 2017, p. 6014–6019.

¹¹ DE LOOZE, Michiel P. – BOSCH, T. – KRAUSE, F. – STADLER, K. S. – O'SULLIVAN, L. W.: Exoskeletons for industrial application and their potential effects on physical workload, in: *Ergonomics*, Vol.59, 5 (2016), p. 671-681.

¹⁵ For example, an electric assist device, a teleoperated device, an industrial manipulator.

¹² INRS, *Acquisition et integration d'un exosquelette en entreprise: Guide pour les préventeurs*, Institut National de Recherche et de Sécurité, 2019, Paris, www.inrs.fr.

On the one hand, exoskeletons can represent an opportunity to reduce muscle, joint and bone strain by supporting workers, preventing musculoskeletal disorders or aiding workers with physical impairments.

On the other hand, new potential health risks may arise precisely because physical strain is redistributed to different parts of the body¹³.

There are also some technical, safety, and ergonomic issues that need to be considered and resolved before implementing professional exoskeletons on a large scale. One of the main problems could be, for example, the level of discomfort caused by wearing the exoskeleton¹⁴.

After highlighting the biomechanical advantage, eliminating discomfort for the user wearing the device could be the next challenge in exoskeleton design, considering that even a minimal level of discomfort could hinder its acceptance.

Another problem with passive devices is the potential for increased muscle activity in the upper and lower limbs, which must be taken into consideration in further product development. Active exoskeletons, on the other hand, may have greater potential than passive ones, lightening the load on many joints in the body. However, with the increase in the number of joints, related actuators and power supply, the weight of the exoskeleton is bound to increase.

The use of anthropomorphic exoskeletons would be highly beneficial. These exoskeletons have a structure similar to that of the human body, featuring a series of powered joints. These devices have certain advantages over non-anthropomorphic exoskeletons, such as their reduced bulk, as they are directly connected to the body.

Another concern is that there are still no international safety standards for the professional application of exoskeletons, which is a significant obstacle to their adoption. To date, only *soft law* sources at the global level have been identified that provide helpful guidance but do not give rise to any legal obligations. This refers to the ISO¹⁵ technical standards, which include safety requirements for industrial robots

¹³ EU-OSHA - European Agency for Safety and Health at Work: Work-related musculoskeletal disorders: Prevalence, costs and demographics in the EU. European Risk Observatory, 2019, Bilbao, Spain.

¹⁴ For example, ABDOLI, Mohammad E. – AGNEW, Michael J. – STEVENSON, Joan M.:

An on-body personal lift augmentation device (PLAD) reduces EMG amplitude of erector spinae during lifting tasks. In: Clinical Biomechanics, Vol. 21, 5 (2006), p. 456-465.

¹⁵ ISO is an acronym that stands for *International Organisation for Standardisation*. It is the world's most crucial organisation responsible for defining technical standards, also known as ISO standards. These include standards relating to management systems. All companies manufacture products or provide services. These products and/or services may have different requirements and characteristics depending on customer needs, applicable mandatory standards and what the organisation intends to offer to its market. However, certain factors must be strictly complied with if a standardised product or service is to be placed on the market, i.e. one that is manufactured in accordance with specific

and collaborative *robots*.

Although these sources are not binding, they serve as a reference model for companies operating in the robotics sector, as they may be encouraged to adopt these standards to increase their market success.

Possible interconnections with Artificial Intelligence

It should be reiterated that robotics is often linked to the topic of artificial intelligence, as AI-based systems can be easily divided into two categories:

1. *software* that operates in the virtual world (voice assistants, search engines, etc.) and
2. *software* that can incorporate AI into *hardware* devices, such as *robots* and exoskeletons¹⁶.

Considering the need to regulate *robots* that act autonomously, the European Parliament adopted a resolution on 16 February 2017, making recommendations to the Commission on civil law rules for robotics, specifically civil liability profiles for any damage caused by such robots. Robotisation processes can have a significant impact on the organisation and labour market, in relation to which the Resolution highlights the problem of the lack of skills to fill vacancies, the need to monitor job losses, the need to ensure respect for fundamental rights and health and safety standards in the workplace by transferring specific dangerous and harmful tasks from humans to *robots*, but also the risks of deterioration caused by new threats due to the growing number of *human/robot* interactions.

This resolution confirms what was said earlier. In one or two points, the European Parliament emphasises the link between robotics and AI.

In fact, "considers that a comprehensive EU system for the registration of advanced *robots* in the internal market should be introduced..., where necessary and relevant for specific categories of *robots*, and calls on the Commission to establish criteria for the classification of *robots* to be registered" (paragraph 2). For these reasons, the

internationally recognised requirements. These requirements are contained in the ISO standards. In the case of management systems, the concept is the same, but it is applied to the management of business processes. In other words, products or services are created through a sequence of processes that each company can manage in the way it deems most appropriate. One of the methods that it can choose is the one proposed in the Technical Standards defined by ISO. In particular, refer to ISO/DIS 18646-4 of 2021, which outlines performance criteria and related test methods for lumbar support robots. Additionally, consider general standards such as EN ISO 10218-1:2011 and ISO/TS 15066:2016, which establish safety requirements for industrial *robots* and collaborative *robots*.

¹⁶ ZAPPALÀ, Loredana: *Intelligenza artificiale* (voce). in: S. BORELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie*, Turin, 2022, p. 133. On profiles of robotics applied to work, see MAIO, Valerio: *Il Lavoro e le nuove sfide della rivoluzione robotica*. In: ADL, 2018, p. 1415 ff.

Commission is asked to consider establishing an EU agency for robotics and artificial intelligence to "provide the technical, ethical and regulatory expertise necessary to support the efforts of relevant public actors, at both Union and Member State level, to ensure a timely, ethical and well-informed response to the new opportunities and challenges...arising from the technological development of robotics" (paragraph 16). Parliament notes the 'great potential offered by robotics to improve workplace safety by transferring certain dangerous and harmful tasks from humans to *robots*, but at the same time points out that it can also create several new risks due to the increasing number of interactions between humans and robots in the workplace; stresses, in this regard, the importance of applying strict and forward-looking rules to interactions between humans and *robots* to ensure health, safety and respect for fundamental rights in the workplace' (paragraph 46).

For this reason, the annex to the Resolution contains many recommendations, such as the Code of Ethics and Professional Conduct for Robotics Engineers, which emphasises that 'research activities in the field of robotics should respect fundamental rights and, in their design, implementation, dissemination and use, should be conducted in the interests of the well-being and self-determination of the individual and society as a whole'.

In other words, 'human dignity and autonomy — both physical and psychological — must always be respected'.

Obviously, the links between the Regulation on Artificial Intelligence¹⁷, on the one hand, and robots and exoskeletons, on the other, will need to be examined in various aspects, starting with the issue of risk classification, which forms the basis of the new European Union legislation.

The statements contained in the 2017 European Parliament Resolution allow us to briefly mention the link between empowerment and human dignity.

Without investigating the notion of dignity in its various meanings, it is necessary to verify whether and, if so, how the technologies referred to in this context are linked to the protection of dignity understood as the endowment or irreducibility of man to *res*¹⁸.

On closer inspection, human enhancement tools do not seem to give rise to the commodification of the human body underlying this notion of dignity, as clearly exemplified by Article 3(1) of the Charter of Fundamental Rights of the European Union, which establishes 'the prohibition on making the human body and its parts as such a source of financial gain'.

¹⁷ On these issues, see, *among others*, PERUZZI, Marco: *Intelligenza artificiale e lavoro. Uno studio sui poteri datoriali e sulle tecniche di tutela*, Turin, 2023.

¹⁸ CASILLO, Rosa: *Diritto al lavoro e dignità*, Editoriale scientifica, 2020, chapter two. Specifically, see BERTOLINI, Andrea: *Governare il potenziamento umano attraverso i principi di dignità e uguaglianza*. in: *Politica del diritto*, Vol. LIII, 3 (2022), p. 433 ff.

Cognitive enhancement and the new frontiers of medicine and biotechnology

The time has come to address the issue of enhancement through pharmacological and biotechnological devices, commonly referred to as *cognitive enhancement*.

This type of enhancement has its origins in sports, as is well known, since competitive athletes sometimes use chemical or biological products to enhance their performance.

In this regard, Article 1(2) of Italian Law No. 376/2000 states that 'doping consists of the administration or intake of drugs or biologically or pharmacologically active substances and the adoption of or submission to medical practices not justified by pathological conditions and suitable for modifying the psychophysical or biological conditions of the organism to alter the competitive performance of athletes'.

The law does not apply to employment relationships, so there is no general prohibition on the use of such substances for the purpose of enhancing work performance¹⁹.

Of interest in this regard is the 2017 European Union Regulation²⁰, which sets out a series of restrictions on the production, marketing and commissioning of medical devices for human use, including those capable of achieving non-pharmacological cognitive enhancement, such as 'products intended to be introduced wholly or partially into the human body by invasive surgical means for the purpose of modifying the anatomy or for fixing parts of the body' and also 'equipment intended for brain stimulation that applies electrical currents or magnetic or electromagnetic fields through the skull to modify the brain's neuronal activity'²¹.

Returning to drugs, these are substances produced to treat certain diseases, which, when administered to healthy individuals, result in cognitive enhancement.

As these are clearly not over-the-counter products, and regardless of the issue of their sale on the black market, it should be noted that they are subject to a medical prescription.

Therefore, it is helpful to refer to Article 76 of the Italian Code of Medical Ethics, a provision amended on 15 December 2017 and appropriately titled 'Enhancement

¹⁹ The drugs referred to are based on nootropic substances that are believed to improve certain mental states such as attention, concentration, memory or motivation. More generally, this category also includes substances that can promote the acquisition of motor or affective skills, such as the ability to manage anxiety associated with performing certain work activities, or that promote confidence and a sense of belonging. See BLOOMFIELD, Brian – DALE, Kate: Fit for work? Redefining 'Normal' and 'Extreme' through human enhancement technologies. In: Organisation, Vol.22, 4(2015), p. 552-5.

²⁰ This is Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

²¹ Annex XVI, Nos. 2 and 6. On this point, see PIZZETTI, Federico G.: Potenziamiento umano e principio lavorista. Spunti di riflessione. In: Rivista di filosofia del diritto, Vol. VII, 2 (2018), p. 265 ff.

Medicine', according to which 'the doctor, ... when asked to perform non-therapeutic services aimed at enhancing the individual's physiological physical and cognitive abilities, shall act in accordance with and safeguard the dignity of the individual in all its individual and social aspects, the identity and integrity of the person and their genetic characteristics, as well as the principles of proportionality and precaution' (para. 1). Furthermore, in such cases, 'the physician shall obtain informed consent in writing, taking care to verify ... the patient's understanding of the risks of the treatment ... [and] shall have a duty to refuse any requests deemed disproportionate and high-risk, including due to the invasiveness and potential irreversibility of the treatment in relation to non-therapeutic but enhancement-oriented benefits'.

In short, the doctor is required to obtain consent from the person concerned for this type of treatment and undertakes not to prescribe such drugs if the request is disproportionate and highly risky.

This implies that even consent to enhancement treatment is insufficient if the risk is high, not least because, ultimately, what is at stake is once again the value of dignity, this time understood not only in its individual sense but also in its social context²².

The issue of consent concerns the prescription of drug treatment, while another aspect is that of the hidden enhancement of the worker.

In fact, there does not seem to be any legal provision obliging workers to disclose the use of performance-enhancing drugs either during the pre-employment phase or during the employment relationship. Still, as argued in doctrine²³, this entails, especially before the start of the employment relationship, the risk of violating the principle of equality and, in the case of public employment, also the principle of impartiality and access through competition referred to in Article 97 of the Constitution.

Furthermore, it should be noted that, in the public sector, Article 55-*quater*, paragraph 1, letter c) of Italian Legislative Decree 165/2001 provides for the application of the penalty of dismissal in the event of 'false documents or declarations made for or during the establishment of the employment relationship or of progression of career advancement', a scenario that would occur in the case of hidden cognitive enhancement. The problem, therefore, is to make this enhancement clear, and this can be achieved, in the case of drug administration, through diagnostic laboratory tests. However, the employer cannot impose these tests either during the pre-employment phase or during the employment relationship, except in specific cases. One such case is the recruitment of military personnel, which is subject to conditions, including the assessment of fitness for military service,

²² CASILLO, Rosa: *cit.*, p. 79 ff.

²³ MAIO, Valerio: *Diritto del lavoro e potenziamento cit.*, p. 531-533.

conducted through general and specialist medical examinations²⁴. These examinations often involve rather detailed diagnostic tests capable of ascertaining the use of substances, which, if not justified for the treatment of specific pathologies, could lead to a declaration of unsuitability and the consequent failure to take up service.

They are intended to treat specific conditions. This is what happened in another case that attracted the attention of administrative case law²⁵, in which a person suffering from a syndrome dependent on altered endocrine gland function was declared fit for recruitment to the prison police. In theory, this would be a cause for unsuitability for recruitment; however, this was not the case in this instance, as the applicant had normal thyroid function, albeit due to the medication they were taking.

This issue was at the centre of a 2010 ruling by the Italian Council of State concerning the case of an aspiring Navy recruit who was deemed unfit for recruitment through a competitive examination due to testing positive for opiates 29.

According to the administrative judges, it is not sufficient for a candidate in a public competition who is subject to a psycho-physical fitness assessment to provide '*ex post*' justification for the presence in biological fluids of substances expressly indicated by the relevant legislation as grounds for unsuitability.

On the contrary, the candidate has the responsibility to provide the relevant commission with prior information, during the personal medical history interview, about any occasional circumstances that could invalidate the medical examination for entirely contingent reasons.

In other words, the Council of State considers that the use of any medication must be declared before the fitness examination; otherwise, there is a risk of being judged unfit, which would jeopardise recruitment.

This approach significantly reduces the possibility of resorting to covert pharmacological cognitive enhancement, at least in the Armed Forces, as the substances administered would likely be detected by the diagnostic tests required for recruitment purposes in that sector. This is unless it is declared in advance that such substances.

It is likely that, if the use of pharmacological cognitive enhancement were to become widespread, legal disputes in this area would increase in direct proportion.

Short concluding remarks

As you have seen, the new frontiers of labour law also touch the topics of the labour market, although in different ways. Human enhancement can have some

²⁴ Art. 580, paragraph 1, Presidential Decree No. 90 of 15 March 2010 (Consolidated text of regulatory provisions on military organisation, pursuant to Art. 14 of Law No. 246 of 28 November 2005).

²⁵ Council of State, Section IV, 6 May 2010, No. 264.

consequences for the labour market, both from the perspective of disability and work performance. Regarding disability, work empowerment could lead to a shift in the perception of disability and a new understanding of the worker's abilities. This new understanding could influence workers' recruitment in the sense that, in the future, disabled workers could probably become regular workers. The use of exoskeletons and soft robots to support workers in the workplace will alter workers' duties and performance and have consequences for productivity that employers cannot ignore. Moreover, I must remind you once again that some of those devices realise a human enhancement that Artificial Intelligence could supervise.

As far as AI is concerned, two issues are crucial.

First, there is a question that legal practitioners, judges and scholars are increasingly asking. How can the protection of rights be guaranteed in the face of decisions based on assessments derived from the use of algorithms?

Judges are beginning to answer this question, and it is striking that the Court of Justice has shown its scepticism in this regard, although not in the field of labour law. The case *Ligue des droits humains v. Conseil des ministres*, dated 21 June 2022, is significant. The case concerns the 2016 PNR Directive on passenger name records written on airline tickets. This code pertains to information related to each passenger's journey, including data necessary for the processing and control of bookings by the airlines and booking agents concerned for each flight booked by or on behalf of any person.

Judges in Luxembourg have been very clear on the use of algorithms and artificial intelligence. In fact, according to the Court, about the criteria that the 'passenger information unit' (PIU) – i.e. the authority designated by the competent directive on the prevention, detection, investigation and prosecution of terrorist offences and serious crimes that each Member State is required to designate – may use, those criteria must be pre-established. And that requirement precludes the use of artificial intelligence technologies in machine learning systems, which are capable of modifying, without human intervention or control, the evaluation process and, in particular, the evaluation criteria on which the result of the application of that process is based, as well as the weighting of those criteria (paragraph 194). Furthermore, the Court of Justice does not believe in the reliability of artificial intelligence technologies because of their opacity, which could make it impossible to verify passenger data, with a consequent risk of infringement of fundamental rights, starting with Article 47 of the Charter of Fundamental Rights of the European Union, according to which "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal". The challenge of artificial intelligence is shifting increasingly towards the pursuit of transparency in decision-making, which is one of the key issues regarding AI and, not surprisingly, lies at the very core of the 2024 AI Act.

This is significantly linked to the second key issue, namely the role of information and consultation, and ultimately, that of social partners. Article 26, paragraph 7 of the AI Act declares that 'Before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system'. This provision aims to combat algorithmic opacity, although it is insufficient, as it is limited to high-risk AI systems and does not specify the information content that must be disclosed.

It is worth concluding this paper with a few questions on social partners. Can the European Union foster the role of social partners in a different way? Or must the social partners play their role within AI systems independently of EU legislation? Without intervening in that field through amendments to the AI Act or through collective agreements, preferably at the EU level, we can apply Shakespeare's motto, 'Much Ado about Nothing'.

Zoznam použitej literatúry

1. ABDOLI, Mohammad E. – AGNEW, Michael J. – STEVENSON, Joan M.: An on-body personal lift augmentation device (PLAD) reduces EMG amplitude of erector spinae during lifting tasks. In: *Clinical Biomechanics*, Vol. 21, 5 (2006), p. 456-465.
2. AIDA, Takamitsu – NOZAKI, Hirokazu – OBAYASHI, Hiroshi: Development of a muscle suit and application to factory labourers. In: *Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation*, IEEE, 9–12 August 2009, Changchun, China. p. 1027–1032
3. BERTOLINI, Andrea: Governare il potenziamento umano attraverso i principi di dignità e uguaglianza. In: *Politica del diritto*, Vol. LIII, 3 (2022), p.435–462.
4. BLOOMFIELD, Brian – DALE, Kate: Fit for work? Redefining 'Normal' and 'Extreme' through human enhancement technologies. In: *Organisation*, Vol. 22, 4(2015), p. 552-5.
5. BRINO, Vania: Wearable devices, in S. BORELLI et al., *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Giappichelli, Turin, 2022. p. 223.
6. CASILLO, Rosa: *Diritto al lavoro e dignità*, Editoriale scientifica, Napoli, 2020.
7. DE LOOZE, Michiel P. – BOSH, T. – KRAUSE, F. – STADLER, K. S. – O'SULLIVAN, L. W.: Exoskeletons for industrial application and their potential effects on physical workload. In: *Ergonomics*, Vol.59, 5 (2016), p. 671-681.
8. EU-OSHA – European Agency for Safety and Health at Work: *Work-related musculoskeletal disorders: Prevalence, costs and demographics in the EU*. European Risk Observatory, Bilbao, 2019.
9. FIATA, Emanuela: *Robotica e Lavoro*. In: M. Biasi (a cura di), *Diritto del lavoro e*

intelligenza artificiale, Milan, 2024, p. 611.

10. GREELY, Henry T.: *Remarks on Human Biological Enhancement*. In: 56 *Kansas Law Review*, 2008, p. 1139-1140
11. INOSE, Hiroki – MOHRI, S. – ARAKAWA H. – OKUI, M. – KOIDE, K. –YAMADA, Y. –KIKUTANI, I. – NAKAMURA, T.: Semi-endoskeleton-type waist assist AB wear suit equipped with compressive force reduction mechanism. In: *Proceedings 2017 IEEE International Conference on Robotics and Automation (ICRA) Singapore*, 29 May–3 June 2017, p. 6014–6019.
12. INRS: *Acquisition et integration d'un exosquelette en entreprise: Guide pour les préventeurs*, Institut National de Recherche et de Sécurité, Paris, 2019, disponibile su: www.inrs.fr
13. MARASSI, Stefania: *Intelligenza artificiale e sicurezza sul lavoro*. In: M. Biasi (a cura di), *Diritto del lavoro e intelligenza artificiale*, Milan, 2024, p. 207.
14. MAIO, Valerio: *Il lavoro e le nuove sfide della rivoluzione robotica*. In: *ADL*, 2018, 1415 ss.
15. MAIO, Valerio: *Diritto del Lavoro e potenziamento*. In: *ADL*, 2018, p.531-533.
16. PERUZZI, Marco: *Intelligenza artificiale e lavoro. Uno studio sui poteri datoriali e sulle tecniche di tutela*, Turin, 2023.
17. PIZZETTI, Federico G.: *Potenziamento umano e principio lavorista. Spunti di riflessione*. In: *Rivista di filosofia del diritto*, Vol. VII, 2 (2018), p. 261 – 272.
18. ZAPPALÀ, Loredana: *Intelligenza artificiale (voce)*. In: S. BORELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie*, Giappichelli, Turin, 2022, p. 133

Kontaktné údaje

Massimiliano Delfino, Full Professor of Labour Law
delfino@unina.it
University of Naples Federico II, Naples, Italy

THE RIGHT TO REASONABLE ACCOMMODATION IN DIGITAL ENVIRONMENT

Silvia Capíková¹

Abstract: Under EU rules, any employee with a disability has the right to reasonable accommodation. This right extends to all work-related activities covered by EU law, from the job application process to the termination of their employment contract. It also extends to working conditions and fringe benefits. Digitalization is changing the nature of the work environment, bringing new opportunities but also risks for people with disabilities or health disadvantages. The right to reasonable accommodation, enshrined in international and national anti-discrimination standards, is being extended in the digital context to new forms of support that go beyond physical workplace adaptations and also include so-called digital workplaces. Persons with disability constitute very heterogeneous population, thus, various disabilities may require different approaches and solutions. Qualitative legal research methodology, combining doctrinal analysis with comparative and contextual interpretation was used. The analysis focuses on identifying legal gaps, conceptual developments, and practical implications for employers and legislators in the digital work environment. We suggest e.g. expanding the personal and material scope of reasonable accommodation in Slovak national legislation in accordance with EU regulatory trends and recent case law.

Key words: labour law, digital transformation, nudging, disability, health impairment, Slovakia

Introduction

Digital technologies can be a useful tool that facilitates work activities and increases employee productivity and satisfaction, but their use can also have a negative effect on the mental and physical health of employees, reducing work efficiency and productivity. The nature and manner of using a particular digital tool can have a significant impact on employees' rights and their work obligations. The need for legal regulation can be identified in relation to the impacts on employees' physical or mental health, protection of privacy and integrity of the individual, cognitive safety, work-life balance and protection against discrimination. It is clear that the law cannot

¹ Comenius University in Bratislava, Faculty of Law, Department of Labour Law and Social Security Law

exhaustively regulate workplace digital practices. From the perspective of labour law, it is therefore important to reflect on the scenarios in which and how labour law should enter into the regulation of social processes related to the digitalization of the work environment.

The Court of Justice of the European Union and several national jurisdictions have developed case law confirming that failure to provide reasonable adjustments can amount to indirect discrimination, especially under EU law. These cases show a clear trend in European jurisprudence: reasonable adjustments are not optional when they are necessary to prevent disproportionate disadvantage, and failure to provide them may be legally challenged as indirect discrimination. There exists also opinions in the recent literature, based on the UN Convention of the Rights of Persons with Disabilities, that the failure of the employer to provide reasonable accommodations should be recognized as the *sui generis* form of discrimination.

The aim of the paper is to analyse how the right to reasonable accommodation of employees with disabilities is transforming in the context of the digitalisation of the work environment, and to identify legal challenges and opportunities for its implementation. We will address the questions of which forms of digital accommodation are legally relevant, and what challenges digitalisation poses for employers in ensuring equal treatment.

This paper adopts a qualitative legal research methodology, combining doctrinal analysis with comparative and contextual interpretation. Primary sources include EU legislation, international treaties such as the UN Convention on the Rights of Persons with Disabilities, and Slovak national law. Secondary sources include academic literature, policy documents, and empirical studies on digital transformation and workplace inclusion. The analysis focuses on identifying legal gaps, conceptual developments, and practical implications for employers and legislators in the digital work environment.

Digital work environment – the concept and challenge for regulation

Digital work environment can be considered as a specific concept that does not yet have a universal definition in the professional literature. We can operationalize it as a concept that refers to both working conditions, tools and social interactions that are mediated by digital technologies. It is not just about working "on a computer", but a complex ecosystem in which work is performed, coordinated, evaluated and communicated through digital means.

In the professional literature, we can find various terms that try to capture the qualitative change that digital technologies have brought to the world of work.

As pointed out by Mičić et al., "There have been a significant number of publications about digital workplace transformation. This is due to technological developments in

the last decades as well as the COVID-19 pandemic. However, there is no adequate overall definition of the term. This leads to misunderstandings and confused interpretation of the digital workplace, sometimes even narrowing it down to a set of tools or a platform. Given the complexity of digital workplace transformation, there is a need to have an integrated prospective and analyze it not just from a technological perspective, but from an organizational and processes point of view as well."²

Some authors emphasize the aspect of digital communication in the performance of work activities, while the physical space in which the employee is located is somewhat in the background.

If we prioritize digital communication with other people as the main feature of the work environment, we could understand the digital work environment in accordance with Bordi et al. as a "digital communication environment in which employees operate", while communication can be synchronous or asynchronous in terms of time, according to the aforementioned authors, and "refers to information-related actions involving either one-to-one or one-to-many communication."³ According to the research of the above authors, work efficiency, the quality of the working environment and the wellbeing of employees are closely related to the so-called information ergonomics, "which aims at increasing wellbeing and productivity through reducing information- and technology-related loads and increasing the suitability of technology for workers and work tasks."⁴ Also Mičić et al. highlighted, that modern workplace requires not only technological but also organizational and process adaptation to achieve full functional and operational transformation from a traditional into a digital workplace. "Social and technological changes have affected the ways of communication, cooperation and collaboration,"⁵ pointing to the need "to develop a separate, unique framework for digital workplace implementation for each of the industries in order to explain the transformation process from its own specific viewpoint."⁶

Most discussions about digitalization focus on office or "white-collar" environments. Use of digital technologies is somehow taken for granted in academia, research, teaching and "knowledge work." In reality, however, digitalization is also significantly

² MIČIĆ, Ljubiša, et al.: Defining the digital workplace: A systematic literature review. In: Strategic Management, vol. 27, no. 2, (2022), pp. 29-43. <https://doi.org/10.5937/StraMan2200010M>. p.29.

³ BORDI, Laura, et al. Communication in the Digital Work Environment: Implications for Wellbeing at Work. In: Nordic Journal of Working Life Studies, vol. 8, no. S3, (Apr. 2018), pp.29 - 48. <https://doi:10.18291/njwls.v8iS3.105275>. p. 29 – 30.

⁴ BORDI, Laura, et al., p.30

⁵ MIČIĆ, Ljubiša, et al., p.29.

⁶ MIČIĆ, Ljubiša, et al., p.42.

affecting “blue-collar” sectors – manufacturing, construction, logistics, healthcare, and agriculture.

Threats and opportunities for white-collar jobs

Digital transformation affected first the corporate management, where it can be defined as "the integration of digital technology into all aspects and operations of an organization, which in turn leads to infrastructural changes in how the organization is operated and delivers value to its customers".⁷

Digital tools especially during COVID-19 pandemic have afforded unprecedented opportunities for teammates to communicate, interact, collaborate, and exchange information in various formats across multiple communities regardless of their location or schedule, and social features that allow for greater geographic flexibility and remote work arrangements.⁸

Some researchers argue, that digital transformation fundamentally alters business operations, products, and processes, and in certain cases, gives rise to entirely new business models.⁹ Indeed, e-commerce allows self-employment (e.g. OnlyFans or Etsy) and boom in creative industry and personalized services, Massive Open Online Courses (MOOC) and asynchronous or synchronous online teaching, etc. It also enabled platform-mediated work, which is disrupting the concept of dependent work, jeopardizing employment status and standards of social protection and dignity of platform workers.¹⁰

The rise of artificial intelligence (AI) and automation is fundamentally changing the nature of work in so-called white-collar professions. While it was previously assumed that manual professions would be most threatened by technological advances, current analyses show that cognitive and administrative activities are equally, if not more, vulnerable to automation. Generative AI can effectively perform tasks such as text creation, data analysis, legal research or decision support – activities that were

⁷ KRAUS, Sascha et al.: Digital transformation in business and management research: An overview of the current status quo. In: International Journal of Information Management, vol. 63, (2022), n. pag. <https://doi.org/10.1016/j.ijinfomgt.2021.102466>

⁸ LANE, Jacqueline. N. et al.: Teams in the Digital Workplace: Technology’s Role for Communication, Collaboration, and Performance. In: Small Group Research, 55, No.1, (2023), pp. 139-183. <https://doi.org/10.1177/10464964231200015>, p.140.

⁹ BOUNCKEN, Riccarda. B., et al.: Knowledge- and innovation-based business models for future growth: digitalized business models and portfolio considerations. In: Review of Managerial Science, 15, 1,(2021), pp. 1-14, <https://doi.org/10.1007/s11846-019-00366-z>

¹⁰ HERMANTO, Hermanto - HENDRIKS, Pieter - Vermeer, Sophie: The Disruption of Labor Law in the Platform Economy: Towards a Normative Reconfiguration. In: Rechtsnormen Journal of Law, Vol. 3, No. 2 (2025), pp.190–198. <https://doi.org/10.70177/rjl.v3i2.2216>

until recently the prerogative of highly qualified professionals.¹¹ This development poses several threats: the risk of job losses, pressure for continuous learning, psychological impacts such as anxiety or loss of professional identity, and increasing competition between generations of workers. At the same time, however, opportunities are emerging – new professions focused on AI ethics, human-technology collaboration, data visualization or personalized services. Educational initiatives, such as Deloitte's Digital DNA program, support the development of skills that are difficult to automate, such as empathy, critical thinking or cross-disciplinary collaboration. Also, mastering AI agents and prompt-engineering for various AI solutions (text transcription, video creation and editing, etc.) are of high demand most recently.

Digital Technologies Supporting Manual Work: Tools for Inclusion and Efficiency

While digital transformation is often associated with office-based professions, recent technological developments have significantly impacted manual and physical work environments as well. A growing number of digital tools are being designed to support workers in manufacturing, construction, logistics, and other blue-collar sectors, with a particular emphasis on safety, efficiency, and accessibility.

One of the most prominent categories includes wearables and assistive technologies. Smart glasses such as Vuzix¹² or RealWear¹³ enable workers to access real-time instructions, video tutorials, and communicate hands-free with supervisors, which is particularly useful in complex or hazardous environments.¹⁴

The integration of Internet of Things (IoT) technologies has also transformed manual workspaces. "Private and public organisations increasingly deploy connected devices such as sensors, that continuously collect and communicate data. These devices, also called Internet of things (IoT), often involve algorithmic systems and complex AI technology. They can contribute to automating arduous tasks, optimise the use of space, monitor employees' pace of work, or even reduce the risks of work-related accidents and diseases. Environmental sensors monitoring air quality, temperature,

¹¹ KELLY, Jack: AI and Automation: Threats and Opportunities for White-Collar Professionals. In: *Forbes*, 2 Mar. 2025. Accessed August 29, 2025. <https://www.forbes.com/sites/jackkelly/2025/03/02/ai-and-automation-threats-and-opportunities-for-white-collar-professionals/>

¹² VUZIX: Introducing Vuzix LX1 Smart Glasses. Accessed September 1, 2025. <https://www.vuzix.com/pages/smart-glasses>

¹³ REALWEAR: The most powerful Smart Glasses for Frontline workers. Accessed September 1, 2025. <https://www.realwear.com/>

¹⁴ JIANG, Luping - ZHANG, Jingdong _ WONG, Yik Dieuw: Digital Technology in Occupational Health of Manufacturing Industries: A Systematic Review. In: *Discover Applied Sciences*, vol. 6, Article No. 631 (2024). <https://doi.org/10.1007/s42452-024-06349-4>

and noise levels contribute to healthier working conditions."¹⁵ Motion sensors are increasingly used to track ergonomic patterns and alert workers to potentially harmful movements, contributing to injury prevention.¹⁶

In the construction sector, drones and 3D printing technologies are revolutionizing building processes. Autonomous aerial robots equipped with additive manufacturing capabilities can construct and repair structures in-flight, even in hard-to-reach or hazardous environments. These systems, inspired by natural builders like bees, operate collaboratively using real-time feedback and path-planning algorithms to ensure precision and adaptability during the build process.¹⁷

In agriculture, digital automation technologies are transforming both crop and livestock production. Automated machinery such as autonomous tractors, drones for targeted input application, and robotic harvesters are increasingly used to address labor shortages and improve resource efficiency. These systems rely on GPS, GNSS, and variable rate technologies (VRT) to optimize input distribution and reduce environmental impact. For example, autonomous crop robots have demonstrated economic feasibility in tasks like weeding and harvesting, particularly in high-income countries.¹⁸

Another important area is the use of mobile applications and digital checklists. In terms of work planning and reporting, digital attendance systems using mobile terminals or biometric identification simplify workforce management. Applications such as Shiftboard¹⁹ facilitate shift scheduling and task coordination, enhancing transparency and team communication.

¹⁵ EL BOUCHIKHI, Maéva - WEERTS, Sophie - CLAVIEN, Christine: Ethical Issues of IoT in Occupational Safety: A Scoping Review. In: *Frontiers in Public Health*, vol. 12, Article No. 1468646 (2024). <https://doi.org/10.3389/fpubh.2024.1468646>

¹⁶ AFODABI, Adedeji - ANTHONY, Yusuf - ABIOLA, Akanmu: Human-in-the-Loop: Digital Twin Framework for Ergonomics of Exoskeletons in Construction. In: *Journal of Information Technology in Construction*, Vol. 29, (2024, p. 1083-1102, <https://doi.org/10.36680/j.itcon.2024.048>

¹⁷ LI, Shuai - LAN, Tian - NGUYEN, Hung-xuan - TRAN, Phuong: Frontiers in Construction 3D Printing: Self-Monitoring, Multi-Robot, Drone-Assisted Processes. In: *Progress in Additive Manufacturing*, vol. 10, 2025, pp. 2001–2030. <https://link.springer.com/article/10.1007/s40964-024-00794-8>

¹⁸ FAO: The State of Digital Automation Technologies and Robotics in Agriculture. In: *The State of Food and Agriculture 2022*. Open Knowledge Repository. Accessed September 1, 2025. <https://openknowledge.fao.org/server/api/core/bitstreams/1c329966-521a-4277-83d7-07283273b64b/content/sofa-2022/digital-automation-technologies-robotics.html>

¹⁹ SHIFTBOARD. Employee Scheduling Software. Accessed September 1, 2025. <https://www.shiftboard.com/employee-scheduling-software/>

Tools and materials are increasingly tracked using RFID tags, QR codes, and automated inventory systems, streamlining logistics and reducing errors.²⁰

Finally, digital technologies can play a crucial role in ensuring accessibility for workers with disabilities. Voice-controlled tools, magnification and screen-reading software for technical documentation are becoming more common.

These innovations demonstrate that digital transformation is not limited to office settings. Thus, when properly implemented, digital tools can not just accommodate tasks to new technologies available, but also support reasonable accommodation in manual professions, contributing to safer, more inclusive, and more efficient workplaces.

For legal discussions on reasonable accommodation, it is important to reflect that digital transformation does not only mean technological change, but also a transformation of work identity. The right to reasonable accommodation should take into account not only physical limitations, but also new forms of work vulnerability that arise as a result of technological developments.

Beyond a Wheelchair: Expanding the Personal and Material Scope of Reasonable Accommodation

"In March 2021, the European Commission adopted the Disability Rights Strategy 2021-2030, the main objective of which is to improve the lives of people with disabilities. The strategy followed on from the European Disability Strategy 2010-2020. Both strategies sought to take into account the diversity of disabilities, taking various forms, including long-term physical, mental, intellectual and sensory impairments."²¹

The definition of disability in EU policy is based on the so-called „social model“ of disability, which is outlined in the UN Convention on the Rights of Persons with Disabilities. CRPD has been ratified by the EU and most of its Member States. According to the UN CRPD, persons with disabilities “include those who have a long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others”. Persons with disability constitute very heterogeneous population, thus, various disabilities may require different approaches and solutions to enable employment participation.

²⁰ AKBARI, Ali: The application of radio-frequency identification (RFID) technology in the petroleum engineering industry: Mixed review, In: Petroleum Research, Available online 16 May 2025, <https://doi.org/10.1016/j.ptlrs.2025.05.001>

²¹ NOVÁKOVÁ, Mária - PAVLÍKOVÁ, Barbara: Zdravotná starostlivosť a ďalšia starostlivosť o zdravotne postihnuté osoby. In: Hamulák, J. a kol.: Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia. Bratislava : Právnická fakulta UK, 2022. p.335.

Although the obligation to provide reasonable accommodation in EU countries is traditionally linked to employees with medically certified and undisputed disabilities, the evolving landscape of public health and medical capabilities calls for a broader interpretation of this right. Advances in medicine have transformed many previously debilitating conditions into manageable chronic illnesses. These conditions may not result in a formal loss of work capacity, but they often lead to fluctuating performance, fatigue, or the need for flexible work arrangements.

E.g., irritable bowel syndrome (IBS) is a common, functional gastrointestinal disorder. Anxiety about abdominal symptoms, such as diarrhea, as well as the severity of IBS, is related to the degree of interference with one's work, impact on the daily performance of workers with IBS and sick leaves.²² While coeliac disease affects 1% of the world population and a feature of the disease is that it presents differently for different people and for those with symptomatic coeliac disease, symptoms can return and remain for an extended period if an autoimmune reaction is triggered. Diet-management techniques are very important for those affected. Beyond these medical challenges, there is confusion in the UK law concerning the status of coeliac disease in employment contexts – the UK Department of Health and Social Care states that coeliac disease is not defined as a disability under the Equality Act of 2010 even though it acknowledges that it is 'a long-term condition'. This ambiguity is also present in UK employment tribunals which demonstrate inconsistent decision-making around its status in their judgments.²³

In developed countries, the number of people who are neurodivergent or have hearing or vision impairments is increasing. Leisure video gaming appears to be an important risk factor for permanent hearing loss and/or tinnitus, because it is common worldwide, and because individuals often play video games at high-intensity sound levels and for several hours at a time.²⁴ According to the latest research, despite advances in treatment, age-related macular degeneration increases dramatically and remains a major public health issue, and is the leading cause of severe vision loss in individuals older than 55 years in high-income countries.

²² SUGAYA, Nagisa: Work-related problems and the psychosocial characteristics of individuals with irritable bowel syndrome: an updated literature review. In: *BioPsychoSocial Med* 18, 12 (2024). <https://doi.org/10.1186/s13030-024-00309-5>, p.1.

²³ STEINHOFF, Anne et al.: The challenges of coeliac disease at work: A contestation of the politics of inclusion. *Sociology of Health & Illness*, Volume 47, Issue 1, Jan 2025, p.1-13. <https://doi.org/10.1111/1467-9566.13826>, p.3-4.

²⁴ DILLARD, Lauren K et al.: Risk of Sound-Induced Hearing Loss from Exposure to Video Gaming or Esports: A Systematic Scoping Review. In: *BMJ Public Health*, vol. 2 (2024), e000253. <https://doi.org/10.1136/bmjph-2023-000253>

It puts at risk the employees performing visually demanding tasks, such as reading, driving, and recognizing faces.²⁵

In this context, the legal framework should consider the needs of individuals with “health impairments” or “medical disadvantages” who do not meet the strict criteria for disability but still face barriers to full participation in the workplace. The distinction between “disability” and “health disadvantage” is increasingly blurred, especially in digital work environments where cognitive load, screen exposure, and asynchronous communication can exacerbate certain conditions.

Reasonable accommodation should therefore be understood not only as a response to physical or sensory limitations, but also as a proactive measure to ensure equity and inclusion for a wider spectrum of health-related vulnerabilities. This includes adjustments such as flexible scheduling, digital tool customization, ergonomic interfaces, and access to assistive technologies. Employers should be encouraged to adopt a preventive and inclusive approach, recognizing that digital work environments can both alleviate and intensify health-related challenges.

Such an expanded understanding aligns with the principles of the UN Convention on the Rights of Persons with Disabilities (CRPD), which recognizes that disability is an evolving, dynamic concept and that disability results from the interaction between persons with impairments in one hand and attitudinal and environmental barriers on the other, that hinders their full and effective participation in society on an equal basis with others.²⁶ Our suggestion also reflects the dynamic nature of work in the digital age, where the boundaries between ability and disadvantage are increasingly shaped by technological, organizational, and social factors.

Pursuant Article 2 of the UN CRPD, “Reasonable accommodation” means necessary and appropriate modification and adjustments not imposing a disproportionate or undue burden, where needed in a particular case, to ensure to persons with disabilities the enjoyment or exercise on an equal basis with others of all human rights and fundamental freedoms.

Although many of digital technologies, machines, software are expensive, increasing digital transformation and expansion of digital sector makes many of them financially available within few years.

The obligation to provide reasonable accommodation in the workplace is well established in European and international law, particularly through the EU Employment Equality Directive (2000/78/EC) and the UN Convention on the Rights of Persons with Disabilities (CRPD). However, the digital transformation of work

²⁵ GUYMER, Robyn H. - CAMPBELL, Thomas G.: Age-Related Macular Degeneration. In: The Lancet, vol. 401, no. 10386, 29 Apr.–5 May 2023, pp. 1459–1472. [https://doi.org/10.1016/S0140-6736\(22\)02609-5](https://doi.org/10.1016/S0140-6736(22)02609-5)

²⁶ UNITED NATIONS (UN): The Convention on the Rights of Persons with Disabilities. Accessed Jun 20, 2025, Available from: <https://www.un.org/disabilities/documents/convention/convoptprot-e.pdf>

introduces new legal and practical challenges for employers seeking to fulfil this obligation.

One of the key challenges is the identification of accommodation needs in digital contexts. Unlike physical workplaces, where barriers may be more visible and tangible, digital environments often involve invisible or cognitive barriers—such as information overload, inaccessible software interfaces, or lack of compatibility with assistive technologies. Employers may lack the expertise to recognize these barriers or to assess their impact on employees with disabilities or health impairments.

Another challenge lies in the dynamic nature of digital tools and platforms. Frequent updates, changes in user interfaces, and the introduction of new systems can disrupt previously established accommodations. Employers must ensure that digital tools remain accessible over time and that employees are adequately trained to use them. This requires ongoing monitoring and collaboration with IT departments, software providers, and accessibility experts.

The principle of “reasonable” accommodation also raises questions about proportionality and undue burden in digital settings. While some accommodations may be low-cost (e.g., enabling screen readers or adjusting font sizes), others—such as customizing enterprise software or integrating assistive technologies—may involve significant financial or technical investment. Employers must balance the duty to accommodate with operational feasibility, while avoiding discriminatory practices.

Furthermore, the shift toward remote and hybrid work complicates the implementation of accommodations. Employers must consider how to support employees working from home, including access to ergonomic equipment, secure and accessible software, and flexible scheduling. The decentralization of workspaces challenges traditional models of workplace responsibility and requires a rethinking of how accommodation is provided and monitored.

In summary, while digitalization offers new opportunities for inclusion, it also demands a more nuanced and proactive approach to reasonable accommodation. Employers must navigate legal ambiguity, technological complexity, and evolving health needs to ensure that all employees can participate fully and equitably in the digital workplace, especially in situation of the need to accommodate job tasks or job performance to an employee in need for digital accommodation.

Understanding Digital Barriers in the Context of Reasonable Accommodation and Anti-Discrimination Law

In the framework of EU anti-discrimination law and the duty to provide reasonable accommodation, digital barriers are understood as structural or systemic disadvantages that arise when digital systems are not designed with accessibility and

inclusion in mind. These barriers can prevent individuals—particularly those with disabilities—from fully participating in the workplace. Such as platforms that do not support screen readers or other assistive technologies, non-captioned video content excludes deaf or hard-of-hearing users from meetings, training, or communication. Complex navigation interfaces pose challenges for users with cognitive or motor impairments. Lack of keyboard navigation affects users who cannot operate a mouse. Mandatory use of apps or portals without alternatives limits access for those unable to use specific digital tools (e.g., for HR services or remote work). And, last but not the least, inflexible digital work arrangements.

To comply with legal obligations and foster inclusive workplaces, employers are expected to audit digital tools for accessibility and usability, provide alternatives or modifications, such as accessible formats or assistive technologies, train staff on inclusive digital practices and accessibility standards, consult employees about their digital needs and barriers they may face.

According to the research of the Bardi et al., work efficiency, the quality of the working environment and the wellbeing of employees in digital environment are closely related to the so-called information ergonomics, "which aims at increasing wellbeing and productivity through reducing information- and technology-related loads and increasing the suitability of technology for workers and work tasks."

The key components of the digital adaptation of the work environment can be defined as follows:

1/ Technological tools. This can include at least:

- Software (MS Teams, Zoom, Slack, ERP systems etc.),
- Assistive technologies (reading software, voice control, magnification tools, etc.).

2/ Working modes:

- Remote work,
- Hybrid work models.

3/ Communication channels for synchronous and asynchronous communication:

- Email, chat, video calls.
- Virtual meetings, digital project management.

4/ Digital culture:

- Standards of behavior in the online space, including the right to disconnect.
- Digital inclusion and accessibility.
- Providing job-specific training and not to rely that more digitally competent colleagues will assist with informal peer learning to their colleagues.

5/ Cybersecurity and data protection.

The lack of clear regulatory guidance on digital accommodation creates legal uncertainty. National labor laws and occupational health regulations often do not explicitly address digital accessibility or remote work adaptations. This gap may lead to inconsistent practices and hinder the enforcement of rights. Employers may

benefit from sector-specific guidelines or model policies that clarify their obligations in digital contexts.

As outlined in our subchapters about state-of-the-art in “white-collar” and “blue-collar” jobs, differences in management of companies perhaps are not so significant while work tasks and physical workplaces differ quite a lot. Mičić et al. suggest “to develop a separate, unique framework for digital workplace implementation for each of the industries.”²⁷

Reasonable Accommodation vs. Indirect Discrimination in EU Case Law

The case law of the Court of Justice of the EU establishes a consistent line of interpretation of the concept of disability and the scope of the obligation to provide reasonable accommodation under Directive 2000/78/EC. In the iconic joined cases HK Danmark (Ring and Skouboe Werge) (C-335/11 and C-337/11), the Court confirmed the autonomous concept of disability in the EU, precisely by reference to the CRPD, while emphasising that an employer may not adopt measures that effectively exclude workers with disabilities without an individual examination of reasonable accommodation. The Kaltoft judgment (C-354/13) also plays an important role in the whole line of case-law, in which the Court confirmed that obesity is not a protected ground in itself, but may constitute a disability if it leads to long-term functional limitations, thus triggering the application of the reasonable accommodation regime. In the field of attendance, the key case is Ruiz Conejero (C-270/16), where the Court held that automated absence policies may constitute indirect discrimination if they specifically disadvantage workers with disabilities and if the employer does not demonstrate that it has assessed the possibility of reasonable accommodation before applying the sanctions. The common core of this case law is the requirement of an individual assessment, the need for a connection between disability and long-term functional limitation, and the employer's obligation to realistically demonstrate that reasonable accommodation would constitute an unreasonable burden.

In its judgment in G.L. v. AB SpA (C-38/24), the Court of Justice of the EU developed the concept of ‘associative discrimination’ in the field of employment and confirmed that the protection provided by Directive 2000/78/EC also applies to workers who are not themselves disabled but who are carers of a person with a disability and who face less favourable treatment as a result of that relationship. The Court emphasised that neutral rules or practices which specifically disadvantage carers may constitute indirect discrimination under Article 2(2)(b) of the Directive unless they are

²⁷ MIČIĆ, Ljubiša, et al.: Defining the digital workplace: A systematic literature review. In: Strategic Management, vol. 27, no. 2, (2022), pp. 29-43. (Crossref), <https://doi.org/10.5937/StraMan2200010M>. p.42.

objectively justified by a legitimate aim and appropriate means of achieving it. As regards the obligation to make reasonable accommodation under Article 5, the Court confirmed that this obligation applies only to workers with disabilities and not directly to their carers; at the same time, the employer may not adopt measures which have a discriminatory effect on carers. The judgment stresses the need for a proportionate approach and states that flexible working arrangements may constitute an appropriate means of ensuring equal treatment, although not in the form of “reasonable accommodation” within the meaning of Article 5. The decision thus reinforces the importance of the UN Convention on the Rights of Persons with Disabilities in the interpretation of EU law, extends protection against discrimination to situations based on custody and confirms that Article 2 of Directive 2000/78/EC also covers cases in which seemingly neutral rules indirectly disadvantage carers.

In the EU legal framework, the obligation to provide “reasonable accommodation” to employees with disabilities is set out as a separate and individual obligation, which complements the traditional discrimination tests. According to Directive 2000/78/EC (Article 5), the employer must take “appropriate measures, where needed in a particular case ..., unless such measures would impose a disproportionate burden”. This is different from the indirect discrimination test, which focuses on the PCP (“provision, criterion or practice”) and requires a comparator, demonstration of a disproportionate impact and the possibility of objective justification.

T. Gyulavári²⁸ recently examined the issue rigorously and suggests to differentiate two judicial tests:

A. Independent Test (CRPD-conform)

CRPD conform interpretation is based on an ‘independent’ reasonable accommodation test. The two-step analysis for accommodation requires an answer to two questions: 1. Is the adjustment necessary to ensure equality? 2. Does the adjustment constitute a disproportionate burden? “If the following conditions of Article 5 are met, discrimination could be stated in EU law, irrespective of the conditions of direct and indirect discrimination: denial of appropriate measures by the employer, which are necessary to enable a person with a disability to have access to, participate in, or advance in employment. In addition, proving disproportionate burden on the employer is a potential justification.”²⁹

The CJEU applied for the first time the independent test of reasonable accommodation under Article 5 of the Directive in the HR Rail judgment (C-485/20). A worker, recruited by the company HR Rail SA, became permanently unfit, during his traineeship, to hold the post to which he had been assigned, due to the onset of a

²⁸ GYULAVÁRI, Tamás: Recent CJEU case law on ‘reasonable accommodation’ at work: towards the recognition of a new discrimination form. ERA Forum, Vol. 24, No. 3 (2023), pp.361–377.

²⁹ GYULAVÁRI, Tamás: Recent CJEU case law on ‘reasonable accommodation’ at work, p.364.

disability. He was then dismissed due to incapacity. The applicant contested that decision, arguing that he was discriminated against on the grounds of disability. In such a situation, was his employer obliged, pursuant to Directive 2000/78/EC and in order to avoid any discrimination on grounds of disability, to assign the applicant to another post for which he was competent, capable and available. This question will lead the Court to consider, in particular, the application of that directive to persons undergoing a traineeship as part of their recruitment and the scope of the concept of 'reasonable accommodation'. The employer offered a temporary transfer but subsequently terminated the employment relationship. In this case, the Court of Justice of the European Union (CJEU) established that trainees, just like workers, can be assigned to another position. The Court held that the obligation to make reasonable accommodation also includes a transfer to another suitable position, if possible, unless this would constitute a disproportionate burden. "The question was whether the EU law concept of 'reasonable accommodation' requires that a worker, incapable of performing the essential functions of the post, be assigned to another position for which he has the necessary competence, capability and availability. So, this was the very first case, where the national court directly targeted the interpretation of the reasonable accommodation duty, including the assessment of a reassignment measure in the light of the disproportionate burden defence."³⁰ However, "the Court did not declare that denial of reasonable accommodation is a form of discrimination, but the violation of equal treatment was indeed based on the sole ground of its denial."³¹

B. Exemption Test

"The second possible interpretation perceives reasonable accommodation as a (satellite) part of the direct and indirect discrimination EU tests, so it is simply an extra exemption clause (exculpatio), in addition to objective justification and occupational requirement defence. In this 'exemption test', first direct or indirect discrimination is scrutinized: whether unequal treatment is directly or indirectly based on disability."³²

The role of reasonable accommodation in the proportionality of direct discrimination was addressed in the Tartu Vangla case (C-795/19) and in the Commission judgment (C-824/19). In Tartu Vangla, Estonian law prohibited a hearing-impaired prison guard from performing his duties without an individual assessment. In the Commission judgment, Bulgarian legislation effectively excluded a blind person from performing his duties as a juror. The judgments stated that absolute legal barriers without the possibility of an individual assessment and reasonable accommodation are contrary

³⁰ GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work, p. 372.

³¹ GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work, p. 373.

³² GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work, p. 364.

to the principle of proportionality. The obligation to make reasonable accommodation must be taken into account when assessing a 'genuine occupational requirement'.

The issue of indirect discrimination on the grounds of disability was examined in the HK Danmark case (C-335/11). An employee with a long-term disability was dismissed for excessive absences. In the judgment, the court stated that indirect discrimination occurs if a neutral rule (e.g. an absence policy) causes a disadvantage to persons with disabilities, unless the employer provides reasonable accommodation to mitigate the impact (which may include, for example, working time adjustments).

The so-called „Bilka test“ (1986) has become the basis for assessing objective justification for indirect discriminatory measures in the EU. An employer (Bilka-Kaufhaus GmbH) excluded part-time workers from a pension scheme. The majority of these workers were women, which raised the question of whether this constituted indirect discrimination on grounds of sex. According to the court, indirect discrimination occurs if an apparently neutral measure (e.g. the conditions for participation in a pension scheme) places a particular group (in this case women) at a disadvantage, unless the employer can demonstrate that: 1. the measure pursues a legitimate business objective and 2. the means of achieving that objective are appropriate and necessary. As suggested by Lane and Ingleby, the judgement „established that an indirectly discriminatory measure is justified if it meets a real need and is appropriate and necessary for meeting that need. This equated justification with necessity.“³³

The definition of reasonable accommodation at work was introduced in EU law by Article 5 of the Employment Equality Directive (hereinafter referred as "Directive"): "employers shall take appropriate measures, where needed in a particular case, to enable a person with a disability to have access to, participate in, or advance in employment, or to undergo training, unless such measures would impose a disproportionate burden on the employer." Thus, as highlighted by T. Gyulavári, the Directive "does not define the denial of reasonable accommodation as a sui generis form of discrimination. It is, therefore, left to the CJEU to clarify, what EU provisions (test) shall be applied to this duty"³⁴ and „the Directive must be interpreted in the light of the EU Charter of Fundamental Rights (CFR) and the CRPD.“³⁵

The definition of 'reasonable accommodation' clarifies the substance and extent of the measures which the employer must take.

³³ LANE Jackie A. - INGLEBY Rachel: Indirect Discrimination, Justification and Proportionality: Are UK Claimants at a Disadvantage? In: Industrial Law Journal, Vol. 47, No.4 (2017), p.532.

³⁴ GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work, p.362.

³⁵ GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work, p. 363.

According to Article 2 of the CRPD 2 : „Discrimination on the basis of disability” means any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment or exercise, on an equal basis with others, of all human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. It includes all forms of discrimination, including denial of reasonable accommodation; “Reasonable accommodationV: means necessary and appropriate modification and adjustments not imposing a disproportionate or undue burden, where needed in a particular case, to ensure to persons with disabilities the enjoyment or exercise on an equal basis with others of all human rights and fundamental freedoms.”

Article 5 of the Employment Equality Directive states: „In order to guarantee compliance with the principle of equal treatment in relation to persons with disabilities, reasonable accommodation shall be provided. This means that employers shall take appropriate measures, where needed in a particular case, to enable a person with a disability to have access to, participate in, or advance in employment, or to undergo training, unless such measures would impose a disproportionate burden on the employer. This burden shall not be disproportionate when it is sufficiently remedied by measures existing within the framework of the disability policy of the Member State concerned.”

In accordance with Article 5, the concept of reasonable accommodations „involves three pillars: accommodation measures, reasonableness, and proportionate burden.”³⁶ Denial of reasonable accommodation is not discrimination when it would be a disproportionate burden on the employer. „To determine disproportionate burden, account should be taken in particular of the financial and other costs entailed, the scale and financial resources of the undertaking and the possibility of obtaining public funding or any other assistance.”³⁷

The CRPD assumes that there are certain barriers that prevent an individual suffering of disability from participating in society, including employment, and that they need to be overcome by certain adjustments (e.g. removal of physical barriers, communication, availability of technology, etc.). In comparison, the scope of the Employment Equality Directive is much more limited. According to Art. 1, this Directive aims to prohibit discrimination on the grounds of religion or belief, disability, age or sexual orientation solely as regards employment and occupation.

According to Gyulavári, both regimes applied in EU – CRPD and Employment Equality Directive recognize “undue burden” as the limit of reasonable accommodation. „The Employment Equality Directive and the CRPD brought about a legal revolution in reasonable accommodation regulation by inserting this duty into

³⁶ GYULAVÁRI, Tamás: Recent CJEU case law on ‘reasonable accommodation’ at work, p.367.

³⁷ GYULAVÁRI, Tamás: Recent CJEU case law on ‘reasonable accommodation’ at work, p.362.

antidiscrimination law. Since the Directive came first, EU law differs from the CRPD", states Gyulavári, however „The fundamental mismatch between EU law and the CRPD is that the Directive does not declare denial of reasonable accommodation as a separate form of discrimination, although this specific interpretation would have many advantages to promote practical implementation.”³⁸

The two-step analysis for accommodation involves first a necessity/equality test: assessing whether a specific measure is necessary to ensure equal access, participation or performance for a person with a disability. It is then necessary to carry out an undue/disproportionate burden test: considering factors such as financial costs, technical feasibility, operational and safety constraints, availability of public assistance and the impact on other employees.

The case law of the Court of Justice of the European Union confirms the importance of an individual assessment. In the *Ca Na Negreta* case (C-631/22), the CJEU held that national law which allows for the automatic dismissal of an employee upon the occurrence of permanent disability without prior examination of the possibility of reasonable accommodation is incompatible with Directive 2000/78/EC, unless the employer first demonstrates that the accommodation would constitute a disproportionate burden³⁹. This legal and factual distinction between the discrimination test and the obligation to accommodate is crucial for the analysis of digital work environments. It shows that the employer must systematically assess and document specific accommodation and cannot avoid the obligation simply by claiming that the tools are “universal”. Failure to comply with this obligation may lead to discrimination and a violation of the employee’s rights if the accommodation has not been properly examined, despite being technically and economically feasible.

In the context of digital tools, these tests are particularly useful: when assessing whether adaptation is necessary, it is possible to verify whether current tools are inaccessible (e.g. missing subtitles, incompatibility with screen readers) and whether alternatives exist (e.g. plugins, APIs, configurations). In terms of burden, it is necessary to evaluate licensing costs, vendor-lock-in (e.g. need for API integration), whether the product already complies with the principles of “accessibility by design”, as well as security or legal constraints (e.g. GDPR, cybersecurity, IT-policy). When making a decision, technical documentation, price quotes, IT and security team opinions, as well as information on possible external funding sources should be collected.

³⁸ GYULAVÁRI, Tamás: Recent CJEU case law on ‘reasonable accommodation’ at work, p. 375.

³⁹ Court of Justice of the European Union: Case C-631/22, *J.M.A.R. v Ca Na Negreta SA*, Judgment of 18 January 2024, ECLI:EU:C:2024:53.

Digital Accommodations and Work Processes

Recent body of research suggests, that digital solutions, especially assistive technologies for disabled people based on Open-Source Hardware and Software (such as: such as Arduino, Raspberry Pi, NVIDIA Jetson, OpenCV, YOLO, MobileNet, EEG and EMG signal conditioning devices, actuators, and sensors such as ultrasonic, LiDar, or flex) can contribute to the accessibility and affordability of assistive technologies that can benefit disabled people suffering of wide scale of disability or impairment (such as visual, mobility, upper body, prostheses, hearing & speaking). Open-source technologies have potential to catalyze the design and deployment of low-cost ATs, which could be sensor-based or computer vision-based that meet high-quality criteria standards.⁴⁰

“Accessibility by design” refers to an approach in which accessibility features are integrated into products, services and digital systems at the earliest stages of design and development, rather than being added as a technical add-on. This concept is based on the principle of universal design, which aims to ensure that digital tools, interfaces and technologies are usable by the widest possible range of users, including people with disabilities, without the need for individual or special adaptations. In practice, it mainly includes following the Web Content Accessibility Guidelines (WCAG) when designing digital interfaces, implementing features such as keyboard control, compatibility with screen readers, sufficient colour contrast, scalable text, subtitles and voice interfaces, as well as applying inclusive design practices that take into account the different visual, auditory, motor or cognitive needs of users.

The principle of accessibility is one of the central principles of the CRPD. Pursuant its Art.2 “universal design” means the design of products, environments, programmes and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. “Universal design” shall not exclude assistive devices for particular groups of persons with disabilities where this is needed. The principle of accessibility is gradually being strengthened in the European legal order by several legal instruments. The European Accessibility Act⁴¹ (Directive (EU) 2019/882), which applies from June 2025, imposes obligations to ensure the accessibility of a wide range of products and services — from e-commerce, websites and smartphones to banking services, terminals and booking systems — and explicitly requires the integration of accessibility into design and manufacturing

⁴⁰ ARIZA, Jnathan Álvarez - PEARCE, Joshua M.: Low-Cost Assistive Technologies for Disabled People Using Open-Source Hardware and Software: A Systematic Literature Review. In: IEEE Access, vol. 10, pp. 124894-124927, 2022, <https://doi.org/10.1109/ACCESS.2022.3221449>, p.124894.

⁴¹ Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (The European Accessibility Act, EAA).

processes. The new Artificial Intelligence Act⁴² (AI Act, Regulation 2024/1689) introduces obligations for high-risk AI systems to prevent discrimination, promote transparency and fairness, which also strengthens the principle of accessibility in algorithmic decision-making. Finally, although the GDPR⁴³ is not a specific accessibility law, its emphasis on the clarity of information and the requirement for “privacy by design” support the principles of accessibility by design in the area of user interfaces and communication with data subjects.

Recent efforts of EU experts are focusing specific disabilities, which appear to be on the rise. Boucher had reviewed assistive technologies specifically for the 3 groups of impairments: „The first, blindness and visual impairments, ranges from mild disorders to severely limited visual perception and blindness. The second, deafness and hearing impairments, also follows a scale from minor disorders and range limitations to more severe impairment and deafness. Autism spectrum disorders (ASD), the third, are lifelong developmental disabilities that vary from Asperger syndrome, where intelligence and verbal communication may be preserved while non-verbal communications skills such as eye contact and facial expression are affected, to more severe disorders combining difficulties in communication and learning with hypersensitivity.“⁴⁴ The study found that current and emerging ATs tend to target the automation of tasks as a substitute for human labour, rather than the augmentation of human labour by blending technology in a way that enhances human control and efficiency. Bouchard suggests, that „ existing ATs – numbering over 60 000 in Europe – are not always used to their full potential, and that consideration should be given to whether more can be done with these technologies, in particular with regard their integration into social services, health, education and employment. In this sense, the development and diffusion of ATs does not depend upon new high-tech solutions, but on social and political action towards inclusion through various means, including technology as well as education, equality, attitudinal change and other initiatives.“⁴⁵

⁴² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

⁴³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

⁴⁴ BOUCHER, Philip: Assistive technologies for people with disabilities. Brussels: European Union, 2018. ISBN 978-92-846-2352-5. <https://doi.org/10.2861/422217>, p.5.

⁴⁵ BOUCHER, Philip: Assistive technologies for people with disabilities. p.12.

This is in line with our suggestion to implement „nudging“ into national legislation, to achieve digital accommodation and make possible measures more apparent for employers and employees.

Suggestions for amendment of the legal framework in Slovakia

In Slovak law, the basic legal regulation for the area of equal treatment is the so-called anti-discrimination law, which is further supplemented in labor law by the Labor Code and the Employment Services Act⁴⁶. Equal treatment of employees without any restrictions or discrimination, i.e. regardless of gender, marital and family status, sexual orientation, race, skin color, language, age, adverse health condition or disability, genetic characteristics, faith, religion, political or other opinion, trade union activity, national or social origin, membership of a nationality or ethnic group, property, gender or other status, is enacted in article 1 of the basic principles of the Labour Code and beyond the Anti Discrimination Act, includes adverse health condition or disability, genetic characteristics and trade union activity into the protected grounds. Toman, Švec and Rak highlight, that "the catalog of discriminatory attributes is declaratory and open, since the phrase "different status" potentially includes any distinguishing feature."⁴⁷

In national legislation, "different treatment is permissible only if the conditions of:

- (i) legality (the law must allow the different treatment)
- (ii) legitimacy (the aim is legitimate - the different treatment is justified by the nature of the activities carried out in the employment or the circumstances in which these activities are carried out, and at the same time this reason constitutes a genuine and determining requirement for the employment) and
- (iii) proportionality (the extent of the different treatment is proportionate) are met."⁴⁸

Across different legal systems, specific professions are often governed by sectoral legislation regulating employee duties and the organization of work. However, the question remains open as to whether the regulation of dependent work should be unified under a general legislative framework, such as a Labour Code, or whether a more diffused model—based on amendments to profession-specific acts—should serve as the primary method for innovating labour law.

⁴⁶ Act No. 5/2003 collection of laws of the Slovak Republic "the Employment Services Act", as amended.

⁴⁷ TOMAN, Jozef - ŠVEC, Marek - RAK, Pavol: Pracovné právo v súvislostiach. Bratislava : Friedrich Ebert Stiftung, 2020, p.6.

⁴⁸ Ibidem.

Slovakia has transposed the Employment Equality Directive into its national legislation. Employers in Slovakia are legally obliged to provide reasonable accommodations, which could be expanded also to the need to include solutions in digital work environments (e.g., accessible software, screen readers). Flexible work arrangements shall be available upon agreement between employer and employee pursuant to the national Labour Code⁴⁹.

Failure to do so may be considered discrimination under Slovak anti-discrimination law. In Slovakia, it is possible to amend the Anti Discrimination Act⁵⁰ which is a cornerstone of anti-discrimination law, with articles or paragraphs which could provide “nudging” for employees beyond the recent vague formulations: “In order to apply the principle of equal treatment in relation to a person with a disability, employers shall take such measures as will enable such a person to have access to a particular employment, to perform a particular activity in employment, to functional or other promotion in employment or to access to vocational training; this shall not apply if the adoption of such measures would be disproportionately burdensome for the employer.”⁵¹ The adoption of a measure that the employer is obliged to adopt under special regulations shall not be considered unduly onerous.⁵² Also, the employer's refusal or omission to adopt measures pursuant to paragraph 1 shall also be considered a failure to comply with the principle of equal treatment on grounds of disability.⁵³ The only exemption is the difference in treatment that “is justified by the nature of the activities performed in employment or by the circumstances in which those activities are performed, if that reason constitutes a genuine and determining employment requirement, provided that the aim is legitimate and the requirement is proportionate.”⁵⁴

The author of this paper suggests this supplementary provision regarding technological tools in to the Act No. 365/2004 Coll.:

“§ 7a – Digital adaptation of the working environment

(1) In order to apply the principle of equal treatment in relation to persons with disabilities or health impairment caused by a chronic health condition, the employer shall ensure the accessibility of digital work tools, in particular software solutions and assistive technologies, which are necessary for the performance of work.

(2) Reasonable adaptation is considered to be in particular:

⁴⁹ Act No. 311/2001 collection of laws of the Slovak Republic “the Labour Code, as amended.

⁵⁰ Act No. 365/2004 collection of laws of the Slovak Republic on Equal Treatment in Certain Areas and on Protection against Discrimination and on Amendments to Certain Acts (Anti-Discrimination Act), as amended.

⁵¹ §7, para. 1 of the Act No. 365/2004 coll.

⁵² §7, para. 3 of the Act No. 365/2004 coll.

⁵³ §7, para. 4 of the Act No. 365/2004 coll.

⁵⁴ §8, para. 1 of the Act No. 365/2004 coll.

a) ensuring the compatibility of work software (e.g. communication, project, ERP systems) with reading software, voice control or magnification tools,
b) enabling individual interface settings (e.g. font size, contrast, navigation),
c) providing assistive technologies, if they are necessary for the performance of work tasks.

(3) The employer is obliged to consult the need for digital adaptation with the employee concerned and to take his or her suggestions into due consideration, if their implementation does not represent a disproportionate burden.

(4) Refusal or failure to provide digital adaptation pursuant to paragraph 2 shall be deemed to be a breach of the principle of equal treatment."

Within the framework of the national legislation of the Slovak Republic, many authors point out the different legal definitions of the term "person with a disability" which are used in various social situations and make the legal status of the person with disability confusing.⁵⁵ "The lack of uniformity in the legislative approach to different groups of people with disabilities is also related to the frequency and variety of purposes for assessing the health status of such a person."⁵⁶

The Labour Code considers a person with a disability to be an employee who, in addition to the recognition of disability, has submitted to the employer a decision on a disability pension issued by the Social Insurance Agency. According to Section 71 of Act No. 461/2003 Coll. on Social Insurance, as amended, paragraph 1 "The insured person is disabled if, due to a long-term adverse health condition, his ability to perform gainful activity decreases by more than 40% compared to a healthy physical person." "A long-term adverse health condition is a health condition that causes a decrease in the ability to perform gainful activity and which, according to medical knowledge, is expected to last for more than one year." Thus, the legal status of the "person with disability" should be reconsidered by the legislators in order to be congruent with UN CRPD definition and to offer more practical guide to employers.

Limitations of the study

This paper focuses primarily on the legal tests for reasonable accommodation in the context of digital work environments. It is no purpose to provide an exhaustive list of digital solutions as they are numerous and in continuous development, as

⁵⁵ BARINKOVÁ, Milena: Osoba so zdravotným postihnutím a úskalia jej zrozumiteľnosti v právnej terminológii. In: *Studia Iuridica Cassoviensia*, Vol. 6, No. 1 (2018), p.89-90.

⁵⁶ KRIPPEL, Mikuláš: Postavenie osôb so zdravotným postihnutím v systémoch sociálneho a zdravotného poistenia. In: Hamulák, J, a kol.: *Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia*. Bratislava : Právnická fakulta UK, 2022, p.167

pointed by experts such as F. Boucher⁵⁷ or Ariza and Pearce⁵⁸. Due to space constraints, it does not address other important regulatory frameworks that interact with digital technologies, such as General Data Protection Regulation (GDPR) and the proposed EU Artificial Intelligence Act. As highlighted by Daňko and Poruban, both GDPR and AI Act frameworks raise significant questions about data processing, algorithmic transparency, and risk management in digital workplaces⁵⁹. However, these topics and also other, such as cybersecurity compliance, fall outside the scope of this study, which is centered on equality and non-discrimination obligations. Future research could explore how privacy and AI governance intersect with accommodation duties, particularly in relation to accessibility-by-design and algorithmic decision-making.

Conclusion

The digital transformation of the workplace presents both opportunities and challenges for the realization of the right to reasonable accommodation. While EU and international law clearly establish this right for persons with disabilities, the evolving nature of digital work environments requires a broader and more dynamic interpretation. Digital barriers—often invisible and systemic—can significantly hinder participation, especially for individuals with health impairments who may not meet the strict legal definition of disability.

This paper has shown that reasonable accommodation must extend beyond physical adaptations to include digital tools, communication platforms, and organizational practices. The concept of digital accommodation encompasses not only assistive technologies and accessible software, but also flexible work arrangements, ergonomic interfaces, and inclusive digital cultures. The paper suggests that employers adopt pro-active measures such as accessibility audits and inclusive design standards (e.g., WCAG 2.1) when implementing digital tools, as part of their equality strategy. These measures are essential to ensure equity and prevent indirect discrimination in increasingly digitized workplaces.

Legal frameworks must evolve to reflect this reality. The proposed amendment to Slovak anti-discrimination law illustrates how national legislation can better support digital inclusion. Employers, legislators, and policymakers must recognize that

⁵⁷ BOUCHER, Philip: Assistive technologies for people with disabilities., p.12.

⁵⁸ ARIZA, Jnathan Álvarez - PEARCE, Joshua M.: Low-Cost Assistive Technologies for Disabled People Using Open-Source Hardware and Software: A Systematic Literature Review, p.124894.

⁵⁹ DAŇKO, Martin - PORUBAN, Andrej: Práva a povinnosti zamestnancov v Akte o umelej inteligencii. In Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024. Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie. Trenčín: Trenčianska univerzita Alexandra Dubčeka v Trenčíne, Fakulta sociálno-ekonomických vzťahov, 2024, s.10.

digital accessibility is not a technical detail but a fundamental aspect of equal treatment in employment.

Ultimately, the right to reasonable accommodation in the digital environment is not only a legal obligation—it is a commitment to dignity, participation, and fairness in the future of work.

Acknowledgements

The author is grateful to the anonymous reviewers for their insightful comments and constructive suggestions on the earlier draft of this paper. Their feedback significantly contributed to improving the clarity and depth of the analysis. The usual disclaimer applies: any remaining errors or omissions are solely the responsibility of the author.

Bibliography

Legislation and case law

1. Act No. 365/2004 collection of laws of the Slovak Republic (coll.) On Equal Treatment in Certain Areas and on Protection against Discrimination and on Amendments to Certain Acts (Anti-Discrimination Act), as amended.
2. Act No. 311/2001 collection of laws of the Slovak Republic “the Labour Code, as amended.
3. Act No. 461/2003 Coll. on Social Insurance, as amended.
4. Act No. 5/2003 collection of laws of the Slovak Republic “the Employment Services Act”, as amended.
5. Court of Justice of the European Union. (2013). HK Danmark, acting on behalf of Ring v Dansk almennyttigt Boligselskab and Skouboe Werge v Dansk Arbejdsgiverforening, Joined Cases C-335/11 & C-337/11, Judgment of the court (Second Chamber), 11 April 2013, ECLI:EU:C:2013:222.
6. Court of Justice of the European Union. Fag og Arbejde (FOA) v. Kommunernes Landsforening (KL), Case C-354/13, Judgment of the Court (Fourth Chamber), 18 December 2014, ECLI:EU:C:2014:2463.
7. Court of Justice of the European Union, Carlos Enrique Ruiz Conejero v. Ferroser Servicios Auxiliares SA, Case C-270/16, Judgment of the Court (Third Chamber) of 18 January 2018, ECLI:EU:C:2018:17.
8. .Court of Justice of the European Union. G.L. v AB SpA, Case C-38/24, Judgment of 11 Sept. 2025. ECLI:EU:C:2025:738.
9. Court of Justice of the European Union, Case C-631/22, J.M.A.R. v Ca Na Negreta SA, Judgment of 18 January 2024, ECLI:EU:C:2024:53.
10. Court of Justice of the European Union, Case C-485/20, HR Rail, Judgment of 10 February 2022, ECLI:EU:C:2022:85.

11. Court of Justice of the European Union, Case C-795/19, Tartu Vangla, Judgment of 15 July 2021, ECLI:EU:C:2021:606.
12. Court of Justice of the European Union, Case C-824/19, Komisia za zashtita ot diskriminatsia, Judgment of 21 October 2021, ECLI:EU:C:2021:862.
13. Court of Justice of the European Union, Case C-170/84, Bilka-Kaufhaus GmbH v Weber von Hartz, Judgment of 13 May 1986, ECLI:EU:C:1986:204.
14. Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation (EU Employment Equality Directive (2000/78/EC)).
15. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services
16. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).
18. UNITED NATIONS (UN): The Convention on the Rights of Persons with Disabilities (CRPD). Accessed Jun 20, 2025, Available from: <<https://www.un.org/disabilities/documents/convention/convoptprot-e.pdf>>

Academic literature and policy documents

1. AFODABI, Adedeji - ANTHONY, Yusuf - ABIOLA, Akanmu: Human-in-the-Loop: Digital Twin Framework for Ergonomics of Exoskeletons in Construction. In: Journal of Information Technology in Construction, Vol. 29, (2024), p. 1083-1102, <https://doi.org/10.36680/j.itcon.2024.048>
2. AKBARI, Ali: The application of radio-frequency identification (RFID) technology in the petroleum engineering industry: Mixed review, In: Petroleum Research, Available online 16 May 2025, <https://doi.org/10.1016/j.ptlrs.2025.05.001>
3. ARIZA, Jnathan Álvarez - PEARCE, Joshua M.: Low-Cost Assistive Technologies for Disabled People Using Open-Source Hardware and Software: A Systematic Literature Review. In: IEEE Access, vol. 10, pp. 124894-124927, 2022, <https://doi.org/10.1109/ACCESS.2022.3221449>
4. BARINKOVÁ, Milena: Osoba so zdravotným postihnutím a úskalia jej zrozumiteľnosti v právnej terminológii. In: Studia Iuridica Cassoviensia, Vol. 6, No. 1 (2018), p. 89-98.

5. BORDI, Laura, et al. Communication in the Digital Work Environment: Implications for Wellbeing at Work. In: Nordic Journal of Working Life Studies, vol. 8, no. S3, (Apr. 2018), pp.29 - 48. <https://doi:10.18291/njwls.v8iS3.105275>. p. 29 – 30.
6. BOUCHER, Philip: Assistive technologies for people with disabilities. Brussels: European Union, 2018. 20p. ISBN 978-92-846-2352-5. <https://doi.org/10.2861/422217>
7. BOUNCKEN, Riccarda. B., et al.: Knowledge- and innovation-based business models for future growth: digitalized business models and portfolio considerations. In: Review of Managerial Science, 15, 1,(2021), pp. 1-14, <https://doi.org/10.1007/s11846-019-00366-z>
8. DAŇKO, Martin - PORUBAN, Andrej: Práva a povinnosti zamestnancov v Akte o umelej inteligencii. In *Aktuálne výzvy v rozvoji ľudských zdrojov: dôsledky krízového obdobia 2024. Zborník vedeckých príspevkov z medzinárodnej vedeckej konferencie*. Trenčín: Trenčianska univerzita Alexandra Dubčeka v Trenčíne, Fakulta sociálno-ekonomických vzťahov, 2024, s.10 - 19. ISBN 978-80-8295-044-4.
9. DILLARD, Lauren K et al.: Risk of Sound-Induced Hearing Loss from Exposure to Video Gaming or Esports: A Systematic Scoping Review. In: BMJ Public Health, vol. 2 (2024), e000253. <https://doi.org/10.1136/bmjph-2023-000253>
10. EL BOUCHIKHI, Maéva - WEERTS, Sophie - CLAVIEN, Christine: Ethical Issues of IoT in Occupational Safety: A Scoping Review. In: Frontiers in Public Health, vol. 12, Article No. 1468646 (2024). <https://doi.org/10.3389/fpubh.2024.1468646>
11. FAO: The State of Digital Automation Technologies and Robotics in Agriculture. In: The State of Food and Agriculture 2022. Open Knowledge Repository. Accessed September 1, 2025. <<https://openknowledge.fao.org/server/api/core/bitstreams/1c329966-521a-4277-83d7-07283273b64b/content/sofa-2022/digital-automation-technologies-robotics.html>>
12. GUYMER, Robyn H. - CAMPBELL, Thomas G.: Age-Related Macular Degeneration. In: The Lancet, vol. 401, no. 10386, 29 Apr.–5 May 2023, pp. 1459–1472.
13. GYULAVÁRI, Tamás: Recent CJEU case law on 'reasonable accommodation' at work: towards the recognition of a new discrimination form. ERA Forum, Vol. 24, No. 3 (2023), pp.361–377.
14. HERMANTO, Hermanto - HENDRIKS, Pieter - VERMEER, Sophie: The Disruption of Labor Law in the Platform Economy: Towards a Normative Reconfiguration. In: Rechtsnormen Journal of Law, Vol. 3, No. 2 (2025), pp.190–198. <https://doi.org/10.70177/rjl.v3i2.2216>

15. JIANG, Luping - ZHANG, Jingdong _ WONG, Yiik Diew: Digital Technology in Occupational Health of Manufacturing Industries: A Systematic Review. In: Discover Applied Sciences, vol. 6, Article No. 631 (2024). <https://doi.org/10.1007/s42452-024-06349-4>
16. KRAUS, Sascha et al.: Digital transformation in business and management research: An overview of the current status quo. In: International Journal of Information Management, vol. 63, (2022), n. pag. <https://doi.org/10.1016/j.ijinfomgt.2021.102466>
17. KRIPPEL, Mikuláš: Postavenie osôb so zdravotným postihnutím v systémoch sociálneho a zdravotného poistenia. In: Hamulák, J, a kol.: Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia. Bratislava : Právnická fakulta UK, 2022. p.166-196.ISBN 978-80-7160-659-8.
18. LANE, Jackie A. – INGLEBY, Rachel: Indirect Discrimination, Justification and Proportionality: Are UK Claimants at a Disadvantage? In: Industrial Law Journal, Vol. 47, No.4 (2017), 531-552.
19. LANE, Jacqueline. N. et al.: Teams in the Digital Workplace: Technology's Role for Communication, Collaboration, and Performance. In: Small Group Research, 55, No.1, (2023), pp. 139-183. <https://doi.org/10.1177/10464964231200015>, p.140.
20. LI, Shuai - LAN, Tian - NGUYEN, Hung-xuan - TRAN, Phuong: Frontiers in Construction 3D Printing: Self-Monitoring, Multi-Robot, Drone-Assisted Processes. In: Progress in Additive Manufacturing, vol. 10, 2025, pp. 2001–2030. Available from: <<https://link.springer.com/article/10.1007/s40964-024-00794-8>>
21. MARINACI, Tiziana et al.: An Inclusive Workplace Approach to Disability through Assistive Technologies: A Systematic Review and Thematic Analysis of the Literature. In: Societies, Vol. 13, no. 11 (2023): 231. <https://doi.org/10.3390/soc13110231>
22. MIČIĆ, Ljubiša, et al.: Defining the digital workplace: A systematic literature review. In: Strategic Management, vol. 27, no. 2, (2022), pp. 29-43. <https://doi.org/10.5937/StraMan2200010M>. p.29.
23. NOVÁKOVÁ, Mária - PAVLÍKOVÁ, Barbara: Zdravotná starostlivosť a ďalšia starostlivosť o zdravotne postihnuté osoby. In: Hamulák, J. a kol.: Sociálna ochrana osôb so zdravotným postihnutím v pracovnom práve a práve sociálneho zabezpečenia. Bratislava : Právnická fakulta UK, 2022. p.334 - 367.ISBN 978-80-7160-659-8
24. SUGAYA, Nagisa: Work-related problems and the psychosocial characteristics of individuals with irritable bowel syndrome: an updated literature review. In: BioPsychoSocial Med 18, 12 (2024). <https://doi.org/10.1186/s13030-024-00309-5>

25. STEINHOFF, Anne et al.: The challenges of coeliac disease at work: A contestation of the politics of inclusion. *Sociology of Health & Illness*, Volume 47, Issue 1, Jan 2025, p.1-13. <https://doi.org/10.1111/1467-9566.13826>
26. TOMAN, Jozef - ŠVEC, Marek - RAK, Pavol: *Pracovné právo v súvislostiach*. Bratislava : Friedrich Ebert Stiftung, 2020. 215 s. ISBN 978–80–89149–90–2.

Non-academic sources

1. KELLY, Jack: AI and Automation: Threats and Opportunities for White-Collar Professionals. In: *Forbes*, 2 Mar. 2025. Accessed August 29, 2025. Available from: <<https://www.forbes.com/sites/jackkelly/2025/03/02/ai-and-automation-threats-and-opportunities-for-white-collar-professionals>>
2. REALWEAR: The most powerful Smart Glasses for Frontline workers. Accessed September 1, 2025. Available from: <<https://www.realwear.com>>
3. SHIFTBOARD. Employee Scheduling Software. Accessed September 1, 2025. <https://www.shiftboard.com/employee-scheduling-software>
4. VUZIX: Introducing Vuzix LX1 Smart Glasses. Accessed September 1, 2025. Available from: <<https://www.vuzix.com/pages/smart-glasses>>

Contact details

Mgr. et Mgr. Silvia Capíková, PhD. et PhD.

silvia.capikova@flaw.uniba.sk

Comenius University in Bratislava, Faculty of Law, Department of Labour Law and Social Security Law

EROTIC LABOUR IN THE PLATFORM ECONOMY: CHALLENGES OF IMPLEMENTING THE EU DIRECTIVE ON IMPROVING WORKING CONDITIONS IN PLATFORM WORK IN SLOVAKIA¹

Juraj Plaza²

Abstract: This paper examines the challenges associated with applying Directive (EU) 2024/2831 on improving working conditions in platform work to the regulation of erotic services and persons working in this sector in Slovakia. The Directive introduces a presumption of employment for workers whose relationship with digital platforms demonstrates elements of management and control. While it is primarily aimed at protecting workers in the gig economy, such as drivers or couriers, an open question remains as to whether its scope may also extend to adult content creators, escort services, and sex workers who are economically dependent on platforms. The article focuses on the novelties that EU regulation brings into the Slovak legal order, options for transposition, the (in)adequacies of the current Labour Code, the ambiguous legal status of sex work, and the broader social stigma surrounding erotic labour, especially in its digital form. It also points out that reclassifying erotic labour as employment could expose platforms to criminal liability.

Keywords: erotic labour, presumption of employment, digital labour platform

Introduction

The rise of the platform economy has transformed how labour is organised, shifting traditional employment relationships into new digital environments. While ride-hailing and food-delivery platforms have attracted the most attention in legal and policy debates, erotic labour mediated by platforms such as OnlyFans, Chaturbate, or LiveJasmin is a rapidly expanding sector that remains underexplored. These forms of work share core characteristics with other types of platform work — algorithmic management, economic dependency, and reliance on global intermediaries — yet are marked by heightened stigma and regulatory neglect. The adoption of Directive (EU) 2024/2831 on improving working conditions in platform work (Platform Work

¹This work was supported by the Scientific Grant Agency of the Ministry of Education, Research, Development and Youth of the Slovak Republic and the Slovak Academy of Sciences (VEGA), grant no. 1/0677/24 Women in crisis.

²Comenius University Bratislava, Faculty of Law, Department of Labour Law and Social Security Law

Directive, PWD) introduces a presumption of employment, rules on algorithmic management, and obligations extending to intermediaries. The Directive must be transposed into national law by December 2026, creating both an opportunity and a challenge for Member States. Slovakia provides a hard case for analysis. Prostitution exists in a legal grey zone: it is neither prohibited nor legalized. Erotic workers can operate only as self-employed persons (SZČO), often under substitute trade licences such as “massage services”. This paper sets out the conceptual framework, situating erotic labour within platform work and outlining both the PWD’s novelties and the Slovak legal context. It also reviews international scholarship on erotic labour in the platform economy as well as analyses the application of the PWD to erotic labour in Slovakia, highlighting tensions between EU obligations and national law.

Real people stories

The everyday realities of erotic labour on digital platforms reveal how deeply commercial and algorithmic structures shape intimate self-presentation. On the landing page of major webcamming sites such as Chaturbate, visitors encounter a mosaic of performers — students, freelancers, and self-described amateurs — whose profiles blur the boundaries between authenticity, marketing, and fantasy. For instance, one performer identifies herself as Abby, a French law student who “dreams big” and streams while studying; another, Brianna, claims to speak eleven languages, though her grammar errors suggest otherwise. Some of the creators strategically utilize³ surface acting, involving the falsification, suppression, or concealing of genuine emotions and also adopting a ‘separate identity’ to satisfy customers.

In similar field, newspapers were full of stories about certain OnlyFans creator claiming breaking the world record in the number of intercoursés with men in 12 hours. Other raising more than 1 million dollars revenue in 3 hours from her subscribers on the day of her 18 birthdays.

Research shows that men often entered sex work accidentally via dating or hookup apps (e.g., Grindr) after receiving offers for paid sex.⁴ One Slovak participant interviewed by the author, described being offered an apartment equipped for live streaming in the centre of Bratislava — illustrating how sexualised digital labour can merge with physical, organised infrastructure.

³ SCHUCHMANN, Swana. ‘I tell them the story that they want to hear that day’: emotion management, emotional labour, and authenticity as a digital sex worker – the case of OnlyFans. *Porn Studies*. 2025. DOI: 10.1080/23268743.2025.2501322, p. 9

⁴ WEBBER, Val et al. Digitally Facilitated Sex Work: A Scoping Review Articulating Men’s Labor Experiences. *The Journal of Sex Research*. 2025. DOI: 10.1080/00224499.2025.2478576, p. 4

Conceptual Framework

Erotic labour has long been marginalised in legal and policy debates, framed either as a matter of morality or criminality rather than as labour. Yet contemporary scholarship demonstrates that erotic work organised through platforms displays the same core features as other types of platform work: **algorithmic management, economic dependency, and infrastructural intermediation**.

Some refer to such labor as “playbour”—a blend of pleasure and work, where creators monetize activities tied to self-expression and intimacy.⁵

OnlyFans creators are compelled into *cross-platform self-branding* due to the lack of internal search functions, creating dependency on Instagram or TikTok for visibility. Camming platforms strictly regulate acceptable content, penalising infractions through shadowbanning or suspension.⁶ Stigma compounds this precarity: erotic labour is simultaneously erased as “not sex” and “not work,” leaving workers marginalised in both policy and public discourse.⁷

Swords, Laing and Cook conceptualise the “platform stack” as a layered architecture through which digital labour is organised, governed, and monetised. The stack consists of three interdependent layers:

1. the network layer, where users interact and value is created through visibility and engagement;
2. the infrastructure layer, encompassing algorithms, moderation systems, and terms of service that regulate acceptable behaviour; and
3. the data layer, where information about workers and consumers is stored, analysed, and monetised.⁸

Each layer embeds a distinct form of control — social, technical, and informational — which collectively constructs the conditions of platform labour. For erotic workers, this architecture translates into algorithmic visibility hierarchies, unilateral enforcement of content policies, and pervasive data surveillance. Rather than neutral intermediaries, platforms emerge as multi-level governance systems that discipline and commodify digital intimacy.

Erotic labour might often seem as not informal freelancing but **structured, controlled, and economically dependent work** mediated by digital platforms.

⁵ HAMILTON, Vaughn et al. “Nudes? Shouldn’t I charge for these?” : *Motivations of New Sexual Content Creators on OnlyFans*. arXiv, 2022. DOI: 10.48550/arXiv.2205.10425, p. 12

⁶ STEGEMAN, Hanne Marleen. Regulating and representing camming: Strict limits on acceptable content on webcam sex platforms. *New Media & Society*. 2024, vol. 26, no. 1. DOI: 10.1177/14614448211059117, p. 335

⁷ EASTERBROOK-SMITH, Gwyn. OnlyFans as gig-economy work: a nexus of precarity and stigma. *Porn Studies*. 2023, vol. 10, no. 3. DOI: 10.1080/23268743.2022.2096682, p. 5

⁸ SWORDS, Jon, Mary LAING and Ian R COOK. Platforms, sex work and their interconnectedness. *Sexualities*. 2023, vol. 26, no. 3. DOI: 10.1177/13634607211023013, p. 280

Platforms have created “planetary sex markets”—proprietary, platform-based labour markets that transcend national borders while remaining governed by private platform infrastructures. These markets enable workers and clients to connect globally but simultaneously impose new constraints through algorithmic control, fees, and regulation.⁹

The EU Platform Work Directive and Slovak law

Directive (EU) 2024/2831 introduces several innovations that directly affect platform workers: **presumption of employment, regulation of algorithmic management, data protection safeguards, extension to intermediaries**. Taken together, these provisions might expand the concept of labour protection in the platform economy. For the provisions to apply, service must fall under the definition of digital labour platform, meaning fulfill 4 criteria listed in art. 2(1)(a):

- I. service is provided at least in part, at a distance by electronic means, such as by means of a website or a mobile application;
- II. service is provided at the request of a recipient of the service;
- III. it involves, as a necessary and essential component, the organisation of work performed by individuals in return for payment, irrespective of whether that work is performed online or in a certain location;
- IV. it involves the use of automated monitoring systems or automated decision-making systems.

Slovak law, however, presents unique challenges. Prostitution is excluded from the Labour Code’s concept of dependent work, meaning that sex workers cannot be employees. As Nevická observes, this places prostitution in a **legal grey zone**: it is not prohibited, but neither is it recognised as labour.¹⁰ Sex workers must instead operate as self-employed persons (SZČO), often registering under substitute licences such as “massage services.” A recent amendment added *operation of an erotic salon* to the list of free trades (licence), but this regulates establishments rather than the work of individual sex workers.¹¹

At the same time, a reform of the Labour Code removed the criterion that dependent work must be performed “at the time determined by the employer.” This change has the potential to broaden the scope of dependent work, making it easier to recognise

⁹ WARIN, Robbie, Chloe K. GOTT and Mark GRAHAM. Planetary sex markets: camming, OnlyFans and the globalization of sex work. *Porn Studies*. 2025. DOI: 10.1080/23268743.2025.2512825, p. 3

¹⁰ NEVICKÁ, Denisa. *Hranica medzi prostitúciou a masážou, alebo ako je upravené poskytovanie erotických služieb na Slovensku?* [online]. Brno: MUNI Press, 2019 [Accessed 26 September 2025]. Available at: <http://dnyprava.law.muni.cz/dokumenty/53457>

¹¹ Available at: https://www.minv.sk/swift_data/source/verejna_sprava/zivnostenske_podnikanie_ozp2/Zoznam%62oodporucanych%20oznaceni%20volnych%20zivnosti.pdf [Accessed 26 September 2025].

forms of labour where subordination derives from algorithmic or economic control rather than rigid scheduling. This reform aligns with the PWD's emphasis on indicators of control rather than contractual form.

Finally, Slovak criminal law complicates matters. The offence of pimping (*kupliarstvo*) criminalises benefiting from another person's prostitution, raising the possibility that platforms recognised as "employers" could simultaneously be criminalised. This tension exemplifies the challenges of transposing the PWD into a legal system that continues to treat prostitution (though criminalising pimping) primarily as a criminal matter rather than as labour.

Erotic Labour on Platforms

International scholarship on platform-mediated sex work provides essential insights into how erotic labour is organised, governed, and experienced. Several recurring themes emerge: economic dependency and visibility labour, employment misclassification, financial governance and exclusion, stigma and discursive erasure. Di Cicco and Beraldo demonstrate that OnlyFans creators must engage in continuous cross-platform self-branding to remain visible, since the platform lacks an internal search function.¹² This dependence forces workers to invest time and resources into unpaid visibility labour, amplifying precarity. Jokubauskaite et al. add quantitative evidence from camming platforms: visibility and earnings are strongly correlated with hours of availability, producing "winner-take-all" dynamics where a small share of performers capture most of the income.¹³ Nocella's analysis of porn content creators in the UK situates them within the intermediate *limb (b)* worker status, which grants some but not all employment protections.¹⁴ This highlights the inadequacy of binary classifications of employee versus self-employed — a problem mirrored in Slovakia, where workers lack any intermediate category.

Franco shows how payment processors such as Visa and Mastercard shape the governance of adult platforms, imposing biometric ID verification, moderation rules, and high fees.¹⁵ These intermediaries exercise de facto regulatory authority, often

¹² DI CICCIO, Margherita and Davide BERALDO. Sex work as cross-platform self-branding. Challenges and strategies of OnlyFans' content creators in a precarious ecosystem. *Platforms & Society*. 2025, vol. 2. DOI: 10.1177/29768624251359797, p. 2

¹³ JOKUBAUSKAITE, Emilija, Bernhard RIEDER and Sarah BURKHARDT. Winner-Take-All? Visibility, Availability, and Heterogeneity on Webcam Sex Platforms. *Social Media + Society*. 2023, vol. 9, no. 4. DOI: 10.1177/20563051231214807, p. 7

¹⁴ NOCELLA, Rebecca Rose. Employment Status on a Spectrum: Porn Content Creators as Limb (b) Workers? *Industrial Law Journal*. p. 24

¹⁵ FRANCO, Rébecca S. "Controlling the keys to the Golden City": The payment ecosystem and the regulation of adult webcamming and subscription-based fan platforms. *New Media & Society*. 2024. DOI: 10.1177/14614448241303465, p. 10

without transparency or accountability. Stegeman documents how camming platforms frame performances as “not sex” and “not work,” enabling them to distance themselves from legal obligations while disciplining performers.¹⁶ Easterbrook-Smith extends this insight, showing that stigma renders OnlyFans workers precarious even compared to other gig workers, since sex work is excluded from mainstream labour rights discourses.¹⁷

Platform Control in Practice: The Case of OnlyFans Terms of Service

The contractual framework of several platforms illustrates the extent of control exercised over workers. Under the OnlyFans' ToS, creators retain 80% of revenue, while the platform automatically deducts 20% from all transactions.¹⁸ Furthermore, breaches of ToS may lead to suspension, account termination, or loss of earnings. The rules are drafted unilaterally by the platform, and enforcement is opaque. All creators must submit government-issued ID and undergo biometric verification before they can earn revenue. Payments are processed through a narrow set of intermediaries, meaning that creators' financial access is entirely mediated by global payment processors.

Beyond the public Terms of Service, the pre-written “Contract between Fan and Creator” on OnlyFans, concluded every time a fan asks for private content, is designed to present the platform as a neutral intermediary, stating explicitly that “the only parties to this Agreement are the Fan and Creator” and that the company “is not a party” except in limited respects. At first glance, this shifts liability and responsibility away from the platform. However, the substantive provisions reveal that OnlyFans retains decisive control. The company reserves the right to collect all payments, deduct its 20% fee, remove content at any time, and enforce compliance with its Terms of Service. The agreement prohibits Fans and Creators from contracting on alternative terms, since it “applies to the exclusion of any other terms.” Creators are obliged to deliver paid content once payment is received, while Fans assume the risk of access interruptions. Dispute resolution is centralised under English law, limiting Creators' ability to rely on local legal protections.

Taken together, these provisions illustrate a paradox: while the platform formally denies being a party to the contract, it retains unilateral control over financial flows, content availability, and the conditions of interaction.¹⁹ The ToS reserve the right for

¹⁶ STEGEMAN, Hanne Marleen. *Regulating and representing camming*. p. 338

¹⁷ EASTERBROOK-SMITH, Gwyn. *OnlyFans as gig-economy work*. p. 8

¹⁸ OnlyFans, Terms of Service [online]. Available at: <https://onlyfans.com/terms> [Accessed 26 September 2025].

¹⁹ OnlyFans, Contract between Fan and Creator [online]. Available at: <https://onlyfans.com/contract> [Accessed 26 September 2025].

OnlyFans to amend terms, commission rates, or rules of acceptable content at any time. Creators must accept these changes to continue working, leaving them in a position of dependency without genuine bargaining power. The question arises whether such indicators of control should ever trigger the presumption of employment under Article 5 of the PWD.

Application of the PWD to Erotic Labour in Slovakia

The Platform Work Directive sets out a broad regulatory framework designed to address misclassification, algorithmic management, and financial dependency in the platform economy. Applying these provisions to erotic labour in Slovakia reveals significant challenges.

Article 5 of the PWD establishes a presumption of employment where indicators of control are present. This is intended to prevent platforms from evading obligations through false self-employment. Even after the 2025 amendment to the Slovak labour code (effective from January 2026) removed the criterion that dependent work must be performed “at the time determined by the employer,” effects of such change remain questionable. Especially in terms of erotic labour where the definition is still too rigid. Articles 7 and following of the PWD introduce obligations for transparency in algorithmic decision-making, particularly regarding ranking, deactivation, and monitoring. Erotic platform workers are highly affected by algorithmic management. These mechanisms create significant asymmetries of power, yet Slovak labour inspectorates currently lack the expertise and resources to monitor such systems. Without institutional capacity, the Directive’s algorithmic safeguards risk remaining unenforced.

The PWD prohibits the processing of sensitive personal data, including biometric data, for the purpose of managing workers. Article 3 extends Directive obligations to intermediaries who organise or control platform labour. This provision is directly relevant to erotic labour, where payment processors and hosting providers exercise regulatory authority. However, Slovak criminal law poses a significant barrier. The offence of pimping (*kupliarstvo*) criminalises benefiting from another’s prostitution, which risks encompassing platforms themselves. Slovakia must transpose the PWD by December 2026. Erotic labour is not a discussed point in the debates on transposition.

Core Chokepoints for Transposition

The application of the Platform Work Directive to erotic labour in Slovakia is not merely a technical question of legislative drafting. It exposes deeper structural barriers within the Slovak legal order. Three chokepoints stand out. The Directive assumes that individuals engaged in platform-mediated tasks fall within the legal

concept of “work.” Slovak law does not share this assumption. Sex workers must rely on substitute trade licences such as “massage services.” The recent introduction of a free trade licence for the *operation of an erotic salon* regulates establishments but does not cover individual workers. Unless erotic labour is recognised as legitimate work (falling under the definition of dependent work), the presumption of employment under Article 5 of the PWD will remain inapplicable. The Directive presupposes the existence of national authorities capable of monitoring algorithmic management and enforcing transparency obligations. Slovak inspectorates, however, lack both the technical expertise and the resources to audit ranking systems, moderation rules, or data-driven performance monitoring. Without significant investment in regulatory capacity, the provisions on algorithmic management and data protection risk being transposed in form but not in substance. Finally, Slovak criminal law criminalises profiting from another person’s prostitution under the offence of pimping (*kupliarstvo*). If platforms are reclassified as “employers” under the Directive, they may simultaneously fall under this offence. This deters platforms from operating openly in Slovakia and also creates uncertainty for workers, who could be left without a lawful channel for asserting their rights. These chokepoints are not isolated. Recognition without enforcement capacity leaves rights symbolic; enforcement capacity without recognition leaves workers invisible; and both are undermined if criminal law continues to frame platforms as illicit actors. Addressing these barriers requires coordinated reform across labour, trade, and criminal law.

Conclusion

Erotic labour in the platform economy is a litmus test for the effectiveness of the EU PWD. Platforms such as OnlyFans and camming sites exhibit all the characteristics the Directive seeks to regulate: algorithmic management, economic dependency, and financial intermediation. Yet in Slovakia, the transposition of the Directive faces three structural chokepoints: the exclusion of prostitution from the definition of dependent work, the absence of regulatory capacity to monitor algorithmic control, and contradictions with criminal law.

These barriers illustrate the danger of a merely symbolic transposition. If erotic labour is left outside the scope of the Directive, the group of workers most exposed to precarity and stigma will remain unprotected, undermining the Directive’s very purpose. Conversely, addressing these obstacles would not only extend protections to erotic workers but also strengthen the Slovak state’s ability to regulate platform work more broadly.

Bibliography

1. DI CICCIO, Margherita and Davide BERALDO. Sex work as cross-platform self-branding. Challenges and strategies of OnlyFans' content creators in a precarious ecosystem. *Platforms & Society*. 2025, vol. 2, p. 29768624251359797. ISSN 2976-8624, 2976-8624. DOI: 10.1177/29768624251359797
2. EASTERBROOK-SMITH, Gwyn. OnlyFans as gig-economy work: a nexus of precarity and stigma. *Porn Studies*. 2023, vol. 10, no. 3, pp. 252–267. ISSN 2326-8743, 2326-8751. DOI: 10.1080/23268743.2022.2096682
3. FRANCO, Rébecca S. "Controlling the keys to the Golden City": The payment ecosystem and the regulation of adult webcamming and subscription-based fan platforms. *New Media & Society*. 2024, p. 14614448241303465. ISSN 1461-4448, 1461-7315. DOI: 10.1177/14614448241303465
4. HAMILTON, Vaughn et al. "Nudes? Shouldn't I charge for these?": Motivations of New Sexual Content Creators on OnlyFans. arXiv, 2022. DOI: 10.48550/arXiv.2205.10425
5. JOKUBAUSKAITĖ, Emilija, Bernhard RIEDER and Sarah BURKHARDT. Winner-Take-All? Visibility, Availability, and Heterogeneity on Webcam Sex Platforms. *Social Media + Society*. 2023, vol. 9, no. 4, p. 20563051231214807. ISSN 2056-3051, 2056-3051. DOI: 10.1177/20563051231214807
6. NEVICKÁ, Denisa. *Hranica medzi prostitúciou a masážou, alebo ako je upravené poskytovanie erotických služieb na Slovensku?* [online]. Brno: MUNI Press, 2019 [accessed 09.10.2025]. ISBN 978-80-210-9702-5. Available at: <http://dnyprava.law.muni.cz/dokumenty/53457>
7. NOCELLA, Rebecca Rose. Employment Status on a Spectrum: Porn Content Creators as Limb (b) Workers? *Industrial Law Journal*
8. SCHUCHMANN, Swana. 'I tell them the story that they want to hear that day': emotion management, emotional labour, and authenticity as a digital sex worker – the case of OnlyFans. *Porn Studies*. 2025, pp. 1–17. ISSN 2326-8743, 2326-8751. DOI: 10.1080/23268743.2025.2501322
9. STEGEMAN, Hanne Marleen. Regulating and representing camming: Strict limits on acceptable content on webcam sex platforms. *New Media & Society*. 2024, vol. 26, no. 1, pp. 329–345. ISSN 1461-4448, 1461-7315. DOI: 10.1177/14614448211059117
10. SWORDS, Jon, Mary LAING and Ian R COOK. Platforms, sex work and their interconnectedness. *Sexualities*. 2023, vol. 26, no. 3, pp. 277–297. ISSN 1363-4607, 1461-7382. DOI: 10.1177/13634607211023013
11. WARIN, Robbie, Chloe K. GOTT and Mark GRAHAM. Planetary sex markets: camming, OnlyFans and the globalization of sex work. *Porn Studies*. 2025, pp. 1–20. ISSN 2326-8743, 2326-8751. DOI: 10.1080/23268743.2025.2512825

12. WEBBER, Val et al. Digitally Facilitated Sex Work: A Scoping Review Articulating Men's Labor Experiences. *The Journal of Sex Research*. 2025, pp. 1–13. ISSN 0022-4499, 1559-8519. DOI: 10.1080/00224499.2025.2478576

Contact details

Mgr. Juraj Plaza

juraj.plaza@flaw.uniba.sk

Department of Labour Law and Social Security Law, Faculty of Law, Comenius University Bratislava

**Sekcia rímskeho práva, kánonického,
cirkevného práva a právnych dejín a právnej
komparatistiky**
Přemeny prameňov práva

VPLYV ÚSTAVNÝCH ZMIEN NA HIERARCHIU PRÁVNÝCH NORIEM (1939 – 1992)

THE IMPACT OF THE CONSTITUTIONAL CHANGES ON THE HIERARCHY OF LEGAL SOURCES (1939 – 1992)

Terézia Švedová¹

Abstrakt: Vývoj slovenského ústavného poriadku v priebehu 20. storočia odráža meniace sa predstavy o právnej autorite a primárnej úlohe rôznych zdrojov práva. Autoritárska ústava Slovenského štátu z roku 1939 centralizovala moc, zlúčila legislatívne a výkonné funkcie a zakotvila nacionalistické a zahraničné (nemecké) prvky. Po roku 1948, v období komunistického režimu, ústavný poriadok zakorenil socialistické právne stereotypy a drasticky obmedzil rozhodovacie procesy v štáte – i napriek existencii parlamentu, ktorý bol oficiálne jediným nositeľom zákonodarnej moci, skutočné centrum sa presunulo do stranických štruktúr Komunistickej strany Československa. Ústavný zákon o federácii, síce v roku 1968 priniesol federatívny model fungovania parlamentu, význam federácie a jeho praktický prínos zostal podriadený obmedzeniam vyplývajúcim z charakteru vtedajšieho režimu. Po Nežnej revolúcii, Ústava Slovenskej republiky z roku 1992 obnovila demokratický ústavný systém, čerpajúc z medzivojnovnej tradície aj zo západných modelov, čím preformovala hierarchiu právnych predpisov smerom k silnejšej ústavnej nadradenosti a delbe moci. Táto trajektória odráža, ako ústavné transformácie predefinovali úlohu a autoritu zákonov a nadnárodných noriem v slovenskom práve.

Kľúčové slová: ústavný poriadok, hierarchia noriem, Slovenský štát, komunistický režim, demokratizačný proces

Abstract: The development of the Slovak constitutional order during the 20th century reflects the changing ideas on legal authority and the primary role of various sources of law. The authoritarian Constitution of the Slovak State of 1939 centralized power, merged legislative and executive functions, and enshrined nationalist and foreign (German) elements. After 1948, during the communist regime, the constitutional order entrenched socialist legal

¹ Katedra právnych dejín a právnej komparatistiky, Právnická fakulta, Univerzita Komenského v Bratislave.

stereotypes and drastically limited decision-making processes in the state - despite the existence of a parliament, which was officially the sole possessor of the legislative power, the real centre shifted to the party structures of the Communist Party of Czechoslovakia. Although the Constitutional Act on Federation in 1968 introduced a federative model into the parliamentary operation, the significance of the federation and its practical benefits remained subject to the limitations stemming from the nature of the regime at that time. After the Velvet Revolution, the 1992 Constitution of the Slovak Republic restored a democratic constitutional system, drawing on both the interwar tradition and Western models, reshaping the hierarchy of legal regulations towards stronger constitutional supremacy and separation of powers. This trajectory reflects how constitutional transformations redefined the role and authority of laws and supranational norms in Slovak law.

Key words: constitutional order, hierarchy of norms, Slovak State, communist regime, democratization process

Úvod

Dňa 26. septembra 2025 Národná rada Slovenskej republiky ako ústavodarný orgán² schválila vládny návrh ústavného zákona, ktorým sa podstatne mení doterajšie znenie čl. 7 ústavného zákona č. 460/1992 Zb. o Ústave Slovenskej republiky (ďalej len „Ústava SR“).³ Čl. 7 Ústavy SR sa dotýka aj problematiky hierarchie právnych noriem, a to najmä vzhľadom na ods. 2 a 5, ktoré vyjadrujú princíp prednosti noriem medzinárodného práva, resp. práva Európskej únie. V zmysle citovanej novely však veci tzv. národnej identity majú byť po novom výlučne predmetom regulácie vnútroštátneho práva. Čo presne možno subsumovať pod pojem národnej identity však momentálne nie je možné jednoznačne determinovať, keďže samotné

² V zmysle ustanovenia čl. 72 v spojení s ustanoveniami čl. 84 ods. 4, 86 písm. a) ústavného zákona č. 460/1992 Z. z. Ústava Slovenskej republiky.

³ Do čl. 7 sa má s účinnosťou od 1. novembra 2025 doplniť odsek 6 a 7 v znení:

„(6) Slovenská republika si zachováva zvrchovanosť predovšetkým vo veciach národnej identity tvorenej najmä základnými kultúrno-etickými otázkami, ktoré sa týkajú ochrany života a ľudskej dôstojnosti, súkromného a rodinného života, manželstva, rodičovstva a rodiny, verejnej morálky, osobného stavu, kultúry a jazyka, ako aj rozhodovania o veciach s tým súvisiacich v oblasti zdravotníctva, vedy, výchovy, vzdelávania, osobného stavu a dedenia.

(7) Nič v tejto ústave a ústavných zákonoch nemožno vykladať ako súhlas Slovenskej republiky s prenosom výkonu časti jej práv vo veciach tvoriacich národnú identitu.“ Zdroj: Schválené znenie ústavného zákona z 26. septembra 2025, ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov [online]. In *Národná rada Slovenskej republiky*. Dostupné dňa [27-09-2025]. Dostupné na: <nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=573829>

ustanovenie hovorí o obsahu tohto pojmu len príkladmo,⁴ z dôvodovej správy k predkladanému návrhu však vyplýva, že primárnym cieľom novely mala byť ochrana tradičných hodnôt v záujme zachovania kultúrneho dedičstva.⁵ Napriek tejto jazykovej vágnosti a interpretačnej nejednoznačnosti je však zrejmé, že sa týmto pretvára doteraz platný systém vnútorného usporiadania právnych noriem v Slovenskej republike.

Je nutné konštatovať, že časté⁶ zmeny vo vnútornom usporiadaní právnych noriem nie sú v našom právnom prostredí cudzím prvkom. Po tom, čo bolo územie Slovenska po tisícročie spravované normami historickej uhorskej ústavy,⁷ možno označiť náš ústavnoprávny vývoj v 20. storočí za turbulentný, vyznačujúci sa častými zmenami základnej normy, pričom tieto zmeny boli vždy úzko prepojené so zmenami v rovine politickej. Od roku 1939 po prijatie Ústavy SR v roku 1992 bola hierarchia noriem v tomto kontexte predmetom častých zásahov. Kľúčovou otázkou, ktorá je predmetom nasledujúcich strán teda je, akým spôsobom sa menil systém, resp. hierarchia právnych noriem na území Slovenska vzhľadom na zásadné zmeny v ústavnom systéme v období rokov 1939 – 1992? V rámci hľadania odpovede na túto základnú otázku skúmame najmä to, ako je upravený vertikálny systém právnych noriem v danom období, kto sa podieľal na tvorbe týchto právnych noriem a ako je riešený konflikt medzi právnymi normami.

K hierarchii právnych noriem vo všeobecnosti

Právny poriadok štátu možno charakterizovať ako komplexný, vnútorne usporiadaný systém, v ktorom sa prepájajú právne normy vydané rôznymi subjektmi od medzinárodných inštitúcií cez národné parlamenty až po samosprávne orgány, s rôznorodým obsahom a zameraním. Imperatív usporiadanosti, ktorý vo svojom diele zdôrazňoval aj Hans Kelsen,⁸ reflektuje jednotu právnych noriem v ich mnohosti, zreteľne artikuluje, ktoré právne normy sú platné, kedy a prečo, čím sa

⁴ Najmä kultúrno-etické otázky, pokiaľ ide o ochranu života a ľudskej dôstojnosti, súkromný a rodinný život, manželstvo, rodičovstvo a rodinu, kultúru a jazyk, ako aj o veci s tým súvisiace, a to najmä v oblasti zdravotníctva, výchovy a vzdelávania.

⁵ Pozri bližšie: Dôvodová správa k návrhu ústavného zákona č. 733, ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov [online]. In *Národná rada Slovenskej republiky*. Dostupné dňa [27-09-2025]. Dostupné na: <nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=560649>

⁶ K tomuto bližšie v predposlednej kapitole venovanej vývoju po roku 1989.

⁷ LYSÝ, Miroslav. *Slovenské právne dejiny I. Vývoj ústavného a správneho práva na Slovensku od najstarších čias po súčasnosť*. Šamorín: Heuréka, 2021. 191 s. ISBN 978-80-8173-114-3. S. 59 – 70.

⁸ KELSEN, Hans. *Čistá právna veda*. Krásno nad Kysucou: Kalligram, 2018. 190 s. ISBN 978-80-89916-21-4. S. 95 – 96.

posilňuje právna istota v adresátoch týchto noriem.⁹ Za epicentrum tejto jednoty možno označiť ústrednú, základnú normu, z ktorej možno odvodiť platnosť právnych predpisov nižšej právnej sily, čím sa vytvára jasná vertikálna hierarchia právnych predpisov. Platnosť základnej normy pritom vyplýva z historického vývoja základných noriem platných v určitom systéme práva.¹⁰ Kelsenova teória „čistého práva“, resp. práva očisteného od externých faktorov však najmä s ohľadom na vývoj právneho poriadku na Slovensku v 20. storočí nemôže obstať. Právny poriadok ako celok a osobitne tak jeho právne normy, jednotlivé platné základné normy nevynímajúc, boli objektom záujmu politickej moci a v celom sledovanom období nesporne reflektovali politickú vôľu i ideológiu. Problematike vnútornej závislosti práva od externých faktorov, najmä politických, ideologických, sociologických, či ekonomických sa venovali teoretici kritických právnych štúdií.¹¹ Kritické právne štúdie odmietajú objektivitu a neutralitu právneho poriadku a jeho noriem. Hierarchia právnych noriem má v podstate len zastierať východiskové mocenské vzťahy v pozadí, pričom aj samotná tvorba, interpretácia a aplikácia práva príslušnými orgánmi je predmetom vnútorného uváženia, a teda môže reflektovať ideológiu.¹²

V právnom systéme je základným kameňom, základnou normou, či ohniskom právneho poriadku ústava, ktorá zaujíma ústredné miesto pri určovaní hierarchie noriem a definuje rámec, v ktorom sa zákony tvoria, interpretujú a presadzujú.

⁹ Porovnaj: MERLI, Franz. Principle of Legality and the Hierarchy of Norms. In SCHROEDER, Werner (ed.): *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation*. London: Bloomsbury, 2016. S. 43 – 44. ISBN 9781849469500.

¹⁰ Tamže, s. 95 – 114. KELSEN, Hans. On the Basic Norm. In *California Law Review* (1959), 47(1), s. 107 – 110. Samozrejme, Kelsenova teória hierarchie právnych noriem bola podrobená kritike. Napríklad Herbert Lionel Adolphus Hart odmietol Kelsenovu teóriu základnej normy a vytvoril pravidlo uznania alebo sociálne pravidlo, na základe ktorého možno identifikovať platnú normu, čo je norma, ktorú authority uznávajú a používajú. Porovnaj: RAZ, Joseph. H. L. A. Hart (1907 – 1992). In *Utilitas* (1993), 5(2), s. 150 – 152. SHAPIRO, Scott J. What is the rule of recognition (and does it exist) [online]? In *Yale Law School, Public Law & Legal Theory Research Paper Series (Research Paper No. 181.)* S. 2 – 5. Dostupné dňa [23-09-2025]. Dostupné na: <<http://papers.ssrn.com/abstract#1304645>> Kritiku si Kelsenova teória vyslúžila napríklad aj od Johna Finnisa; v zmysle jeho prirodzenoprávnej teórie nie je hierarchia noriem odvádzaná od základnej normy, ale od normy, resp. normatívneho systému stojaceho nad národných právnym poriadkom (morálka). Pozri napríklad: FINNIS, John. *Natural Law and Natural Rights*. Oxford: Clarendon Press, 2011. 494 s. ISBN 978-0-19-959914-1.

¹¹ Z anglického originálu Critical Legal Studies. Jedná sa o interdisciplinárne hnutie, ktoré sa sformovalo na začiatku 80. rokov 20. storočia. Jeho hlavnou metódou je kriticky analyzovať právne normy, inštitúcie a ich vzťah k moci. Jedným z prvkov kritiky právneho systému, ktorý je predmetom záujmu kritických právnych štúdií je aj hierarchia. Zdroj: MORADI, Shuresh. A Critical Legal Study of the Declaration of the Rights of Man and of the Citizen. In *Beijing Law Review* (2019), 10, s. 1154 – 1156.

¹² Pozri bližšie: UNGER, Roberto Mangabeira. *The Critical Legal Studies Movement*. Cambridge: Harvard University Press, 1986. 128 s. ISBN 0-674-17735-3. KELMAN, Mark. *A guide to critical legal studies*. Cambridge: Harvard University Press, 1987. 360 s. ISBN 0-674-36756-1.

Poskytuje základné princípy, ktoré načrtávajú štruktúru vzťahu medzi štátom, jeho inštitúciami a jeho občanmi. Ústavné zmeny však môžu tento normatívny poriadok výrazne narušiť. Takéto narušenia sú obzvlášť hlboké v režimoch, kde je moc koncentrovaná v rukách jednotlivcov, resp. úzkej skupiny osôb a mechanizmy kontroly výkonu moci sú obmedzené alebo neexistujú vôbec. Zmena ústavy v týchto kontextoch často slúži hlboko politickým cieľom, pričom pretvára hierarchiu právnych noriem s cieľom legitimizovať autoritársku kontrolu. Autoritatívne a totalitné režimy sa svojou povahou snažia centralizovať moc a eliminovať právny pluralizmus. Ústavné zmeny v týchto systémoch často stierajú hranice medzi právom a ideológiou a podriaďujú právne normy vôli dominantnej strany alebo vodcu. Výsledkom je reštrukturalizovaná právna hierarchia, v ktorej ústava už nefunguje ako obmedzenie moci, ale ako jej nástroj a v ktorej sú vytvorené také mechanizmy, ktoré vládnucej elite umožňujú udržiavať si moc vo svojich rukách.¹³

Parlament ako prežitok

Slovenský štát, ktorý vznikol 14. marca 1939 na troskách destabilizovanej Československej republiky, možno charakterizovať ako autoritatívny štát. I keď sa v mnohých prvkoch inšpiroval talianskym fašizmom a nemožno mu uprieť ani blízkosť s nemeckým nacizmom, jeho ideologická náplň nebola naplno rozpracovaná a napokon ani ideologicky homogénna.¹⁴ Právny systém Slovenského štátu bol formálne postavený na základe ústavného zákona č. 185/1939 Sl. z. o Ústave Slovenskej republiky (ďalej len „Ústava 1939“), prijatej 21. júla 1939. Táto ústava predstavovala základný normatívny rámec pre výkon štátnej moci a tvorbu právnych

¹³ Porovnaj: LOEWENSTEIN, Karl. Law in the Third Reich. In *The Yale Law Journal* (1936), 45(5), S. 802. ARENDT, Hannah. *The Origins of Totalitarianism*. New York: Harcourt Brace, 1976. S. 364- 419, 460 – 479. ISBN 0-15-670153-7.

¹⁴ Typicky možno spomenúť vnútorný konflikt medzi umierneným krídlom HSL'S vedeným Jozefom Tisom a radikálnym krídlom, ktorého predstaviteľom sa stal Vojtech Tuka. DRÁBIK, Jakub. *Fašizmus*. Bratislava: Premedia, 2019. S. 463 – 467. ISBN 978-80-8159-781-7. Akési dištancovanie sa ideológie Slovenského štátu of podoby fašizmu v Taliansku či nacistického Nemecka možno badať aj v skorších dielach či prejavoch predstaviteľov Slovenského štátu. Napríklad poslanec slovenského snemu Vojtech Tvrdý pri prijímaní ústavy uviedol: „*Tvorcovia slovenskej ústavy nemohli ísť ale jednostranne ani podľa iných cudzích vzorov. Povšimli si všetky nové zdravé prúdy autoritatívnych štátnych systémov, (...) avšak nemohli ich jednoducho natiahnuť na slovenské pomery (...).*“ Zdroj: Tesnopisecká zpráva o 6. zasadnutí Slovenského snemu v Bratislave v piatok 21. júla 1939 [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/006schuz/s006002.htm>> Obdobne hlavný ideológ režimu Štefan Polakovič zdôrazňoval vlastnú cestu Slovenska pri tvorbe kontúr a obsahu jej štátneho režimu. Porovnaj: POLAKOVIČ, Štefan. *K základom slovenského štátu*. In HRUBOŇ, Anton (ed.). *Ludácka čítanka*. Bratislava: Premedia, 2019. S. 87 – 94. ISBN 978-80-8159-761-9.

predpisov, pričom nám poskytuje pomerne jasný obraz o štruktúre právnych noriem tvoriaci právny systém ako celok.

Odmietnutie klasického parlamentarizmu,¹⁵ a teda aj roly samotného parlamentu ako zákonodarného orgánu, sa prejavilo aj na výslednom usporiadaní právneho poriadku. Základná zákonodarná a ústavodarná úloha naďalej patrila parlamentu – snem bol oprávnený prijímať zákony a ústavné zákony, ktoré mohli meniť alebo dopĺňať ústavnú materiu. Do výlučnej právomoci snemu patrilo prijímať zákony o brannej povinnosti, zákony, ktorými sa ukladajú nové trvalé finančné bremená občanom, zákony o organizácii súdov, o ich pôsobnosti a príslušnosti. Tieto oblasti nemohli byť nahradené inými normotvornými nástrojmi. Ústava tiež deklarovala princíp nadradenosti nad ostatnými právnymi predpismi.¹⁶

Ďalšou zložkou moci, ktorá mohla kreovať právne normy, bola vláda. Tá mala právomoc vydávať nariadenia s mocou zákona podľa § 44 Ústavy 1939, avšak len v prípadoch, ak to vyžadovalo zamedzenie nenahraditeľnej ujmy pre hospodárske, finančné alebo politické záujmy štátu. Zároveň však platilo, že touto formou nebolo možné riešiť otázky spadajúce do výlučnej právomoci snemu alebo vyžadujúce zákonnú úpravu podľa ústavy.¹⁷ Jediný krát, kedy došlo k zásahu do nariadenia právomoci vlády snenom, využíjúc tak ústavou zverenú kompetenciu, bolo na 84. zasadnutí snemu v marci 1942, na ktorom snem zrušil platnosť nariadenia s mocou zákona č. 267/1941 Sl. z. o ochrane nájomníkov. Ústavnoprávny výbor konštatoval, že toto nariadenie nebolo v súlade s § 44 ods. 1 a § 79 ods. 2 Ústavy 1939, pretože ochrana nájomníkov predstavovala obmedzenie súkromného vlastníctva, ktoré si vyžadovalo zákonnú formu. Snem následne prijal zákon, ktorým prevzal obsah nariadenia a zároveň zrušil pôvodné nariadenie.¹⁸

Okrem nariadení s mocou zákona mohla vláda vydávať aj bežné nariadenia podľa § 43 ústavy. Tieto mali nižšiu právnu silu a slúžili predovšetkým na vykonávanie zákonov a ústavných zákonov.

¹⁵ Napriek tomu, že Slovenský štát bol ústavou prehlásený za parlamentnú republiku, toto označenie nebolo pretavené do ústavnoprávnej reality a možno ho označiť za fiktívne. Porovnaj: NEUMANN, Martin. Tvorba ústavy Slovenskej republiky z 21. července 1939 a cesta k jejému prijetí. In *Právněhistorické studie* (2022), 52(1), s. 126 – 127. ZAVACKÁ, Katarína. K tradícii nariadenia právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 216. ISBN 80-210-3021-6.

¹⁶ Ustanovenia § 21 ods. 2 a § 24 písm. b), e), f) a g), § 96 a § 97 ods. 1 a 2 ústavného zákona č. 185/1939 Sl. z. o Ústave Slovenskej republiky. Porovnaj: NEUMANN, Martin. Tvorba ústavy Slovenskej republiky z 21. července 1939 a cesta k jejému prijetí. In *Právněhistorické studie* (2022), 52(1), s. 126 – 127.

¹⁷ ZAVACKÁ, Katarína. K tradícii nariadenia právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 216 - 224. ISBN 80-210-3021-6.

¹⁸ Zpráva o 84. zasadnutí Snemu Slovenskej republiky v Bratislave v stredu 18. marca 1942 [online]. In *Poslanecká snemovňa parlamentu České republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/o84schuz/so84001.htm>>

Ústava v § 98 predpokladala zriadenie Ústavného senátu ako orgánu ochrany ústavnosti, ktorý by bol kompetentný posudzovať súlad podústavných predpisov s ústavou a ústavnými zákonmi, zloženého zo senátnych prezidentov Najvyššieho súdu a Najvyššieho správneho súdu. Senát mal, v zmysle ustanovenia § 6 ods. 1 ústavného zákona o ústavnom senáte konať len na návrh prezidenta republiky, snemu, stáleho výboru snemu, vlády alebo Štátnej rady. V prípade rozhodnutia o nesúlade určitého právneho predpisu s Ústavou 1939, resp. ústavným zákonom mal tak Ústavný senát urobiť uznesenie, pričom toto uznesenie malo byť zverejnené bez odôvodnenia v Slovenskom zákonníku a s odôvodnením v Úradných novinách, pričom nesúladný predpis by stratil platnosť odo dňa zverejnenia uznesenia v Slovenskom zákonníku.¹⁹ Hoci bol 4. februára 1942 na 80. schôdzi snemu ústavný zákon o Ústavnom senáte prijatý, tento orgán nikdy nezačal reálne fungovať.²⁰

(Po)vojnový (ne)ústavný chaos

Po vzniku exilovej vlády Československej republiky a ustanovení tzv. dočasného štátneho zriadenia (1939 – 1945), ktorým sa malo kontinuálne nadviazať na právny stav predmníchovského Československa pri súčasnej absolútnej neplatnosti právnych aktov prijatých po 30. septembri 1938,²¹ bolo obdobie rokov 1939 – 1945 poznačené nemožnosťou riadnej normotvorby, v dôsledku čoho vznikla praktická potreba osobitného normotvorného mechanizmu. Tým sa stali dekréty prezidenta republiky, vydávané na základe ústavného dekrétu č. 2/1940 Úr. vest. o dočasnej úprave výkonu zákonodarnej moci. Dekréty nahrádzali bežný legislatívny proces a boli neskôr dodatočne ratifikované zákonom č. 57/1946 Sb., čím získali spätnú zákonnú (a ústavnú) legitimitu. Mnohé z nich zásadne menili charakter československého právneho poriadku – jednak z dôvodu revízie legislatívy prijatej počas existencie slovenského a protektorátneho režimu, ale aj v súvislosti s

¹⁹ Návrh č. 453 poslanca Dr. Martina Sokola a spoločníkov na vydanie ústavného zákona o Ústavnom senáte [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <https://www.psp.cz/eknih/1939ssr/tisky/to453_00.htm>

²⁰ Porovnaj: NEUMANN, Martin. Tvorba ústavy Slovenskej republiky z 21. července 1939 a cesta k jejému prijatí. In *Právněhistorické studie* (2022), 52(1), s. 128 - 129. 33. Zpráva o 80. zasadnutí Snemu Slovenskej republiky v Bratislave v stredu 4. februára 1942 [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/o80schuz/so80002.htm>>

²¹ To znamená, že *de iure* naďalej v zásade platila Ústavná listina (zákon č. 121/1920 Sb. z. a n.) a právne predpisy, ktoré boli na území Československa, resp. Slovenska prijaté po 30. septembri 1938, vrátane Ústavy 1939, mali byť nulitné. Povojnový právny režim sa teda opieral aj o pôvodné normy prvej ČSR; ich aplikácia však bola značne selektívna a často modifikovaná aktuálnymi politickými a spoločenskými požiadavkami. Pozri napríklad: LYSÝ, Miroslav. *Slovenské právne dejiny I. Vývoj ústavného a správneho práva na Slovensku od najstarších čias po súčasnosť*. Šamorín: Heuréka, 2021. S. 50 - 54. ISBN 978-80-8173-114-3.

povojnovou obnovou štátu a spravodlivosti.²² Je však nutné pripomenúť, že dekretálna právomoc prezidenta sa územia Slovenska prakticky dotkla až po oslobodení území a postupnom preberaní moci centrálnou vládou po vojne.

Počas Slovenského národného povstania v roku 1944 vystúpila na scénu Slovenská národná rada (SNR) ako orgán, ktorý si revolučne prisvojil zákonodarnú a výkonnú moc na území Slovenska. Zásadný význam malo nariadenie SNR č. 1/1944, ktoré malo ústavnoprávny charakter a ktorým bol založený nový slovenský právny subporiadok. Tento akt možno chápať ako revolučný z hľadiska dejín aj práva. V zmysle konceptu "právnej revolúcie", ako ju definuje Jean-Louis Halpérin, išlo o zásadnú, rýchlu, násilnú a trvalú zmenu, ktorá viedla k zavedeniu nového právneho systému.²³

Významným problémom bolo konkurenčné napätie medzi nariadeniami SNR a dekrétmi prezidenta republiky, napríklad v otázkach recipovania právneho poriadku, či reštitúcie arizovaného majetku.²⁴ Tento praktický právny stav vyplývajúci z charakteru doby, ktorého bol produktom bol vyriešený tým, že kým na úrovni medzinárodného práva bola zachovaná kontinuita československého štátu, z vnútroštátneho hľadiska SNR založila svojím prvým nariadením nové ohnisko slovenského právneho subporiadku.²⁵ Riešenie vzťahu medzi SNR a jej nariadeniami a právnymi aktmi prijatými centrálnymi československými orgánmi napokon priniesli tzv. Pražské dohody, pričom vývoj smeroval k obmedzeniu právomocí SNR a bol ovplyvnený rastúcim vplyvom Komunistickej strany Československa v rámci politického systému Národného frontu. Po prijatí 3. pražskej dohody sa vytvoril právny úzus, v zmysle ktorého nariadenia SNR kompatibilné so zákonmi zostali v platnosti, nariadenia v rozpore so zákonmi boli derogované buď novelizáciou, alebo prijatím nových zákonov s celoštátnou platnosťou. Príkladom je reštitučný zákon č. 128/1946 Zb.²⁶

²² ZAVACKÁ, Katarína. K tradícii nariaďovacej právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 224 – 238. ISBN 80-210-3021-6.

²³ Porovnaj: ZAVACKÁ, Katarína. K tradícii nariaďovacej právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 225 – 227. ISBN 80-210-3021-6. GÁBRIŠ, Tomáš. Revolučné akty a (dis)kontinuita z pohľadu teórie práva a dejín práva. In LYSÝ, Miroslav – POVAŽAN, Michal. *Premeny ústavného práva. Kontinuita a diskontinuita*. Bratislava: Atticum, 2014. S. 76 – 79, 84 – 85. ISBN 978-80-89758-00-5.

²⁴ ZAVACKÁ, Katarína. K tradícii nariaďovacej právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 228 – 234. ISBN 80-210-3021-6.

²⁵ GÁBRIŠ, Tomáš. Revolučné akty a (dis)kontinuita z pohľadu teórie práva a dejín práva. In LYSÝ, Miroslav – POVAŽAN, Michal. *Premeny ústavného práva. Kontinuita a diskontinuita*. Bratislava: Atticum, 2014. S. 76 – 79. ISBN 978-80-89758-00-5.

²⁶ ZAVACKÁ, Katarína. K tradícii nariaďovacej právomoci na Slovensku. In *Česko-slovenská historická ročenka*, 2002. Brno: Masarykova Univerzita v Brne, 2002. S. 234 – 237. ISBN 80-210-3021-6.

KSČ a Národné zhromaždenie

Po februárovom prevrate v roku 1948, kedy Komunistická strana Československa (KSČ) prevzala moc, bola prijatá nová Ústava Československej republiky z 9. mája 1948,²⁷ označovaná aj ako Ústava 9. mája. Formálne nadväzovala na demokratické tradície prvej republiky, avšak reálne odrážala začiatok budovania centralizovaného socialistického štátu.

Systém právnych predpisov sa v zásade vrátil k jednoduchšej hierarchickej štruktúre, na vrchole ktorej stála ústava, pričom tá mala v právnom systéme v zmysle ustanovenia § 171 ods. 3 prioritu pred právnymi normami nižšej právnej sily. Ústava 9. mája tiež obsahovala zásadné garancie ústavnosti, a to najmä v podobe ustanovenia § 65, v zmysle ktorého bolo predsedníctvo Národného zhromaždenia oprávnené vykonávať kontrolu zákonodarného procesu a ústavnosti, i keď nešlo o súdnu kontrolu v pravom slova zmysle. V tomto kontexte je o to zaujímavejšie ustanovenie § 172 ods. 2 Ústavy 9. mája, ktoré explicitne určovalo, že zákony prijaté po 9. júni 1948²⁸ pokiaľ odporovali Ústave 9. mája alebo ústavným zákonom, boli neplatné. Zákon, ktorý by bol v rozpore s ústavou teda mal byť neplatný *ex offio*. Vystáva otázka, akú pozíciu v tomto ohľade malo zohrávať predsedníctvo Národného zhromaždenia ako orgán kompetentný posudzovať ústavnosť právnych predpisov. Vzhľadom na znenie ustanovení § 65 a § 172 možno dôjsť k záveru, že takého rozhodnutie predsedníctva Národného zhromaždenia by malo len deklaratórny účinok. Funkcia predsedníctva Národného zhromaždenia kontroly ústavnosti už v súvislosti s ústavnými zmenami v roku 1960 zanikla, keďže ústavný zákon č. 100/1960 Zb. Ústava Československej socialistickej republiky (ďalej len „Ústava ČSSR“) už takéto ustanovenie neobsahoval.²⁹

Do štruktúry právnych noriem možno zasadiť v tomto období opatrenia predsedníctva Národného zhromaždenia. Predsedníctvo v čase, kedy Národné zhromaždenie nezasadalo alebo bolo odročené, resp. po tom, čo Národnému zhromaždeniu uplynulo volebné obdobie, mohlo vydávať neodkladné opatrenia, ktoré mali silu zákona a ktoré podliehali dodatočnej ratihabícii zo strany Národného zhromaždenia.³⁰

Významný prvkom v systéme právnych noriem po februárovom prevrate³¹ sa stali rozhodnutia KSČ formulované na zjazdoch či výstupoch Ústredného výboru. I keď

²⁷ Ústavný zákon č. 150/1948 Sb.

²⁸ Deň, kedy bola ústava vyhlásená a nadobudla účinnosť.

²⁹ Ústava ČSSR vo svojom ustanovení § 111 ods. 2 obsahuje len strohú formuláciu „*Zákony ani iné právne predpisy nesmú odporovať ústave.*“

³⁰ Ustanovenie § 66 ústavného zákona č. 150/1948 Sb. Ústava Československej republiky.

³¹ Na tomto mieste možno spomenúť aj pramene práva stojace popri klasickej štruktúre, a to pravidlá socialistického spolužitia špecificky v oblasti občianskoprávnych vzťahov. Pozri bližšie: 6.GÁBRIŠ,

Ústava 9. mája ešte nepoznala KSČ ako ústavnú kategóriu, na rozdiel od právneho stavu po prijatí socialistickej ústavy v roku 1960, význam vnútrostraníckych rozhodnutí na kreovanie právnych noriem je nesporný.³² Vôľa strany sa stala základným stavebným kameňom právneho systému, z ktorého následne vychádzali rozhodnutia štátnych orgánov, a teda i keď priznať straníckym uzneseniam či rozhodnutiam charakter normatívneho aktu by bolo problematické, je zjavné, že boli hnacím motorom všetkých právnych predpisov prijatých po februári 1948 až zmeny v politickom systéme po Nežnej revolúcii, ktoré prebiehali v novembri – decembri 1989.³³ Samotný proces tvorby ústavy ako základnej normy bol vzhľadom na usporiadanie štátnej moci od popudu k jej zmenám, cez prípravu jej návrhu až odobrenie tohto návrhu tak, aby mohol prejsť schvaľovacím procesom, ktorý formálne vyžadovala ústava, plne v rukách KSČ.³⁴

Na základe spoločenských požiadaviek v období pražskej jari v roku 1968 došlo k prijatiu ústavného zákona o československej federácii (č. 143/1968 Zb.), ktorým bola ČSSR transformovaná na federatívny štát so samostatnými republikovými orgánmi – Českou socialistickou republikou (ČSR) a Slovenskou socialistickou republikou (SSR). Federalizácia priniesla do systému symetrické rozdelenie štátnej moci medzi federálne a republikové orgány. Súčasťou ústavných reforiem malo byť aj zriadenie ústavného súdu (šiesta hlava ústavného zákona), ako inštitúcie určeného na kontrolu ústavnosti právnych predpisov, a to na celofederálnej úrovni, ale i v prípade konfliktu medzi národným a federálnym predpisom.³⁵ Hoci ústavný súd bol koncepčne zakotvený, v skutočnosti nezačal reálne fungovať – najmä kvôli politickému obratu

Tomáš – LACLAVÍKOVÁ, Miriam. Pravidlá socialistickeho spolužitia ako špecifický nástroj socialistickeho práva (neukončená polemika civilistiky v ČSSR). In *Právněhistorické studie* (2025), 55(2), s. 101 – 121. To, že právo po roku 1948 bolo úzko prepojené s ideológiou KSČ svedčia aj mnohé iné aspekty totalitného režimu, vrátane zmien v systéme súdnictva. Pozri napríklad: ZAPLETALOVÁ, Petra. Soudružské soudy jako nástroj socialistické demokracie ve vybraných státech východního bloku. In *Právněhistorické studie* (2024), 54(3), s. 139 – 164.

³² ARENDT, Hannah. *The Origins of Totalitarianism*. New York: Harcourt Brace, 1976. S. 365. ISBN 0-15-670153-7. ZDOBINSKÝ, Stanislav, et al. *Státní právo socialistických zemí*. Praha: Panorama, 1983. S. 61.

³³ Porovnaj: ZDOBINSKÝ, Stanislav, et al. *Československá ústava. Komentář*. Praha: Panorama, 1988. S. 11 – 32, 63 – 69. MATOUŠEK, Stanislav. *Štátní právo ČSSR*. Bratislava: Obzor, 1987. S. 92 – 98. PEŠEK, Jan. *Centrum moci. Aparát Ústředního výboru Komunistické strany Slovenska 1948 – 1989*. Bratislava: AEP, 2007. S. 12 – 36. ISBN 80-88880-71-8. LYSÝ, Miroslav. *Slovenské právní dějiny I. Vývoj ústavního a správního práva na Slovensku od nejstarších čias po súčasnosť*. Šamorín: Heuréka, 2021. S. 118. ISBN 978-80-8173-114-3.

³⁴ Ani dobová právna doktrína skutočnú úlohu strany v normotvornom procese neskrývala. Pozri: ZDOBINSKÝ, Stanislav, et al. *Státní právo socialistických zemí*. Praha: Panorama, 1983. S. 73 – 75.

³⁵ Ustanovenie § 86 ods. 1 a § 87 ústavného zákona č. 143/1968 Zb. o československej federácii.

po auguste 1968 a následnej normalizácii. Ústavná kontrola teda aj naďalej chýbala, a ústavné garancie zostávali v zásade deklaratívne.³⁶

Demokratizácia a právny štát – post-komunistický ústavný model

K zásadnému zlomu v ústavnom vývoji Československa došlo po novembri 1989, kedy sa tzv. nežná revolúcia stala impulzom pre rozpad totalitného režimu. Jedným z prvých krokov bola novelizácia ústavy, ktorou sa zrušilo kľúčové ustanovenie, čl. 4 Ústavy ČSSR, ktorý zaručoval vedúce postavenie KSČ.³⁷ Týmto zásahom došlo de lege k zrušeniu monopolného postavenia KSČ aj v normotvorbe.

V rámci transformácie ústavného systému bola opätovne oživená myšlienka inštitucionálne zabezpečenej ústavnej kontroly. V nadväznosti na to bol prijatý ústavný zákon č. 91/1991 Zb. o Ústavnom súde Českej a Slovenskej Federatívnej Republiky, ktorým bol zriadený Ústavný súd ČSFR, a to nielen v rovine formálnej, ale aj faktickej, keď už v roku 1991 začal reálne fungovať ako nezávislý súdny orgán na ochranu ústavnosti. Ústavný súd bol vybavený právomocou posudzovať súlad právnych predpisov s ústavou, ako aj rozhodovať o ústavných sťažnostiach jednotlivcov, čím sa zásadne posilnila ochrana základných práv a slobôd.³⁸ Tento krok predstavoval dôležitý pilier obnovy právneho štátu a výrazný odklon od formálnej ústavnosti predchádzajúcich režimov.

Spoločenské a politické zmeny vyvolali aj potrebu úplne nového ústavného rámca, ktorý by reflektoval demokratické hodnoty, oddelenie moci, právny štát a zaručoval základné práva a slobody občanov. V tomto kontexte prebiehali práce na príprave nových ústav ako v celoštátnom, tak aj v republikovom rámci. Proces kulminoval po rozpade Českej a Slovenskej Federatívnej Republiky (ČSFR) k 1. januáru 1993, keď nadobudli účinnosť nové samostatné ústavy oboch nástupníckych štátov: Ústava Slovenskej republiky, prijatá 1. septembra 1992 (účinná od 1. 1. 1993) a Ústava Českej republiky, prijatá 16. decembra 1992.³⁹ Tieto nové ústavy predstavujú základné právne dokumenty moderných demokratických štátov a sú výsledkom historického vývoja, ktorý siaha od prvorepublikovej ústavnosti, cez totalitné deformácie až po obnovenie demokracie a právneho štátu na konci 20. storočia.

³⁶ CHOVANEC, Jaroslav. Historicko-právne východisko k vzniku Ústavného súdu SR (ústavné súdnictvo podľa úst. zák. o čs. federácii. In *Štát a právo* (2020), 2-3, s.118 – 129.

³⁷ Ústavný zákon č. 135/1989 Zb., ktorým sa mení ústavný zákon č. 100/1960 Zb. Ústava Československej socialistickej republiky.

³⁸ CHOVANEC, Jaroslav. Historicko-právne východisko k vzniku Ústavného súdu SR (ústavné súdnictvo podľa úst. zák. o čs. federácii. In *Štát a právo* (2020), 2-3, s.118 – 129.

³⁹ Pozri bližšie: RYCHLÍK, Jan. Rozdělení Československa 1989-1992. Praha: Vyšehrad, 2022. 512 s. ISBN 978-80-76016-019.

Záver

V súlade s myšlienkovou líniou kritických právnych štúdií a na základe skutočností identifikovaných v tomto článku možno jednoznačne konštatovať, že právny poriadok neexistuje oddelene od politicko-spoločenskej reality a ako taký reflektuje mocenské zmeny v štáte. V každom období, ktoré sme analyzovali je zreteľné svojské mocenské pôsobenie vládnucich skupín na právny systém a jednotlivé jeho normy, vrátane základnej normy, t. j. ústavy. V období vojnového autoritatívneho Slovenského štátu ťažisko normotvorby prešlo z parlamentu na vládu v podobe nariadení s právnou silou zákona a neexistovala funkčná kontrola ústavnosti. V období rokov 1944 – 1948 zas hlavnú úlohu v oblasti formovania štruktúry právnych noriem niesla SNR ako revolučný orgán, produkt praktických potrieb vyplývajúcich zo Slovenského národného povstania. V rokoch 1948 – 1989 následne najvýznamnejšie postavenie zastávali štruktúry Komunistickej strany Československa ako vedúcej mocenskej sily v štáte, ktorých rozhodovacie procesy boli predsadené pred ústavné orgány tvoriace právne normy. Príznačné pre tieto obdobia je tiež neexistencia efektívnej kontroly ústavnosti, i keď ústavný poriadok vytvorenie takéhoto orgánu predpokladal ako v období Slovenského štátu, tak aj po roku 1948. Keďže sa však jednalo o autoritatívne, resp. totalitné režimy, takáto kontrola ústavnosti bude nevyhnutne len fiktívna, keďže v opačnom prípade by si vládnuca elita musela priznať, že v jej myšlienkach existuje vnútorný rozpor. Skúsenosť s ústavnými zmenami v 20. storočí nám o to intenzívnejšie signalizuje potrebu chrániť základné ústavné hodnoty a vyvarovať sa častým svojvoľným a neuváženým zmenám ústavy.

Zoznam použitej literatúry

1. ARENDT, Hannah. On the Nature of Totalitarianism. In KOHN, Jerome (ed.). *Essays in Understanding (1930 – 1954)*. New York: Harcourt Brace, 1994. S. 328 – 360. ISBN 0-15-172817-8.
2. ARENDT, Hannah. *The Origins of Totalitarianism*. New York: Harcourt Brace, 1976. 527 s. ISBN 0-15-670153-7.
3. DRÁBIK, Jakub. *Fašizmus*. Bratislava: Premedia, 2019. 644 s. ISBN 978-80-8159-781-7.
4. FINNIS, John. *Natural Law and Natural Rights*. Oxford: Clarendon Press, 2011. 494 s. ISBN 978-0-19-959914-1.
5. GÁBRIŠ, Tomáš. Revolučné akty a (dis)kontinuita z pohľadu teórie práva a dejín práva. In LYSÝ, Miroslav – POVAŽAN, Michal. *Premeny ústavného práva. Kontinuita a diskontinuita*. Bratislava: Atticum, 2014. S. 71 – 92. ISBN 978-80-89758-00-5.

6. GÁBRIŠ, Tomáš – LACLAVÍKOVÁ, Miriam. Pravidlá socialistického spolužitia ako špecifický nástroj socialistického práva (neukončená polemika civilistiky v ČSSR). In *Právněhistorické studie* (2025), 55(2), s. 101 – 121.
7. CHOVANEC, Jaroslav. Historicko-právne východisko k vzniku Ústavného súdu SR (ústavné súdnictvo podľa úst. zák. o čs. federácii). In *Štát a právo* (2020), 2-3, s.118 – 129.
8. KELMAN, Mark. *A guide to critical legal studies*. Cambridge: Harvard University Press, 1987. 360 s. ISBN 0-674-36756-1.
9. KELSEN, Hans. *Čistá právna veda*. Krásno nad Kysucou: Kalligram, 2018. 190 s. ISBN 978-80-89916-21-4.
10. KELSEN, Hans. On the Basic Norm. In *California Law Review* (1959), 47(1), s. 107 – 110.
11. LOEWENSTEIN, Karl. Dictatorship and the German Constitution: 1933-1937. In *The University of Chicago Law Review* (1937), 4(4), s. 537 – 574.
12. LOEWENSTEIN, Karl. Law in the Third Reich. In *The Yale Law Journal* (1936), 45(5), s. 779 – 815.
13. LYSÝ, Miroslav. *Slovenské právne dejiny I. Vývoj ústavného a správneho práva na Slovensku od najstarších čias po súčasnosť*. Šamorín: Heuréka, 2021. 191 . ISBN 978-80-8173-114-3.
14. MATOUŠEK, Stanislav. *Štátne právo ČSSR*. Bratislava: Obzor, 1987. 484 s.
15. MERLI, Franz. Principle of Legality and the Hierarchy of Norms. In SCHROEDER, Werner (ed.): *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation*. London: Bloomsbury, 2016. S. 37 – 45. ISBN 9781849469500.
16. MORADI, Shuresh. A Critical Legal Study of the Declaration of the Rights of Man and of the Citizen. In *Beijing Law Review* (2019), 10, s. 1137 – 1171.
17. NEUMANN, Martin. Tvorba ústavy Slovenskej republiky z 21. července 1939 a cesta k jejému prijatí. In *Právněhistorické studie* (2022), 52(1), s. 113 – 131.
18. PEŠEK, Jan. Centrum moci. Aparát Ústredného výboru Komunistickej strany Slovenska 1948 – 1989. Bratislava: AEP, 2007. 268 s. ISBN 80-88880-71-8.
19. POLAKOVIČ, Štefan. *K základom slovenského štátu*. In HRUBOŇ, Anton (ed.). *Ludácka čítanka*. Bratislava: Premedia, 2019. S. 87 – 94. ISBN 978-80-8159-761-9.
20. RAZ, Joseph. H. L. A. Hart (1907 – 1992). In *Utilitas* (1993), 5(2), s. 145 – 156.
21. RYCHLÍK, Jan. Rozdělení Československa 1989-1992. Praha: Vyšehrad, 2022. 512 s. ISBN 978-80-76016-019.
22. SHAPIRO, Scott J. What is the rule of recognition (and does it exist) [online]? In *Yale Law School, Public Law & Legal Theory Research Paper Series Research Paper No. 181*. 34 s. Dostupné dňa [23-09-2025]. Dostupné na: <http://papers.ssrn.com/abstract#1304645>

23. UNGER, Roberto Mangabeira. *The Critical Legal Studies Movement*. Cambridge: Harvard University Press, 1986. 128 s. ISBN 0-674-17735-3.
24. ZAPLETALOVÁ, Petra. Soudružské soudy jako nástroj socialistické demokracie ve vybraných státech východního bloku. In *Právněhistorické studie* (2024), 54(3), s. 139 – 164.
25. ZAVACKÁ, Katarína. K tradícii nariaďovacej právomoci na Slovensku. In *Česko-slovenská historická ročenka, 2002*. Brno: Masarykova Univerzita v Brne, 2002. S. 195 – 238. ISBN 80-210-3021-6.
26. ZDOBINSKÝ, Stanislav, et. al. *Československá ústava. Komentář*. Praha: Panorama, 1988. 531 s.
27. ZDOBINSKÝ, Stanislav, et al. *Státní právo socialistických zemí*. Praha: Panorama, 1983. 419 s.

Právne predpisy

1. Zákon č. 121/1920 Sb. z. a n., ktorým sa uvádza Ústavná listina Československej republiky
2. Zmluva o ochrannom pomere medzi Nemeckou ríšou a Slovenským štátom zo dňa 23. marca 1939
3. Ústavný zákon č. 185/1939 Sl. z. Ústava Slovenskej republiky
4. Ústavný dekrét č. 2/1940 Úr. vest. o dočasnej úprave výkonu zákonodarnej moci
5. Ústavný zákon č. 150/1948 Sb. Ústava Československej republiky
6. Ústavný zákon č. 100/1960 Zb. Ústava Československej socialistickej republiky
7. Ústavný zákon č. 143/1968 Zb. o československej federácii
8. Ústavný zákon č. 135/1989 Zb., ktorým sa mení ústavný zákon č. 100/1960 Zb. Ústava Československej socialistickej republiky
9. Ústavný zákon č. 91/1991 Zb. o Ústavnom súde Českej a Slovenskej Federatívnej Republiky
10. Ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky
11. Ústavný zákon č. 90/2001 Z. z., ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov
12. Ústavný zákon č. 422/2020 Z. z., ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov
13. Schválené znenie ústavného zákona z 26. septembra 2025, ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov [online]. In *Národná rada Slovenskej republiky*. Dostupné dňa [27-09-2025]. Dostupné na: <nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=573829>

Stenoprotokoly, dôvodové správy, primárne pramene

1. Dôvodová správa k návrhu ústavného zákona č. 733, ktorým sa mení a dopĺňa Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov

- [online]. In *Národná rada Slovenskej republiky*. Dostupné dňa [27-09-2025]. Dostupné na: <nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=560649>
2. Tesnopisecká zpráva o 6. zasadnutí Slovenského snemu v Bratislave v piatok 21. júla 1939 [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/006schuz/s006002.htm>>
 3. Návrh č. 453 poslanca Dr. Martina Sokola a spoločníkov na vydanie ústavného zákona o Ústavnom senáte [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <https://www.psp.cz/eknih/1939ssr/tisky/to453_00.htm>
 4. Zpráva o 80. zasadnutí Snemu Slovenskej republiky v Bratislave v stredu 4. februára 1942 [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/080schuz/s080002.htm>>
 5. Zpráva o 84. zasadnutí Snemu Slovenskej republiky v Bratislave v stredu 18. marca 1942 [online]. In *Poslanecká snemovňa parlamentu Českej republiky*. Dostupné dňa [26-09-2025]. Dostupné na: <<https://www.psp.cz/eknih/1939ssr/stenprot/084schuz/s084001.htm>>

Kontaktné údaje

Mgr. Terézia Švedová, PhD.

terezia.cokynova@flaw.uniba.sk

Katedra právnych dejín a právnej komparatistiky

Právnická fakulta

Univerzita Komenského v Bratislave

PÁR POZNÁMOK K PRAMEŇOM HISTORICKÉHO A POZITÍVNEHO KÁNONICKÉHO PRÁVA

A FEW REMARKS ON THE SOURCES OF HISTORICAL AND POSITIVE CANON LAW

Vojtech Vladár¹

Abstrakt: Pramene práva možno označiť za jeden z najdôležitejších zdrojov informácií nielen pre právnikov, právnych historikov, ale i ostatných vedcov. V prameňoch kánonického práva sa pritom odjakživa odzrkadľoval vývoj Katolíckej cirkvi ako právne dokonalej spoločnosti. Z pohľadu zákonodarnej moci je zaujímavé, že držitelia úradu rímskeho biskupa sa svojej kompetencie univerzálneho zákonodarcu ujali až postupne, pričom do 13. storočia boli hlavným kánonickoprávnym prameňom súkromné zbierky. Obdobne možno sledovať, že zatiaľčo v raných prameňoch poväčšine dochádzalo ku kombinácii morálnych a právnych noriem, situácia sa zmenila za čias klasického kánonického práva, keď právny systém Katolíckej cirkvi začal dominovať (spolu s rímskym právom) právnictvu ako takému. Tento prístup sa opätovne zmenil až po vydaní platného Kódexu kánonického práva, v ktorom sa opätovne prejavili snahy o kombinovanie právnych noriem s normami morálnymi. Hlavným cieľom príspevku je poukázať na uvedené fenomény na príklade konkrétnych historických či platných kánonickoprávnych prameňov Latinskej cirkvi a nachádzať dôvody tohto vývoja.

Kľúčové slová: kánonické právo, pramene práva, pápež, morálne a právne normy, história, súčasnosť

Abstract: Sources of law can be considered one of the most important sources of information not only for lawyers, legal historians, but also for other scholars. The sources of canon law then have always reflected the development of the Catholic Church as a legally perfect society. From the perspective of legislative power, it is interesting that the holders of the office of Bishop of Rome assumed their powers of universal legislator only gradually, with private collections being the main source until the 13th century. Similarly, it can be observed that while in the early sources there was mostly a combination of moral and legal rules, the situation changed during the time of classical canon law, when the

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav kánonického práva.

legal system of the Catholic Church began to dominate (together with Roman law) the jurisprudence as such. This approach changed again only with the publication of the valid Code of Canon Law, in which efforts to combine legal and moral rules were again manifested apparently. The main goal of the paper is to point out the above phenomena using the example of specific historical or valid canon law sources of the Latin Church and to find the reasons for this development.

Key words: canon law, sources of law, Pope, moral and legal rules, history, present day

Úvod

Téma prameňov práva patrí k tým najdôležitejším pri štúdiu každého právneho systému, keďže tie prirodzene predchádzajú jeho vzniku. V prípade kánonického práva možno uvedené konštatovanie ilustrovať skutočnosťou, že i vzniku Evanjelií predchádzala ústna Tradícia, ktorá sa neskôr dočkala písomného zaznamenania. Aj z toho dôvodu býva problematika prameňov pravidelne zaraďovaná medzi ústredné témy každej monografie zaoberajúcej sa pozitívnym právom, pričom na ne nezabúda ani literatúra venujúca sa právnym dejinám. Štúdiom tejto problematiky môžeme zároveň detailne skúmať účinky práva v určitých, pre nás už dnes uzavretých obdobiach, cez ktoré môžeme sledovať vývoj rôznorodých právnych vzťahov a právnych inštitútov od ich vzniku, až do prípadného zániku alebo transformácie, spolu s ich dosahom na život členov Katolíckej cirkvi. Pramene málokterého právneho systému sa pritom vyznačujú takou výnimočnosťou, ako tie kánonickoprávne, keďže obsahujú vzácne informácie nielen pre kánonistov, respektíve právnikov či právnych historikov vo všeobecnosti, ale taktiež odborníkov na všeobecné dejiny, sociológov, filozofov, filológov atď.² Ako sa totiž na to bežne zabúda, z dôvodu úzkeho prepojenia kresťanského náboženstva so spoločenským životom Cirkvi počas celých stáročí determinujúcim spôsobom ovplyvňovala vývoj v Európe.³ Hlavným cieľom tohto článku je pozrieť sa na pramene historického i pozitívneho kánonického práva skrze fenomény postupného ujímania sa funkcie univerzálneho zákonodarcu zo strany rímskeho biskupa, ako aj obsahovej analýzy vybraných prameňov z pohľadu prepájania práva a morálky. Tak, ako je v kánonistike zaužívané, chronologicky budeme postupovať v súlade s členením dejín kánonického

² Bližšie som sa touto problematikou zaoberal v článku VLADÁR, Vojtech: Význam štúdia prameňov kánonického práva pre súčasnú vedu. In *Revue církevního práva*. Roč. 29 (2023), č. 3, s. 13–29.

³ Bližšie k tejto problematike pozri BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995, s. 84n.

práva na podklade prameňov, aplikovanou kardinálom Pietrom Gasparri († 1934) v jeho známom Predhovore ku Kódexu kánonického práva z roku 1917.⁴

Ius historicum

Ius antiquum

Ak sa bližšie pozrieme na tzv. obdobie starobylého práva, počas apoštolskej doby, t.j. za života apoštolov a ich bezprostredných žiakov (teda približne v posledných dvoch tretinách 1. storočia), ešte nemôžeme hovoriť o nejakom cirkevnom, či kánonickom práve *stricto sensu*. Život kresťanov v oblasti práva bol totiž riadený prevažne právnou obyczajou.⁵ Prvotná Cirkev na navyše spočiatku kládla dôraz na normy morálneho kódexu, tak ako ich prijala v Ježišovom „kázaní na hore“.⁶ Až s rastom počtu členov Cirkvi bolo nutné začať vytvárať organizačné štruktúry a nahradiť tzv. pneumatickú demokraciu, v ktorej Cirkev dovtedy existovala. Takto sa najneskôr v 2. storočí presadil monarchický episkopát, z ktorého sa postupne vyvíjal aj primát rímskeho biskupa – Petrovho nástupcu v jej vedení.⁷ V priebehu prvých troch storočí od vzniku Cirkvi ťažisko normotvorby spočívalo predovšetkým v miestnych cirkvách. Takéto ustanovenia partikulárneho práva však v tejto dobe nie raz nadobúdali univerzálny charakter a postupom času sa šírili ďalej, a to najmä prostredníctvom ústneho podania a spisov cirkevných Otcov. V tomto období nemôžeme, najmä kvôli decentralizovanej správe, vôbec hovoriť o pápežskom zákonodarstve. Jurisdikcia rímskych biskupov sa totiž obmedzovala na riešenie rôznych sporov,⁸ keďže od začiatku sa rôzne cirkevné autority v sporných prípadoch obracali o rozhodnutie práve k nim. Pápežské listy, ako odpovede na takéto otázky, sa od pápeža Félix I. (268–273) pritom začínajú nazývať ako dekretálie (*litterae decretales*). Vďaka autorite, ktorú rímski biskupi požívali, tieto rozhodnutia v individuálnych prípadoch postupne nadobúdali normatívny charakter. Hlavným prameňom tohto obdobia bola ale

⁴ Porov. Praefatio ad Codicem iuris canonici anno 1917.

⁵ To prirodzene neznamená, že by už vtedy neexistovali určité pravidlá správania sa (normy) pre príslušníkov Cirkvi, ktorých zachovávanie bolo sankcionované autoritou apoštola, ako o tom svedčí aj Druhý list apoštola Pavla Korintskej cirkevnej obci: „... sme pripravení potrestať každú neposlušnosť, kým nebude vaša poslušnosť úplná“ (2Kor 10,6). Porov. HRDINA, Antonín: *Kánonické právo*. Praha: Eurolex Bohemia, 2002, s. 25.

⁶ Porov. Mt 5,1–7, 29 a Lk 6,17–49.

⁷ Počas prvých storočí však môžeme štruktúru prvotnej Cirkvi vo všeobecnosti popísať ako vystavanú skôr na princípe kolegiálnom, než hierarchickom. Porov. VRANA, Vladimír: *Dejiny cirkevného práva*. Košice: Univerzita P. J. Šafárika, 1992, s. 21.

⁸ Ako príklad by sme mohli spomenúť napríklad rozhodnutie rímskeho biskupa Sotera I. (165–174), ktorý zakázal podporu herézy montanistov; Kalixta I. (217–222), ktorý vydal edikt o pravidlách pokánia; Viktora I. (189–199) v spore o slávenie Veľkej Noci alebo tiež rozhodnutie rímskeho biskupa Štefana I. (254–257) v spore o krst heretikov proti biskupovi Cypriánovi († okolo r. 268). Porov. TRETERA, Jiří R.: *Cirkevní právo*. Praha: Jan Krigl nakladatelství, 1993, s. 20–21.

právna obyčaj a právo kresťanskej Cirkvi počas prvých troch storočí jej existencie bolo zamerané najmä na udržanie disciplíny medzi veriacimi a koncentrovalo sa takmer výlučne na vnútorné záujmy skupiny, čo sa prirodzene začalo meniť v súvislosti so slobodou, ktorá bola Cirkvi priznaná cisárom Konštantínom I. Veľkým (306–337) v roku 313 tzv. Milánskym ediktom.⁹ Na úrovni všeobecného práva sa od 4. storočia zároveň začínajú objavovať nálezy všeobecných (ekumenických) snemov,¹⁰ ktoré spočiatku na Východe cisári vyhlasovali ako ríšske zákony. Pre poznanie prameňov práva tohto obdobia sú však najdôležitejšie súkromné zbierky kánonického práva, pretože spravidla len v nich sa nám zachovali.

Ako prvý referenčný prameň obdobia starobylého práva spomenieme pseudo-apoštolskú zbierku „Doktrína dvanástich apoštolov“, známu hlavne pod gréckym názvom *Διδαχὴ τῶν δώδεκα ἀποστόλων* (*Doctrina duodecim Apostolorum*) z doby okolo roku 100. Tento spis vznikol v Sýrii alebo v Palestíne a predstavuje kresťanské spracovanie starožidovských inštrukcií pre tzv. prozelytov – t.j. pohanov, ktorí prestúpili k židovstvu, užívali práva pohostinstva a boli chránení zákonom. Spis má tri časti¹¹ a šesťnásť kapitol a býva označovaný aj ako katechizmus dvoch ciest – života a smrti.¹² Po Novom Zákone ide o jeden z najstarších zachovaných kresťanských prameňov, pričom úžasnú cenu má najmä pre dejiny cirkevného práva a liturgie.¹³

⁹ V praxi to znamenalo, že sa kresťanská Cirkev stala zákonom uznanou spoločnosťou s právom vlastniť i dediť majetok. Okrem toho sa stala právnickou osobou a duchovenstvo od tejto doby požívalo imunitu formou oslobodenia od naturálnych dávok, verejných služieb a štátnych úradov. Milánsky edikt by sme v podstate mohli považovať aj za dekrét potvrdzujúci slobodu svedomia a náboženského vierovyznania v Rímskej ríši. V prípade tohto prameňa však v skutočnosti nešlo o edikt, ale reskript predstavujúci nariadenie vo forme „obežníku“ pre všetkých miestodržiteľov rímskych provincií (prokonzulov). Porov. Lact., *De mort.* 48,2–13 a Eus., *Hist.* 10,5,1–13. Bližšie k tejto problematike pozri napríklad NEMEC, Matúš: *Štát, cirkev a právo v Rímskej ríši v prvých štyroch storočiach po Kristovi*. Bratislava: Iura Edition, 2005, s. 47.

¹⁰ Prvým takýmto snemom bol koncil v Nicei (Prvý nicejský) v roku 325. Bližšie k tejto problematike pozri napríklad GAJDOŠ, Marcel: *Dokumenty prvých dvoch ekumenických koncilov*. Prešov: Petra, 1999.

¹¹ V prvej časti sú zahrnuté mravné predpisy. V predobrazu dvoch ciest, cesty života a cesty smrti, autor najskôr poskytuje krátky prehľad mravouky. Druhá časť obsahuje liturgické pokyny pre prijatie sviatosti krstu, ustanovenia o pôste (pôst v stredu a v piatok), svätení nedele (ide o prvú známu správu o prenesení sobotného odpočinku na nedeľu), modlitbe a Eucharistii. V tretej časti sú uvedené cirkevnoprávne predpisy o povinnostiach duchovných, o vnútornom zriadení Cirkvi, apoštoloch, prorokoch – učiteľoch, biskupoch a diakonoch. Práca obsahuje i Epilóg, v ktorom autor vyzýva kresťanov, aby vytrvali vo viere a pripomína im, že majú odmietat pukušiteľa vo svete, pripravujúc sa na príchod Ježiša Krista, ktorý príde v sláve. Porov. MORDEL, Štefan: *Patrológia*. Spišská Kapitula – Spišské Podhradie: Nadácia Kňazského seminára biskupa Jána Vojtaššáka, 2004, s. 47.

¹² Porov. ŘÍČAN, Rudolf – MOLNÁR, Amedeo: *12 století církevních dějin*. Praha: Kalich, 1990, s. 67.

¹³ Porov. KRAJČI, Jozef: *Historické pramene a všeobecné normy cirkevného práva*. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, 1997, s. 7.

Práve toto dielo sa stalo základom pre všetky ostatné pseudo-apoštolské zbierky.¹⁴ Pokiaľ ide o jeho obsah, typická je kombinácia kánonickoprávnej matérie s matériou morálnou, pričom prirodzene dominuje tá druhá. Tento prameň sa pritom presadil bez akýchkoľvek zásahov zo strany kompetentných cirkevných autorít, ktoré sa o tieto procesy pričinili prakticky len tým, že jeho šíreniu nekládli žiadne prekážky, považujúc ho za pravoverný. Práve tento prístup možno s určitosťou označiť za najdôležitejší pri formovaní skladby prameňov starobylého práva, v rámci ktorého dominovali súkromné zbierky, pričom zákonodarná autorita Katolíckej cirkvi sa prejavovala len ojedinele, aj to skôr na spôsob istého druhu „case law“ vo forme spomínaných pápežských dekretálií.

Druhou zbierkou, ktorou sa budeme zaoberať, je kolekcia *Capitularia regum Francorum*, obsahujúca predovšetkým zozbierané kapitulárie franských kráľov a cisárov, a to najmä z obdobia tzv. karolínskej renesancie. Toto dielo pochádza z roku 827 a za jeho autora sa považuje opäť Ansegisius z Fontanelly († 833). Uvedený prameň je usporiadaný do štyroch kníh, pričom prvé dve obsahujú *capitularia ecclesiastica*, teda kapitulárie týkajúce sa cirkevných záležitostí.¹⁵ V rokoch 840 až 847 k nej pribudli ďalšie tri knihy, ktoré ale obsahujú kapitulárie vymyslené a za ich autora sa označuje istý diakon Benedikt (*Benedictus levita*). Ansegisiova zbierka dosiahla v galo-franskej oblasti, ale i v Itálii, značnú popularitu a na konciloch a snemoch bola dokonca uznávaná za dočasne platné všeobecné kánonické právo.¹⁶ Pri tejto zbierke je zrejmé, ako absencia zákonodarnej činnosti zo strany univerzálnej autority Katolíckej cirkvi viedla k čiastočnému uzurpovaniu si tejto funkcie svetskými autoritami, k čomu čoraz viac dochádzalo od čias presadenia sa východného a neskôr i západného césaropapizmu. Aj z toho dôvodu jej obsah netvorí len cirkevné zákonodarstvo, ale jej súčasťou sú i normy štátneho práva upravujúceho cirkevné záležitosti. Napriek tomu, že k jej potvrdeniu zo strany univerzálneho cirkevného zákonodarcu nikdy nedošlo, v praxi sa udržala po celé stáročia, ovplyvňujúc vývoj cirkevnej organizácie vo viacerých ohľadoch prakticky až do moderných čias. Jej úspech pritom súvisel predovšetkým so skutočnosťou, že na jej ustanovenia sa odvolával i autor najdôležitejšej kánonickoprávnej zbierky vôbec, teda Graciánovho dekrétu, ktorý platil od svojho zostavenia okolo roku 1140 až do roku 1918, keď bol zrušený prvým Kódexom kánonického práva z roku 1917.

¹⁴ Porov. TRETERA, Jiří R.: *Církevní právo*. Praha: Jan Krigl nakladatelství, 1993, s. 30.

¹⁵ Porov. WIEL, Constant Van de: *History of Canon Law*. Louvain: Peeters Press, 1991, s. 150. Tieto obsahovali zákonodarstvo Pipina III. Krátkeho (751–768), Karola I. Veľkého (768/800–814), Ľudovíta I. Pobožného (813/814–840) a Lothara I. (817/840–855). Porov. MICHAL, Jaroslav: Stručný přehled vývoje kanonického práva do r. 1917. In *Teologické studie. Litera slovem oživená. Sborník semináře v Hradci Králové r. 1984*. Praha: Česká katolická Charita, 1985, s. 23.

¹⁶ Porov. MRKÝVKA, Petr – VESELÁ, Renata: *Vybrané otázky z dějin kanonického práva*. Brno: Masarykova univerzita, 1992, s. 35–36.

Ako tretiu referenčnú zbierku uvedieme *Collectio Cardinalis Deusdedit*, teda Zbierku kardinála Deusdedita († okolo r. 1097), ktorá pochádza približne z roku 1087 a patrí k tzv. gregoriánskym zbierkam. Takto bývajú označované najmä rímske diela, ktoré vznikli pod vplyvom reformných snáh pápeža Gregora VII. (1073–1085) a boja o investitúru.¹⁷ Reformne zameraní pápeži totiž videli práve v kánonickom práve kľúčový nástroj pre vykonanie zmien v Cirkvi.¹⁸ Tieto zbierky čerpali hlavne z rímskych archívov, a to najmä zo spisov z najstaršieho obdobia vývoja Cirkvi, pripúšťajúc zásadne len pravé pramene, ktoré boli pápežom buď priamo vydané alebo ním aspoň potvrdené.¹⁹ Pre všetky je typické, že boli spracované v intenciách pápežskej svetovlády. Zbierka kardinála Deusdedita pozostáva zo štyroch kníh, ktoré poňali všeobecné cirkevné predpisy (o duchovenstve, cirkevnom majetku a imunitách), čerpajúc materiál priamo z rímskeho archívu (ale tiež zo Pseudo-izidoriánskych dekretálií), s cieľom podať zrozumiteľný prehľad kánonickej tradície a zároveň podporiť silu a autoritu Apoštolskej Stolicy.²⁰ Napriek tomu, že tento prameň je spracovaný v intenciách pápežskej svetovlády, netreba zabúdať na skutočnosť, že aj v jeho prípade išlo o dielo súkromné. Z obsahového hľadiska zase dalo vonkajšie vyjadrenie tendenciám vtedajšej doby, reflektujúc myšlienky gregoriánskych reformátorov, ktorí poukazovali na hrubé zasahovanie do vnútorných cirkevných záležitostí zo strany predstaviteľov svetskej moci. Celkom prirodzene, keďže jej úlohou bolo čo najviac posilniť postavenie rímskeho biskupa, nevyhnutné bolo odvolávať sa predovšetkým na právne normy v pápežských dekretáliách.

Ius novum medii aevi

Pre obdobie tzv. klasického práva, ktoré trvalo od zostavenia Graciánovho dekrétu do Tridentského koncilu (1545–1563), je príznačný veľký rozvoj teológie, umenia ale tiež práva. Čo sa týka prameňov práva tejto periódy, tie už obsahujú široko rozvinuté a pevne konštituované kánonické právo, ktoré našlo svoje odzrkadlenie v zbierkach

¹⁷ Porov. NACCI, Matteo: *Ius Proprium ac Nativum*: Brief Reflections on the Historical Evolution of the Sources of Canon Law. In *History Research*. Roč. 6 (2016), č. 2, s. 106.

¹⁸ Porov. BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995, s. 35.

¹⁹ Porov. BUŠEK, Vratislav: *Učebnice dějin práva církevního I*. Praha: Všehrd, 1946, s. 77.

²⁰ Porov. SOMERVILLE, Robert – BRASINGTON, Bruce: *Prefaces to Canon Law Books in Latin Christianity*. London: Yale University Press, 1998, s. 109. Predhovor ku knihe je prezentovaný ako venovací list pápežovi Viktorovi III. (1086–1087). V rámci neho sa osobitne zdôrazňuje, že katastrofálny koniec pontifikátu Gregora VII. v nijakom prípade nezmenšil autorovu vieru v jedinečnú autoritu Rímskej cirkvi, „... aj keď prišla o biskupa.“ Pápež Gregor VII. bol totiž opustený mnohými kardinálmi na začiatku roku 1080 a utiekol do Salerna so svojimi normanskými záchrancami pred obliehaním Ríma cisárom Henrichom IV. (1056/1084–1105). Porov. SCHATZ, Klaus: *Dějiny papežského primátu*. Brno: Centrum pro studium demokracie a kultury, 2002, s. 91n.

12. až 16. storočia. Z hľadiska dejín kánonického práva sa toto obdobie priamo označuje za zlatý vek, keďže kánonické právo sa v ňom vyprofilovalo ako samostatná vedecká i pedagogická disciplína (*scientia iuris Ecclesiae*), popri teológii a svetskom práve.²¹ Ak hovoríme o predgraciánskom práve ako o práve kánonickom, je to trochu nepresné. Tieto normy mali totiž často skôr cirkevnoprávny charakter (v užšom, či širšom zmysle slova).²² Od stvorenia Graciánovho diela však popri znalcoch rímskeho práva (legisti) figurujú i znalci cirkevného (kánonisti) a tzv. učené práva (*iura docta*)²³ predstavujú právo rímske a právo kánonické.²⁴ Čo sa týka zloženia kánonickoprávnych prameňov, dominuje im jednoznačne pápežské zákonodarstvo.²⁵ To sa neobmedzuje len na tvorbu nových právnych predpisov ale usiluje sa tiež o kodifikáciu noriem obsiahnutých v starších zbierkach, vydávaním nových úradných zbierok. V tomto období sa teda stretávame so zbierkami, ktoré pochádzajú priamo od moci zákonodarnej, pričom nie sú len obyčajnými kompiláciami, ale sú priamo knihami zákonov – kódexmi. Objavujú sa ale i diela, ktoré nemali úradný charakter, avšak napriek tomu z vnútorných alebo vonkajších príčin nadobudli význam zbierok úradných. Najdôležitejšie kolekcie tohto obdobia sa napokon stali súčasťou zbierky *Corpus iuris canonici*.²⁶ Ako prvú referenčnú zbierku tohto obdobia musíme, samozrejme, spomenúť Graciánov dekrét (*Concordia Discordantium Canonum, Decretum Gratiani*), ktorý predstavuje najdôležitejší medzník kánonickoprávneho vývoja. Keď ho porovnáваме

²¹ Kánonické právo bolo do tej doby súčasťou teológie. Konkrétne bolo späté s teológiou morálnou a bolo považované za jej disciplinárnu (praktickú) časť. Porov. MICHAL, Jaroslav: *Dějiny pramenů poznání kanonického práva s přihlédnutím k dějinám práva římského*. Praha: Ústřední církevní nakladatelství, 1967, s. 39.

²² Porov. MRKÝVKA, Petr – VESELÁ, Renata: *Vybrané otázky z dějin kanonického práva*. Brno: Masarykova univerzita, 1992, s. 39.

²³ Nazývané tak boli z dôvodu kontrastu k obyčajovému právu a samosprávnemu štatutárnemu právu, ktoré neboli predmetom formálneho štúdia na univerzitných právnických fakultách. Porov. BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995, s. 59 – 60.

²⁴ Porov. ČERNÝ, Miroslav: Počátky kanonistiky jako samostatné právní vědy. In *Právněhistorické studie*. Roč. 45 (2015), č. 2, s. 5n.

²⁵ Postavenie pápežstva v tomto období, najmä vďaka víťazstvu nad svetskou mocou zachytenom vo Wormskom konkordáte (r. 1122), fakticky spelo ku skutočnej vláde nad celou univerzálnou Cirkvou. V tomto období sa tiež v Cirkvi definitívne zakotvila zásada celibátu, utužili sa farnosti a vzrástol význam kláštorov a novozakladaných cirkevných univerzít. Porov. VRANA, Vladimír: *Dejiny cirkevného práva*. Košice: Univerzita P. J. Šafárika, 1992, s. 34. To, že táto doba je vrcholnou dobou pápežskej moci dosvedčuje i fakt, že Gracián nazýval pápežské dekretálie ako *canones*, a teda presne tak, ako sa do tej doby nazývali uznesenia koncilov. Týmto spôsobom dal výraz skutočnosti, že zákonodarná moc pápežov sa im v tejto dobe skutočne vyrovnala a nahradila pre celú Cirkev moc všeobecných koncilov. Porov. BUŠEK, Vratislav: *Učebnice dějin práva církevního I*. Praha: Věšhrad, 1946, s. 86.

²⁶ Porov. RITTNER, Edward: *Církevní právo katolické*. Praha: Právnická jednota, 1887, s. 35.

s inými zbierkami, musíme konštatovať, že v jeho prípade nejde iba o kolekciu kánonov, ale môžeme ho označiť priamo za traktát, v ktorom autor predkladá svoje tvrdenia a usiluje sa ich dokázať tak vnútornými ako aj vonkajšími argumentmi. Gracián pritom pri svojej práci nečerpал len z prameňov pôvodných (t.j. koncilových nálezov, pápežských dekretálií, zo spisov svätých Otcov či zo Svätého Písma) ale aj z neskorších zbierok (*Dionysiana*, *Pseudo-izidoriana*, *Collectio Anselmo dedicata*, *Collectio Burchardi*, *Polycarpus*, zbierky Iva zo Chartres atď.). Väčšinu z nich mal autor Dekréty k dispozícii priamo, niektoré však pravdepodobne citoval len spamäti.²⁷ Mnohé miesta v jeho diele vychádzajú tiež priamo z justiniánskej kodifikácie rímskeho práva²⁸ a iné zase z práva germánskeho. Je teda zrejmé, že z obsahového hľadiska Gracián nečerpал len z prameňov kánonického práva, ale bežne sa odvolával aj na authority rímskeho či germánskeho práva vrátane rôznych teologických prameňov. I keď týmto zdrojom nemožno priznať váhu prameňov práva, v skutočnosti sa na ne cirkevné súdy historicky bežne odvolávali, čo pretrvalo až do roku 1918. Aj pri tomto diele je však nevyhnutné zdôrazniť, že išlo o rýdzo súkromnú zbierku, ktorá sa nikdy nedočkala oficiálneho potvrdenia, respektíve vyhlásenia zo strany najvyššieho cirkevného zákonodarcu.

Ako druhú referenčnú zbierku pre obdobie klasického kánonického práva spomenieme *Liber extra*, respektíve „Dekretálie Gregora IX.“, predstavujúce prvé komplexné, univerzálne, oficiálne a výlučné dielo v histórii Katolíckej cirkvi. Jeho autor, Rajmund z Peňafortu († 1275), konajúci na pokyn pápeža Gregora IX. (1227–1241), vzal za základ svojej práce Päť starobylých kompilácií (*Quinque compilationes antiquae*), spolu s normami pochádzajúcimi od Gregora IX.²⁹ Takýmto spôsobom vznikla zbierka, ktorú pápež spolu s promulgačnou bulou *Rex pacificus* z 5. septembra 1234 zaslal univerzitám v Bologni a v Paríži. Z toho dôvodu v prípade *Liber extra* hovoríme o úradnom prameni, keďže všetky v nej obsiahnuté dekretálie (autentické i sfalšované) majú silu zákona.³⁰ Jej hodnota pritom spočíva najmä v tom, že ide o prvú zbierku výlučnú, čo znamená, že ňou boli zásadne derogované všetky

²⁷ Porov. KAŠNÝ, Jiří: Metoda v kanonickém právu. In *Revue církevního práva*. Roč. 13 (2007), č. 1, s. 8.

²⁸ Porov. BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995, s. 59. Je nevyhnutné ale tiež povedať, že samotný Gracián sa v rímskom práve skutočne vyznal, čo dosvedčujú najmä jeho *dicta*. Zrejme to však boli naozaj až prví komentátori Dekréty, ktorí rozšírili asimiláciu civilného rímskeho práva do práva kánonického, spájajúc tak právne tradície starobylých cisárov s kánonistickou tradíciou, dávajúc tak obe v službu pápežstva a intelektuálneho sveta vrcholného a neskorého stredoveku. Porov. SOMERVILLE, Robert – BRASINGTON, Bruce: *Prefaces to Canon Law Books in Latin Christianity*. London: Yale University Press, 1998, s. 173. Bližšie k tejto problematike pozri VETULANI, Adam: *Z badań nad prawem rzymskiem w dekrecie Gracjana*. Kraków: Drukarnia uniwersytetu jagiellońskiego, 1935.

²⁹ Porov. WIEL, Constant Van de: *History of Canon Law*. Louvain: Peeters Press, 1991, s. 103n.

³⁰ Porov. BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995, s. 55.

dekretálie, ktoré nie sú obsiahnuté buď v Graciánovom dekréte, alebo v nej samotnej.³¹ Pápež Gregor IX. jej publikovaním zároveň pre budúcnosť zakázal zostavovať ďalšie súkromné zbierky bez súhlasu Apoštolskej Stolice.³² Ako je teda zrejmé, toto dielo bolo spracované na pokyn najvyššej cirkevnej zákonodarnej autority s cieľom, aby nahradilo všetky doterajšie kánonickoprávne zbierky (s výnimkou Graciánovho dekrétu). Aj z toho dôvodu obsiahlo prakticky výlučne pápežské dekretálie, čím dalo jasne najavo, že tento prameň má do budúcnosti v právnom systéme Katolíckej cirkvi dominovať. Pokiaľ ide o prepojenie práva s morálkou, to je zrejmé predovšetkým v Graciánovom dekréte, nie však už v diele *Liber extra*, ktorého vzorom boli predovšetkým pramene rímskeho práva, a to najmä justiniánska kodifikácia.³³

Ius novissimum

Toto obdobie zahŕňa dobu od konania Tridentského koncilu v polovici 16. storočia až do vydania prvého Kódexu kánonického práva v roku 1917. Períoda poklasického práva býva tiež označovaná ako obdobie legislatívneho pokoja, pretože počas jeho trvania nebola vydaná žiadna úradná kánonickoprávna zbierka.³⁴ Len pápežské buly a iné listiny priebežne dopĺňali to, čo bolo obsiahnuté v *Corpus iuris canonici*.³⁵ Základom práva tohto obdobia sú tak uznesenia Tridentského koncilu, zbierka *Corpus iuris canonici*, pápežské buly a dekréty Prvého vatikánskeho koncilu (1869 – 1870). Najväčší význam pre kánonické právo v tomto období mal ale Tridentský koncil a jeho zákonodarstvo, ktoré naznačili viaceré nové smery v jeho vývoji. Pápež Pius IV. (1559–1565) bulou *Benedictus Deus* 26. januára 1564 v Ríme promulgoval všetky koncilové dekréty, prísne zakazujúc aby sa bez jeho povolenia k nim vydávali komentáre, glosy, poznámky a sebe, ako hlave Cirkvi, vyhradil tiež vysvetľovanie

³¹ Z tohto dôvodu nemôžeme túto zbierku označiť za úplne exkluzívnu, keďže neobsiahla celé právo a zachovala v platnosti i *Decretum Gratiani*. Porov. MRKÝVKA, Petr – VESELÁ, Renata: *Vybrané otázky z dejín kanonického práva*. Brno: Masarykova univerzita, 1992, s. 42.

³² Svoju vôľu vyjadril pápež v spomínanej promulgačnej bule slovami: *Volentes igitur, ut hac tantum compilatione universi utantur in iudiciis et in scholis, districtius prohibemus, ne quis praesumat aliam facere absque auctoritate sedis apostolicae specialis*. Porov. Rex pacificus. Bližšie k tejto problematike pozri napríklad PEJŠKA, Josef: *Církevní právo I. Ústavní právo církevní*. Semily: Nákladem vlastním, 1932, s. 28. Z tohto dôvodu aj glosy k tejto zbierke nezískali nikdy moc zákona, ako sa to napríklad stalo pri *Glossa ordinaria Decreti Gratiani*. Porov. MICHAL, Jaroslav: *Dějiny pramenů poznání kanonického práva s přihlédnutím k dějinám práva římského*. Praha: Ústřední církevní nakladatelství, 1967, s. 53.

³³ Porov. Rex pacificus.

³⁴ Jedinú výnimku pritom predstavuje prvá časť Bulária pápeža Benedikta XIV. (1740–1757). Porov. HRDINA, A.: *Kanonické právo, EUROLEX BOHEMIA*, Praha (2002), s. 44

³⁵ Porov. TRETERA, Jiří R.: *Církevní právo*. Praha: Jan Krigl nakladatelství, 1993, s. 33.

nejasných miest.³⁶ Z hľadiska obsahu prameňov poklasického obdobia možno v prvom rade konštatovať, že boli koncipované v rovine klasických koncilových dekrétov, respektíve pápežských dekretálií (zhromažďované predovšetkým v pápežských bulariách). S ohľadom na túto skutočnosť a pápežské disponovanie oboma koncilmami, možno konštatovať, že pápežské zákonodarstvo v tejto dobe kánonickému právu jednoznačne dominovalo. Pokiaľ ide o vzťah práva a morálky, v dekrétach Tridentského a Prvého vatikánskeho koncilu dochádzalo k ich odlišovaniu, podobne ako v pápežských dekretáliách tohto obdobia.³⁷

Ius codificatum

Obdobie kodifikovaného práva začína prijatím prvého Kódexu kánonického práva z roku 1917 a končí zákonodarstvom Druhého vatikánskeho koncilu (1962–1965), keď bol celou radou čiastkových zákonov rozsiahle novelizovaný Kódex kánonického práva z roku 1917, až boli napokon promulgované platné kódexy (západný i východný), do ktorých boli tieto zákony poväčšine inkorporované. Prvý Kódex bol promulgovaný na Turíce 27. mája 1917 apoštolskou konštitúciou *Providentissima Mater Ecclesia* a účinnosť nadobudol na Turíce ďalšieho roka, teda 19. mája 1918.³⁸ V jeho prípade išlo o historicky prvý úradný, autentický, jednotný, univerzálny a výlučný zákonník vzťahujúci sa na Latinskú cirkev.³⁹ Enormný význam tohto Kódexu spočíva najmä v skutočnosti, že v jeho prípade nešlo len o zbierku dokumentov ale stručne, jasne a v logickom poriadku usporiadané praktické abstraktné normy.⁴⁰ Práve v tom sa najvýznamnejšie odlišoval od do toho času

³⁶ Porov. FILO, Vladimír: *Kánonické právo. Úvod a prvá kniha*. Bratislava: Rímskokatolícka bohoslovecká fakulta UK, 1997, s. 27. Úradná zbierka týchto rozhodnutí vyšla v roku 1564 pod názvom *Canones et decreta sacrosancti oecumenici et generalis Concilii Tridentini*. Hodnotnú kompiláciu obsahujúcu uznesenia tohto koncilu však predstavuje aj kolekcia *Concilium Tridentinum*. V jej prípade ide o kompletne kritické dielo, obsahujúce celú dokumentáciu spojenú s Tridentským koncilom. Prvýkrát táto zbierka vyšla v Nemecku v roku 1901. Porov. RITTNER, Edward: *Církevní právo katolické*. Praha: Právnická jednota, 1887, s. 56.

³⁷ Porov. VRANA, Vladimír: *Dejiny cirkevného práva*. Košice: Univerzita P. J. Šafárika, 1992, s. 54.

³⁸ Porov. PEJŠKA, Josef: *Církevní právo I. Ústavní právo církevní*. Semily: Nákladem vlastním, 1932, s. 35. Porov. HRDINA, A.: *Kánonické právo*. Praha: Eurolex Bohemia, 2002, s. 53. Dňa 15. septembra 1917 pápež Benedikt XV. zriadil, z dôvodu potreby autentického výkladu možných nejasností v texte, prostredníctvom pápežského *motu proprio Cum Iuris canonici codicem* Komisiu pre autentický výklad Kódexu (*Commissio seu Consilium ad Codicis canones authentica interpretandos*), ktorej nálezy mali byť publikované v Aktoch Apoštolskej Stolice. Porov. KAŠNÝ, Jiří: Metoda v kánonickom právu. In *Revue církevního práva*. Roč. 13 (2007), č. 1, s. 18 a MRKÝVKA, Petr – VESELÁ, Renata: *Vybrané otázky z dějin kanonického práva*. Brno: Masarykova univerzita, 1992, s. 50–51.

³⁹ Porov. KRAJČÍ, Jozef: *Historické pramene a všeobecné normy cirkevného práva*. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, 1997, s. 13.

⁴⁰ Porov. FILO, Vladimír: *Kánonické právo. Úvod a prvá kniha*. Bratislava: Rímskokatolícka bohoslovecká fakulta UK, 1997, s. 29.

dominujúcich pápežských dekretálií, ktoré vo viacerých pohľadoch evokovali tvorbu práva na spôsob „case law“. Obdobne je zrejmé, že zákonodarcom prvého Kódexu bola najvyššia autorita Katolíckej cirkvi, teda pápež. Z hľadiska jeho pomeru medzi právom a morálkou ho možno označiť za výsledok najvýraznejších snáh o odlišenie týchto dvoch disciplín, sledujúc vzory najkvalitnejších prameňov rímskeho práva, podobne, ako to bolo v prípade zbierky *Liber extra*.

Ius vigens

V súčasnosti predstavuje hlavný normatívny text Latinskej cirkvi Kódex kánonického práva z roku 1983, ktorý bol promulgovaný 25. januára 1983 pápežom Jánom Pavlom II. (1978–2005) apoštolskou konštitúciou *Sacrae disciplinae leges*.⁴¹ Ten možno označiť za prepracovanú a revidovanú verziu prvého Kódexu kánonického práva z roku 1917 v duchu dokumentov a záverov Druhého vatikánskeho koncilu. Tento všeobecný koncil z eklesiologického hľadiska vyzdvihol dôležitosť práva v živote Cirkvi a jeho úlohu v samotnom Tajomstve spásy (*mysterium salutis*) (Lumen gentium 14).⁴² Na druhej strane však došlo k čiastočnému zatlačeniu právnicko-inštitucionálneho rozmeru Cirkvi do úzadia a do popredia boli postavené jej prvky nadprirodzeného charakteru, ktoré spočívali najmä na princípoch vedomia viery (*sensus fidei*) a rozoznávania znamení čias (*signa temporum*), odzrkadľujúcich kontinuálne a dynamické pôsobenie Ducha Svätého v ľudskej spoločnosti.⁴³ Koncilové dokumenty obdobne viackrát požadovali uprednostnenie Cirkvi ako spoločenstva veriacich, na úkor rýdzo právnických hierarchických koncepcií. S ohľadom na kolegiálny charakter snemových zasadnutí, rokovaní i prijímanie záverov, bola súčasne vyzdvihnutá potreba obmedzenia centralizačných tendencií univerzálneho práva v prospech decentralizácie a autonómie partikulárnych cirkví

⁴¹ Kódex nadobudol účinnosť 27. novembra 1983. Právo východných katolíckych cirkví *sui iuris* bolo kodifikované na univerzálnej úrovni v Kódexe kánonov východných cirkví (*Codex canonum ecclesiarum orientalium*). Východný Kódex bol promulgovaný (podobne ako západný) pápežom Jánom Pavlom II., a to apoštolskou konštitúciou *Sacri canones* z 18. októbra 1990. Účinnosť nadobudol 1. októbra 1991. Bližšie som sa touto problematikou zaoberal VLADÁR, Vojtech: Kodifikácia práva východných katolíckych cirkví. In *Historia et theoria iuris: printový a e-časopis pre mladých vedeckých pracovníkov právnických fakúlt na Slovensku*. Roč. 2 (2010), č. 3, s. 12n.

⁴² Porov. POJAVNIK, Ivan: *Mysterium concilu*. Olomouc: Matice cyrilometodějská, 1998, s. 262–263.

⁴³ Porov. Mt 16,2–4 a Lk 12,54–56. Tento pojem sa používa na vymedzenie všetkých udalostí, javov, procesov a rozvojových tendencií (nie vždy kladných), ktoré sú charakteristické pre určité historické obdobie a sú výzvou k eticko-spoločenskému konaniu. Porov. Gaudium et spes 4. In AAS 58 (1966), s. 1025–1120. Bližšie k tejto problematike pozri ALBERIGO, Giuseppe: *Stručné dejiny II. vatikánskeho koncilu*. Brno: Barrister & Principal, 2008, s. 40 a 159–160; GEROSA, Libero: *Právo Cirkvi*. Prešov: Petra, 2005, s. 90–93 a MORIN, Dominique: *Učení II. vatikánskeho koncilu*. Praha: Paulínky, 1999, s. 24.

(princíp subsidiarity).⁴⁴ Z pohľadu obsahu platného Kódexu, sa do neho dostalo množstvo noriem spadajúcich do oblasti morálnej teológie. Z toho dôvodu v ňom možno nájsť viaceré normy bez sankcie, pričom zákonodarca nie raz neváha pristúpiť k pochvale ich adresátov a pod.⁴⁵ Za všetko napokon vypovedá i skutočnosť, že počas rekodifikačných prác sa musel najvyšší cirkevný zákonodarca obrátiť na členov komisie s pripomienkou, aby v prvom rade neopomenuli, že nový Kódex si má zachovať charakter právnického diela.

Záver

Ako bolo zrejmé z predchádzajúceho výkladu, dejiny prameňov práva Katolíckej cirkvi sa vyznačujú značnou zložitosťou a rôznorodosťou, pričom nachádzať spojivá medzi jednotlivými etapami tohto vývoja je častokrát až nemožné. Pramene práva totiž i v tomto právnom systéme vždy prirodzene reflektovali stav a potreby society, na úpravu spoločenských vzťahov ktorej boli stvorené. Práve spleť dejín Katolíckej cirkvi sa tak odzrkadľuje aj v spleti prameňov jej práva, za ktorými musíme vždy vidieť nielen ich prirodzený cieľ, za ktorým vznikli, ale taktiež ďalšie okolnosti. Ak by sme sa osobitne zamysleli nad autoritou zákonodarcu, je zrejmé, že obyčajové, respektíve silne decentralizované poňatie riadenia kresťanských spoločností v skutočnosti neskončilo za čias ranej Cirkvi, ale pokračovalo ďalej, pričom prvým, kto si uzurpoval právo autoritatívnych a vo viacerých ohľadoch i exkluzívnych zásahov do záležitosti jednotlivých partikulárnych cirkví boli predstavitelia východného a potom i západného césaropapizmu. Až v súvislosti s týmito procesmi boli rímski biskupi nútení chopiť sa realizovania svojich právomocí univerzálneho zákonodarcu a nahradiť element v cirkevnom živote krajne nežiaduci. Pokiaľ ide o fenomén kombinovania noriem morálky a práva, ten dominoval predovšetkým v prameňoch prvotnej Cirkvi, pričom ojedinelé návraty k nemu sa objavovali v cirkevných spoločenstvách nasledujúcich ideály raného kresťanstva, a to či už napríklad v podobe ranostredovekej írskej partikulárnej cirkvi alebo rôznych protestantských spoločností, ktoré nie raz dospeli až k radikálnemu záveru o celkovej potrebe odmietnutia práva v živote cirkvi.⁴⁶ Je vskutku zaujímavé, že tento prístup sa sčasti prejavil aj pri rekodifikačných prácach, ktorých výsledkom je platný Kódex kánonického práva z roku 1983. Práve uvedené skutočnosti nám ponúkajú

⁴⁴ Porov. FRANZEN, August: *Malé dejiny cirkve*. Kostelní Vydří: Karmelitánské nakladatelství, 2006, s. 312.

⁴⁵ Porov. napríklad cann. 129 § 2 a 1155 CIC 1983. Bližšie k tejto problematike pozri napríklad PŘIBYL, Stanislav: Biblické základy kánonického práva. In *Revue církevního práva*. Roč. 28 (2022), č. 2, s. 61n.

⁴⁶ Bližšie k tejto problematike pozri napríklad WIEL, Constant Van de: *History of Canon Law*. Louvain: Peeters Press, 1991, s. 54 a BUŠEK, Vratislav: *Učebnice dějin práva církevního I*. Praha: Všehrd, 1946, s. 185.

možnosť ich zváženia v kontexte ideí cyklenia dejín hlásanej niektorými filozofmi, ktorá predstavuje zaujímavý východiskový bod pre analýzu rôznorodých fenoménov vývoja ľudstva.⁴⁷ Prirodzenou otázkou, ktorá sa nám potom ponúka je, či možno na tieto procesy nahliadať optimisticky alebo skôr pesimisticky. Je teda celkový vývoj prameňov kánonického práva potrebné hodnotiť v kontexte nepoučenia sa z minulosti (v kontexte preferovania lineárnych perspektív) alebo je vhodnejšie hovoriť o prirodzenom návrate k pôvodným ideálom, na ktorých celé kresťanské spoločenstvo vzniklo?⁴⁸ Každopádne možno minimálne konštatovať, že právo dostávalo historicky prednosť pri presadzovaní centralizácie v Cirkvi, zatiaľ čo pri decentralizovanom fungovaní cirkevného spoločenstva sa poväčšine opomínalo na úkor morálnych východísk. Na druhej strane, nekritické presadzovanie druhého prístupu nie raz viedlo k potrebe návratu k právu.⁴⁹

Zoznam použitej literatúry

1. ALBERIGO, Giuseppe: *Stručné dějiny II. vatikánského koncilu*. Brno: Barrister & Principal, 2008.
2. BOTEK, Libor: Změny v trestním právu od vydání CIC/1983. In *Revue církevního práva*. Roč. 29 (2023), č. 3.
3. BRUNDAGE, James A.: *Medieval Canon Law*. London: Longman, 1995.
4. BUŠEK, Vratislav: *Učebnice dějin práva církevního I*. Praha: Všehrd, 1946.
5. ELIADE, Mircea: *Mýtus o věčném návratu*. Praha: Oikymen, 2009.
6. FILO, Vladimír: *Kánonické právo. Úvod a první kniha*. Bratislava: Rímskokatolícka bohoslovecká fakulta UK, 1997.
7. FRANZEN, August: *Malé dějiny církve*. Kostelní Vydří: Karmelitánské nakladatelství, 2006.
8. GAJDOŠ, Marcel: *Dokumenty prvních dvou ekumenických koncilů*. Prešov: Petra, 1999.
9. GEROSA, Libero: *Právo Církvi*. Prešov: Petra, 2005.
10. HRDINA, Antonín: *Kánonické právo*. Praha: Eurolex Bohemia, 2002.

⁴⁷ Bližšie k tejto problematike pozri napríklad ELIADE, Mircea: *Mýtus o věčném návratu*. Praha: Oikymen, 2009, s. 79n.

⁴⁸ Porov. MAREK, Jaroslav: *O historismu a dějepisectví*. Praha: Academia, 1992, s. 10 a 141.

⁴⁹ Dôkazom toho je napokon i nedávna rekodifikácia kódexových kánonov trestného práva sprísňujúca pôvodnú úpravu. Bližšie k tejto problematike pozri napríklad BOTEK, Libor: Změny v trestním právu od vydání CIC/1983. In *Revue církevního práva*. Roč. 29 (2023), č. 3, s. 49n; NAGY, Jakub: Změny ve zvláštní části VI. knihy CIC/1983. In *Revue církevního práva*. Roč. 31 (2025), č. 1, s. 9n a PÉTIOVÁ, Veronika: Prescrizione in caso di abusi sessuali di minori e adulti vulnerabili. In CITO, Davide – POZZO, Massimo del (ed.): *La giustizia penale nella chiesa: tutela della vittima e garanzie dell'imputato*. Roma: Pontificia Università della Santa Croce, 2025, s. 483–493.

11. KAŠNÝ, Jiří: Metoda v kanonickém právu. In *Revue církevního práva*. Roč. 13 (2007), č. 1.
12. KRAJČI, Jozef: *Historické pramene a všeobecné normy cirkevného práva*. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, 1997.
13. MAREK, Jaroslav: *O historismu a dějepisectví*. Praha: Academia, 1992.
14. MICHAL, Jaroslav: Dějiny pramenů poznání kanonického práva s přihlédnutím k dějinám práva římského. Praha: Ústřední církevní nakladatelství, 1967.
15. MICHAL, Jaroslav: Stručný přehled vývoje kanonického práva do r. 1917. In *Teologické studie. Litera slovem oživená. Sborník semináře v Hradci Králové r. 1984*. Praha: Česká katolická Charita, 1985.
16. MORDEL, Štefan: *Patrológia*. Spišská Kapitula – Spišské Podhradie: Nadácia Kňazského seminára biskupa Jána Vojtaššáka, 2004.
17. MORIN, Dominique: *Učení II. vatikánského koncilu*. Praha: Paulínky, 1999.
18. MRKÝVKA, Petr – VESELÁ, Renata: *Vybrané otázky z dějin kanonického práva*. Brno: Masarykova univerzita, 1992.
19. NACCI, Matteo: *Ius Proprium ac Nativum*: Brief Reflections on the Historical Evolution of the Sources of Canon Law. In *History Research*. Roč. 6 (2016), č. 2.
20. NAGY, Jakub: Změny ve zvláštní části VI. knihy CIC/1983. In *Revue církevního práva*. Roč. 31 (2025), č. 1.
21. NEMEC, Matúš: Štát, cirkev a právo v Rímskej ríši v prvých štyroch storočiach po Kristovi. Bratislava: Iura Edition, 2005.
22. PEJŠKA, Josef: *Církevní právo I. Ústavní právo církevní*. Semily: Nákladem vlastním, 1932.
23. PÉTIOVÁ, Veronika: Prescrizione in caso di abusi sessuali di minori e adulti vulnerabili. In CITO, Davide – POZZO, Massimo del (ed.): *La giustizia penale nella chiesa: tutela della vittima e garanzie dell'imputato*. Roma: Pontificia Università della Santa Croce, 2025.
24. POJAVNIK, Ivan: *Mysterium koncilu*. Olomouc: Matice cyrilometodějská, 1998.
25. PŘIBYL, Stanislav: Biblické základy kanonického práva. In *Revue církevního práva*. Roč. 28 (2022), č. 2.
26. RITTNER, Edward: *Církevní právo katolické*. Praha: Právnická jednota, 1887.
27. ŘÍČAN, Rudolf – MOLNÁR, Amedeo: *12 století církevních dějin*. Praha: Kalich, 1990.
28. SCHATZ, Klaus: *Dějiny papežského primátu*. Brno: Centrum pro studium demokracie a kultury, 2002.
29. SOMERVILLE, Robert – BRASINGTON, Bruce: *Prefaces to Canon Law Books in Latin Christianity*. London: Yale University Press, 1998.
30. TRETERA, Jiří R.: *Církevní právo*. Praha: Jan Krigl nakladatelství, 1993.
31. VETULANI, Adam: *Z badań nad prawem rzymskiem w dekrecie Gracjana*. Kraków: Drukarnia uniwersytetu jagiellońskiego, 1935.

32. VLADÁR, Vojtech: Kodifikácia práva východných katolíckych cirkví. In *Historia et theoria iuris*: printový a e-časopis pre mladých vedeckých pracovníkov právnických fakúlt na Slovensku. Roč. 2 (2010), č. 3.
33. VLADÁR, Vojtech: Význam štúdia prameňov kánonického práva pre súčasnú vedu. In *Revue církevního práva*. Roč. 29 (2023), č. 3.
34. VRANA, Vladimír: *Dejiny cirkevného práva*. Košice: Univerzita P. J. Šafárika, 1992.
35. WIEL, Constant Van de: *History of Canon Law*. Louvain: Peeters Press, 1991.

Kontaktné údaje

prof. doc. JUDr. Mgr. Vojtech Vladár, PhD.

vojtech.vladar@flaw.uniba.sk

Univerzita Komenského v Bratislave, Právnická fakulta, Ústav kánonického práva

JE GOLDPLATING ŠKODLIVÝ?

IS GOLD-PLATING DELETERIOUS?

Martin Šimkovič¹

Abstrakt: Európska legislatíva je často obviňovaná z vytvárania nepriaznivých účinkov, ktoré vplývajú na samotné ciele vnútorného trhu Európskej únie. Či už sa na to pozeráme akokoľvek, Komisia (EÚ) považuje takúto kritiku do značnej miery ako neopodstatnenú. Poukazuje na to, že sú to samotné členské štáty, ktoré najmä v prípade európskych smerníc sú zodpovedné za rozhodnutia o spôsobe ich prijímania a implementácie do vnútroštátnych právnych poriadkov. Ako vieme, európske právne akty obsahujúce minimálne požiadavky umožňujú členským štátom realizovať ich významnú právomoc pri implementácii právnych noriem a to hneď viacerými spôsobmi. V prípadoch, keď vnútroštátna implementácia európskych právnych predpisov prekročí požadovanú minimálnu úroveň vyžadovanú pri zachovaní legality, dochádza k neprimeranému spôsobu implementácie a teda ku goldplatingu, ktorý spôsobuje nežiadúce dodatočné náklady, administratívnu záťaž a s tým spojené ďalšie obmedzenia. A aj keď goldplating nie je nezákonný, zvyčajne sa prezentuje ako zlá prax ktorej sa dalo vyhnúť. Násť jasnú a jednotnú definíciu goldplatingu v dokumentoch či priamo v právnych predpisoch bolo ešte donedávna pomerene zložité, napriek tomu vnímanie tohto javu do istej miery zostáva nejednotné. Predmetom tohto článku je hľadanie odpovede na otázku, či je možné považovať goldplating skutočne len za negatívny jav ako sa to vo všeobecnosti predpokladá, alebo môžeme v súvislosti s týmto javom hovoriť aj o pozitívach.

Kľúčové slová: goldplating, implementácia, prameň práva, právny akt EÚ, nejednotnosť

Abstract: European legislation is often accused of creating adverse effects that affect the very objectives of the internal market of the European Union. No matter how we look at it, the Commission (EU) considers such criticism to be largely unfounded. It points out that it is the Member States themselves, particularly in the case of European directives, who are responsible for deciding how to adopt and implement the law. As we know, European legal acts

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav Európskeho práva

containing minimum requirements allow Member States to exercise their significant power to implement legal acts in a number of ways. In cases where the national implementation of European legislation exceeds the required minimum level required to maintain legality, there is an disproportionate method of implementation, i.e. gold-plating, which causes unwanted additional costs, administrative burdens and other restrictions associated with it. Nevertheless goldplating is not illegal, it is usually presented as a bad practice that could have been avoided. Although finding a clear and uniform definition of goldplating in documents or directly in legislation has been quite difficult until recently, the perception of this phenomenon remains somewhat inconsistent. The subject of this article is to find an answer to the question of whether gold-plating can really be considered only as a negative phenomenon as is generally assumed or whether we can also talk about positive aspects of this phenomenon.

Key words: goldplating, implementation, source of law, EU legal act, disunity

Úvod

Problematika goldplatingu a jeho konceptualizácia vychádza z nejednotného uplatňovania európskych právnych nástrojov, ktoré sú zhmotnené v rôznych prameňoch práva Európskej únie (EÚ) vo forme sekundárnych právnych aktov.² Príkladom takej nejednotnosti je využívanie právomocí členských štátov pridávať v rámci implementačného procesu osobitné procesné požiadavky nad rámec tých, ktoré sú navrhované alebo je to nastavenie prísnejšieho sankčného režimu než požaduje samotná európska norma (na čo sú ale veľa krát členské štáty aj oprávnené), čo v konečnom dôsledku však len prispieva k prehĺbovaniu nekonzistentnosti uplatňovania samotného aktu. Ani v prípadoch prijímania nariadení ako záväzných a priamo uplatniteľných nástrojov nie je situácia až taká jednoznačná. Nariadenia si totižto niekedy vyžadujú prijatie opatrení na ich primerané vykonávanie s ohľadom na špecifické okolnosti v právnych poriadkoch.³ A aj keď nariadenia musia byť implementované do národných právnych systémov krajín až pozoruhodne

² VOERMANS, Wim: Gold-Plating and Double Banking: An Overrated Problem? In: SNIJDER, Henk – VOGENAUER, Stefan: Content and Meaning of National Law in the Context of Transnational Law. Munich: Sellier European Law Publishers, 2021, s. 79-88. ISBN: 978-3-86653-127-7. V súvislosti s prameňmi práva EÚ pozri: FUNTA, Rastislav – JURIŠ, Filip – KLÍMEK, Libor: Európske právo. Bratislava: Wolters Kluwer, 3. doplnené a rozšírené vydanie, 2023, s. 174 a nasl. ISBN: 978-80-571-0662-3.

³ CRAIG, Paul - De BÚRCA, Gráinne: EU Law: Text, Cases and Materials. Oxford: Oxford University Press, 7th edition, 2020, s. 136 a nasl. ISBN 978-0-19-885664-1.

podobným spôsobom,⁴ z viacerých štúdií je zrejmé, že aj tento nástroj je podrobovaný neraz kritike, keďže vytvára neprimerané požiadavky na povinnosti a konkurenčné nevýhody.⁵ Neprehľadnosť prijímania právnych aktov ešte viac zvyrazňujú situácie, keď obmedzenia pri implementácii nie sú výsledkom ani tak prijatia nariadenia či iného právneho aktu, sú však vytvárané dodatočnými požiadavkami prijatými národnými vládami v rámci implementačného procesu a ktoré - aj keď presahujú rozsah pôvodného návrhu aktu - v konečnom dôsledku sú prijímané v rámci zákonnosti.

Uvedené názorné príklady a mohli by sme uviesť ďalšie, prispievajú k neprehľadnosti uplatňovania európskych právnych nástrojov a k vytváraniu nežiadúceho javu vo forme goldplatingu,⁶ na čo dokonca poukazujú pravidelne už aj správy samotnej Komisie (EÚ) či iné relevantné štúdie.⁷ Naposledy to bola Draghiho správa upozorňujúca, že neprimeraná regulačná záťaž a časté zmeny právnych predpisov EÚ vedú k tomu, že „...národné legislatívy často len prepisujú európske právne akty alebo implementujú zákony s odlišnými požiadavkami a normami postupne v jednej krajine a následne tak urobia v ďalšej krajine“.⁸

⁴ TICHÝ, Luboš a kolektív: Evropské právo. Praha: C.H. Beck, 5 prepracované vydanie, 2014, s. 202. ISBN: 978-80-7400-546-6.

⁵ DI FRANCO, Eleonora: Gold-plating: How EU States over-regulate themselves and then blame Brussels, 2018. Dostupné online: [Gold-plating: how EU States self-overregulate and then blame Brussels](#). Pozri aj: ATTHOFF, Karin – WALLGREN, Mia: Clarifying Gold-Plating: Better Implementation of EU Legislation. In: Board of Swedish Industry and Commerce for Better Regulation (NNR). Stockholm: Swedish Better Regulation Council (Regelrådet), Roč. 6, č. 1, 2012, s. 8 – 9 a s. 14. Dostupné online: https://nnr.se/wp-content/uploads/Clarifying_gold_plating_november_2012.pdf. Pozri tiež: JANS, H. Jan – SQUINTANI, Lorenzo - ARAGAO, Alexandra - MACRORY, Richard – WEGENER W. Bernhard: Gold Plating of European Environmental Measures? In: Journal for European Environmental and Planning Law. Cambridge University Press, Roč. 4, č. 2 (2009), s. 21. Doi: 10.2139/ssrn.1485386.

⁶Pojem „goldplating“ pochádza z právneho poriadku Spojeného kráľovstva (UK) a používa sa v zmysle vnútroštátneho práva, ktoré kladie na podniky záťaž, ktorú nevyžadujú právne predpisy EÚ. Prvá známa zmienka o tomto termíne pochádza z roku 2001 počas prejavu generálneho riaditeľa Konfederácie britského priemyslu s názvom „koniec „gold-platingu“. Pozri: SQUINTANI, Lorenzo: Goldplating: Beyond Minimum Harmonisation. Cambridge: Cambridge University Press, 2019, s. 13. ISBN: 9781108574532.

⁷ Napríklad analýza 13 právnych predpisov EÚ, ktorú vypracovala spoločnosť Business Europe, poukázala na duplicitu v 169 požiadavkách vrátane rozdielov (29 %) a úplných nekonzistentností (11 %). Pozri: The future of European competitiveness Part A | A Competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 69. Dostupné online: [97e481fd-2dc3-412d-be4c-f152a8232961_en](#).

⁸Pozri zverejnený dokument Komisie (EÚ): The future of European competitiveness Part A | A competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 70. ISBN 978-92-68-22716-9. Dostupné online: [97e481fd-2dc3-412d-be4c-f152a8232961_en](#)

K vymedzeniu goldplatingu a k jeho (ne)zákonnosti

Aj keď goldplating nie je nezákonný, zvyčajne sa prezentuje ako zlá prax spojená so zvyšovaním nákladov a s ďalšími nežiadúcimi účinkami, ktorým sa dalo vyhnúť.⁹ Nájsť jasnú a jednotnú definíciu goldplatingu v dokumentoch či priamo v právnych predpisoch bolo ešte donedávna pomerene zložité, ostáva však stále do značnej miery nejednotná. Vhodným spôsobom je tak jeho vymedzenie, ktoré je prakticky vždy spojené s tzv. superekvivalenciou, ktorá nastáva najmä v prípadoch, keď vnútroštátna implementácia smernice presahuje požadované minimum potrebné na jej dodržanie.¹⁰ Aj keď superekvivalencia je spájaná aj s prípadmi skoršej implementácie aktu zo strany členského štátu ako požaduje samotná európska norma, v tomto prípade si dovoľíme čiastočne polemizovať s týmto názorom.¹¹ Prikláňame sa k názoru, že v tomto prípade o goldplating nejde, nakoľko argumentovať len zvyšovanými nákladmi v súvislosti s implementáciou je nedostatočné a nenapĺňa ďalšie aspekty spojené s goldplatingom.

V súčasnosti za východiskový bod definovania goldplatingu považujeme definíciu Komisie (EÚ), ktorá tento pojem spája s procesom prijímania dodatočných požiadaviek nad rámec tých, ktoré boli vyžadované.¹² Nakoľko od konca roka 2022 v právnom poriadku Slovenskej republiky vznikla povinnosť pri predkladaní legislatívnych predpisov preberajúcich európske akty povinnosť identifikovať a vyhodnotiť goldplating, v zmysle novelizovaných Legislatívnych pravidiel vlády Slovenskej republiky a uvedenej metodiky môžeme goldplating definovať spôsobom, že vzniká v prípadoch pri navrhovaní prísnejšej právnej úpravy ako je

⁹ Ako už poznamenal taliansky Najvyšší súd v jednom zo svojich rozhodnutí, goldplating nie je zásadou práva EÚ, ktorá zaväzuje členské štáty k implementácii smerníc a zároveň im ponecháva slobodu vybrať si najvhodnejšie prostriedky na dosiahnutie zamýšľaného výsledku. Pozri: Rozhodnutie Najvyššieho súdu Talianskej republiky z 27. mája 2000 (Constitutional Italian Court, JUDGMENT NO. 100 of 2020).

¹⁰ EÚ poskytuje členským štátom určitú mieru voľnej úvahy v rámci zmlúv v rámci dodržiavania svojich princípov tvorby legislatívy bez ohľadu na to, že sa o tom stále akademicky diskutuje. Pozri viac: SQUINTANI, Lorenzo: Gold-plating: A misleading overarching concept. In: SQUINTANI, Lorenzo - RAKIPI, Jon: Beyond minimum harmonisation. Cambridge: Cambridge Studies in European Law and Policy, 2019, s. 13–71. ISBN: 9781108481007.

¹¹ MICKUTE, Karolina: How to identify and avoid gold-plating EU regulations. In: Center for Liberal Studies, 2021, s. 2- 6. Dostupné online: [How-to-identify-avoid-gold-plating.pdf](#) a tiež: TSIPOURI, Lena: Smart Governance of the internal market for business. In: Report to the European Economic and Social Committee, 2014, s. 20 až 24.

¹² Dokument Komisie (EÚ): The future of European competitiveness Part B | B Competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 320. ISBN 978-92-68-22715-2. Dostupné online: [ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en](#)

právna úprava v legislatíve EÚ alebo ak sa navrhuje vykonať transpozícia smernice EÚ nad rámec minimálnych požiadaviek EÚ.¹³

Dovoľme si ale poznamenať, že goldplating môžeme vymedziť aj negatívnym spôsobom.¹⁴ Aj napriek tomu, že v praxi je používanie tohto pojmu pomerne frekventované, treba povedať, že veľakrát ide aj o nepresné a neodborné pomenovanie, nakoľko pomenovať akýkoľvek jav vzdalujúci sa od obsahu európskeho právneho aktu automaticky za goldplating je veľmi povrchné. Príkladom je označovanie nesúladu textu smernice a príslušnej vnútroštátnej normy a to aj napriek tomu, že smernica obsahuje doložku zákazu zníženia úrovne ochrany. Aj keď nepochybne v praxi môžu nastať i ďalšie situácie, ktoré je možné označiť goldplatingom, jeho negatívne vymedzenie nám môže napomôcť, že nie všetko zaraďujeme pod tento pojem. Vhodný príklad predstavujú situácie nesprávneho vykonania, nevykonania či oneskorenia transpozície smernice, ktoré spúšťajú osobitný procesný postup konania o porušení predpisov, ktoré sú v tomto aspekte transpozície pozorne monitorované na úrovni EÚ. Nakoniec ani uplatňovanie vnútroštátnych technických noriem v oblastiach, ktoré nesúvisia s transpozíciou smernice môžu mať rovnaký účinok ako goldplating, v konečnom dôsledku ním ale nemusí byť. A mohli by sme pokračovať ďalej v uvádzaní nesprávneho označovania goldplatingu. Nakoniec, za goldplating nemôžeme označovať ani požiadavky európskych nariadení len preto, že vytvárajú neodôvodnenú byrokráciu a tým zvyšujú náklady napríklad pre podnikateľský sektor.¹⁵

K obmedzovaniu goldplatingu

Aj keď podľa aktuálnej správy Komisie (EÚ) sa Únia primárne zameriava na zabezpečenie správnej a včasnej transpozície smerníc, obavy z goldplatingu úplne nevymizli a to aj napriek tomu, že prijímané opatrenia zo strany Komisie (EÚ) sú

¹³ Článok III bod 4 Jednotnej metodiky pre posudzovanie vybraných vplyvov platnom znení z 1. októbra 2023 schválené uznesením Vlády SR č. 479/2023 zo dňa 27.9.2023.

¹⁴ V súčasnosti je výraz „goldplating“ definovaný EÚ v kontexte Agendy lepšej regulácie (*Better Regulation Agenda*), priamo ovplyvňovaná definíciami, ktoré predtým vytvorilo Spojené kráľovstvo a Holandsko počas obdobia rokov deregulácie. Pozri informácie, ktoré zverejňuje Komisia (EÚ) v súvislosti s agendou požiadaviek na lepšiu reguláciu: https://commission.europa.eu/law/law-making-process/better-regulation_en

¹⁵ V tomto prípade je ale potrebné poznamenať, že tento jav predstavuje problém minimálne pre zavedenú lepšiu správu EÚ (*better governance*), ktorá v súčasnosti podlieha nastavenému programu Komisie (EÚ) a nápravným opatreniam zo strany európskych inštitúcií, nie členských štátov. Program REFIT predstavuje program regulačnej vhodnosti a efektívnosti (*Regulatory Fitness and Performance Programme*), ktorého účelom je identifikácia možností zjednodušenia, vyhľadávania zbytočných regulačných nákladov a identifikácie oblastí na zlepšenie výkonnosti, ktoré tvoria neoddeliteľnú a stabilnú súčasť tvorby politik a programovania EÚ.

postupne zavádzané už od roku 2001.¹⁶ A keďže celkovo je goldplating vnímaný ako negatívny jav, EÚ naďalej spolu s členskými štátmi vyvíjajú viaceré procesy za účelom jeho znižovania.¹⁷ Dovoľujeme si však uviesť určité pochybnosti nad týmto prístupom, nakoľko zavádzané postupy odstraňovania či obmedzovania goldplatingu sa naďalej výrazne líšia na úrovni národnej či regionálnej správy členských štátov a kriticky vnímame aj skutočnosť, že nie všetky politiky EÚ majú nastavený mechanizmus jeho odstraňovania. Nakoniec najlepším dôkazom, že tento proces má stále veľkú časť cesty pred sebou je Draghiho správa, ktorá navrhuje možnosť pridať do článku o transpozícii smerníc novú štandardnú požiadavku, ktorá by od členských štátov vyžadovala systematické posudzovanie vplyvov svojich transpozičných opatrení s použitím rovnakej metodiky ako v prípade inštitúcií EÚ. Naviac, výsledky tohto posúdenia by mali byť zverejnené s cieľom zvýšenia transparentnosti.¹⁸

Okrem toho sa objavujú snahy o obmedzovanie goldplatingu zavádzaním *soft law* legislatívy, čo možno vnímať ako pozitívny spôsob riešenia uvedenej problematiky. Zavádzanie mäkkej legislatívy by do veľkej miery mohlo prispieť k usmerňovaniu domácich zákonodarcov pri predkladaní legislatívnej normotvorby najmä v prípadoch právnych aktov požadujúcich minimálnu úroveň harmonizácie. Akokoľvek, už len diskusiu na túto tému je potrebné vnímať pozitívne a preto v rámci diskusie si dovoľujeme navrhnúť, že uvedené odporúčania a usmernenia v rámci mäkkej legislatívy by mali sledovať princíp „dodržiavaj alebo vysvetli“, čo by viedlo k tomu, že zákonodarca musí vecne odôvodniť každý návrh či iniciatívu, ktorá ide nad rámec požiadaviek právneho aktu. Nakoniec aj väčšie zameranie na inštitucionalizáciu zmierňovania tohto javu by predstavoval prínos do diskusie pri riešení daného problému.

¹⁶ Zverejnený dokument Komisie (EÚ): European Commission (2025) Commission takes action to ensure complete and timely transposition of EU directives. European Commission, 2025. Dostupný online: [Commission takes action to ensure complete and timely transposition of EU directives](#).

¹⁷ Príkladom je jednotná metodika na posudzovanie vybraných vplyvov, ktorá bola schválená uznesením vlády SR č. 234/2021 v roku 2021. Aktualizáciou jednotnej metodiky boli v Slovenskej republike zavedené princípy *one-in-one out*, resp. *one-in-two-out* (1in1out, resp. 1in2out), princípy nazvané ako mechanizmus znižovania byrokracie a nákladov, ktorý predstavuje nástroj lepšej regulácie, ktorý je plnením záväzku predovšetkým z Komponentu č. 14 Plánu obnovy a odolnosti SR, pričom potreba jeho zavedenia bola identifikovaná v Stratégii lepšej regulácie - RIA 2020 a v Programovom vyhlásení vlády SR (2021 - 2024). Ďalej je to zavedenie princípu ochrany pred neopodstatneným goldplatingom, ktorý je jednou z úloh reformy s názvom „*Opatrenia na zníženie regulačného zaťaženia podnikania*“ Komponentu č. 14.

¹⁸The future of European competitiveness Part B | B Competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 324. ISBN 978-92-68-22715-2. Dostupné online: [ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en](#)

Bez ohľadu na uvedené snahy a prístupy, vo vedeckej literatúre nájdeme viacero názorov, podľa ktorých pojem goldplating je sporný vo vzťahu k jeho obmedzovaniu.¹⁹ Napríklad, keď sa pozrieme na štúdie zaoberajúce sa skúmaním do akej miery členské štáty využívajú svoje zákonné právo ísť nad rámec noriem EÚ zistíme, že aj keď toto právo teoreticky existuje, v praxi sa uplatňuje len zriedkavo.²⁰ A to sú pomerne prekvapujúce zistenia. V skutočnosti sa zdá, že mnohé členské štáty prijali všeobecnú zásadu akceptovania „žiadneho goldplatingu“ a tento poznatok je kľúčový, pretože ukazuje, že stratégie zmierňovania goldplatingu nie sú neutrálnymi administratívnymi nástrojmi, ale strategickými rozhodnutiami ovplyvnenými veľakrát „vnútroštátnym spoločenským dianím“ či akokoľvek to inak nazveme. Iní autori v súvislosti s goldplatingom a jeho obmedzovaním poukazujú, že praktická implementácia môže ísť nad rámec formálneho dodržiavania legislatívy. Podľa zistení z realizovaných štúdií, k prekračovaniu minimálnych zákonných požiadaviek dochádza aj z dôvodu, že národné štandardy boli nastavené už pred prijatím samotného európskeho aktu a tým dochádza k interpretácii normatívneho textu (zvlášť v prípade smerníc) rozsiahlejším spôsobom.²¹ Nedávno publikované zistenia skúmajúce goldplating cez optiku administratívnej diskrepancie a implementačných praktík preukázali, že implementácia právnych aktov je dokonca vo väčšine prípadov sprevádzaná domácimi inštitucionálnymi normami a preferenciami zainteresovaných strán.²² Podobne aj v iných štúdiách venujúcim sa implementácii právnych aktov v EÚ bolo preukázané, že faktory ako administratívna kapacita,

¹⁹ RADAELLI, Claudio: Europeanisation: Solution or problem? In: European Integration online Papers (EIoP), Roč. 8, č. 16 (2004), s. 56 až 76. Dostupné online: <https://ssrn.com/abstract=601163>. Pozri tiež: SQUINTANI, Lorenzo: Gold-plating: A misleading overarching concept. Cambridge: Cambridge University Press, 2019, s. 13–71. ISBN:9781108646055. Ďalej pozri: VOERMANS, Wim: Gold-Plating and Double Banking: An Overrated Problem? In: SNIJDER, Henk – VOGENAUER, Stefan: Content and Meaning of National Law in the Context of Transnational Law. Munich: Sellier European Law Publishers, 2021, s. 79–88. Dostupné online: <https://ssrn.com/abstract=1318236>.

²⁰ Príkladom je environmentálna oblasť. O týchto zisteniach pozri: JANS, H. Jan - SQUINTANI, Lorenzo – ARAGAO, Alexandra - MACRORY, Richard – WEGENER Bernhard: Gold-Plating of European Environmental Measures? In: Journal for European Environmental and Planning Law. Groningen: University of Groningen, Roč. 4, č. 2 (2009), s. 16. Doi: 10.2139/ssrn.1485386.

²¹ ZHELYAZKOVA, Asya – CANSARP, Kaya – REINI, Schrama: When Practice Goes beyond Legislators' Expectations: Analysis of Practical Implementation Exceeding Legal Compliance with EU Directives. In: Journal of Common Market Studies. Willey online library, Roč. 56, č. 3 (2018), s. 520–538. Doi: 10.1111/jcms.12637.

²² ZHELYAZKOVA, Asya – THOMANN, Eva: I did it my way: Customisation and Practical Compliance With EU Policies. In: Journal of European Public Policy. Willey online library, Roč. 29, č. 3 (2021), s. 427–447. Doi: 10.1080/13501763.2020.1859599.

politické zosúladienie a inštitucionálna koordinácia formujú spôsob, akým sa právne akty implementujú.²³

Vzorce nadmernej implementácie často viedli k inštitucionalizovaným stratégiám zmierňovania zameraným na to, aby sa v budúcnosti predišlo takýmto tendenciám. Z tohto pohľadu je nepochybne zaujímavým zistením ako uvádzajú niektorí autori, že samotné tvrdenia o goldplatingu nemajú empirické dôkazy o ekonomickej škode, čo znamená, že mnohé tvrdenia o goldplatingu pramenia z nedorozumenia,²⁴ čo posilňuje argument, že zmierňovanie goldplatingu je „potenciálne samoobmedzujúce“.²⁵

Goldplating nielen ako negatívny jav

Prirodzene sa vytvára priestor pre úvahy, či činnosti spájané s obmedzovaním goldplatingu a jeho striktným označovaním ako negatívnym javom sú jedinou správnou možnosťou. Avôbec, je nutné uvažovať o goldplatingu len ako o negatívnom jave? Vôbec nie. Dokonca sa prikláňame k názoru, že goldplating môže mať za istých okolností aj pozitívne účinky.

Goldplating ako pozitívny jav je možné vnímať v rámci určitej miery spochybnenia jeho negatívneho vnímania a teda v kontexte zavádzaných režimov či procesných požiadaviek, ktoré sú prijímané pri procese jeho zmierňovania. Rôzne stratégie zmierňovania goldplatingu totižto zabraňujú štátom vo využívaní „legitímnej“ slobody výslovne povolenej smernicami EÚ a to aj v prípadoch, že prijatie legislatívnych noriem môže slúžiť národným cieľom alebo politickým ambíciám. Voermans v tejto súvislosti konštatuje, že goldplating nie je vo svojej podstate

²³ MASTENBROEK, Ellen: Surviving the Deadline: The Transposition of EU Directives in the Netherlands. In: SAGE Publications, Roč. 4, č. 4 (2003), s. 371 – 395. Doi: 10.1177/146511650344001 a tiež: TOSHKOV, Dimiter: Public opinion and policy output in the European Union: A lost relationship. In: SAGE Publications, Roč. 12, č. 2 (2011), s. 169-191. Doi.org/10.1177/1465116510395 a tiež: FALKNER, Gerda - HARTLAPP, Miriam – TREIB, Oliver: Worlds of compliance: Why leading approaches to European Union implementation are only sometimes-true theories. In: European Journal of Political Research, Roč. 46, č. 4 (2009), s. 396-416. Doi: <https://doi.org/10.1111/j.1475-6765.2007.00703.x>.

²⁴ Na túto skutočnosť už poukazuje Schaefer s Youngom vo svojej štúdii poukazovaním na hlasovanie pri smerniciach, keď hlasovanie nastáva až potom, čo sa o nich hlasuje v jednom alebo viacerých členských štátoch. Pozri: SCHAEFER, Sarah - YOUNG, Edward: Burdened by Brussels or the UK? Improving the Implementation of EU Directives. London: A joint publication by the Foreign Policy Centre and the Federation of Small Businesses, 2006. S. 12 – 51. ISBN: 1-905833-04-0.

²⁵ JANS, H. Jan - SQUINTANI, Lorenzo – ARAGAO, Alexandra - MACRORY, Richard – WEGENER, Bernard: Gold-Plating of European Environmental Measures? In: Journal for European Environmental and Planning Law, Roč. 4, č. 2 (2009), s. 24. Doi: 10.2139/ssrn.1485386.

negatívny, v niektorých prípadoch je dokonca politicky alebo spoločensky žiaduci.²⁶ Násť ale správny pomer medzi goldplatingom a jeho zmiernením je mimoriadne zložitý, keďže zavedením prísnych obmedzení v procese transpozície môžu stratégie zmiernovania goldplatingu riskovať uzavretie legitímnych možností pre dosahovanie vyšších, napríklad environmentálnych, sociálnych alebo spotrebiteľských noriem, ktoré presahujú minimálne požiadavky EÚ. Navyše ako správne poznamenáva Jans, problémom je aj absencia samotného procesu vedúceho k väčšej transparentnosti a dostupnosti údajov o prípadoch, keď členské štáty oznámili Komisii (EÚ) goldplating alebo prijatie „ochranárskych“ národných noriem.²⁷

Goldplating ako pozitívny jav je možné vidieť aj z inej perspektívy. Zastávame názor, že za istých okolností je opodstatneným javom, čo najlepšie dokumentujú prípady vychádzajúce z praxe. V takých prípadoch môžeme hovoriť o opodstatnenom goldplatingu. Príkladom je oblasť pracovného práva a vzťah zamestnanec a zamestnávateľ, pri ktorom preukázaný goldplating v prípade rozšírenia výnimiek stanoveným európskym aktom môže mať v konečnom dôsledku pozitívny vplyv pre zamestnanca, zatiaľ čo pri zamestnávateľovi je to naopak. Samozrejme za istých okolností to môže platiť aj opačne. Uvedme ďalší príklad. V oblasti práva sociálneho zabezpečenia implementovanie pozitívnych sociálnych vplyvov vo verejnom záujme v konečnom dôsledku nemusí byť dôvodné, aby bolo označované ako goldplating, resp. aby zavedené normy boli následne odstránené.²⁸ Podobne aj v oblasti finančného práva, implementácia normatívnych pravidiel prejavujúca sa zavádzaním pravidiel nad rámec pôvodných požiadaviek môže mať v konečnom dôsledku pozitívny význam pre ochranu spotrebiteľa. Obdobne aj v ďalších prípadoch, zámerné rozhodnutie prekročiť požadované minimálne požiadavky môže mať pozitívny vplyv, tak ako to bolo v prípade transponovania smernice prania špinavých peňazí (AML).²⁹ Je však potrebné vnímať uvedený problém objektívne a preto je nutné poznamenať, že nastavenie „nadregulovaných“ pravidiel či požiadaviek v niektorých, najmä ekonomických oblastiach, môže mať negatívny vplyv na

²⁶ VOERMANS, Wim: Gold-Plating and Double Banking: An Overrated Problem? In: SNIJDER, Henk – VOGENAUER, Stefan: Content and Meaning of National Law in the Context of Transnational Law. Munich: Sellier European Law Publishers, 2021, s. 79-88. Dostupné online na: <https://ssrn.com/abstract=1318236>.

²⁷ JANS, H. Jan - SQUINTANI, Lorenzo – ARAGAO, Alexandra - MACRORY, Richard – WEGENER, Bernhard: Gold-Plating of European Environmental Measures? In: Journal for European Environmental and Planning Law, Roč. 4, č. 2 (2009), s. 32. Doi: 10.2139/ssrn.1485386.

²⁸ DZURJANÍKOVÁ, Zuzana: Goldplating. In: Zo súdnej praxe, Wolters Kluwer, Roč. 15, č. 6 (2023), s. 6 – 13.

²⁹ Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES.

ekonomickú slobodu podnikania, čo zase vplýva už na deformáciu trhu ako takého. Celkovo vzaté ale môžeme konštatovať, že v prípadoch opodstatneného goldplatingu, ktorý nesie v sebe určitú pridanú hodnotu a ktorú môžeme identifikovať ako realizáciu legitímneho verejného záujmu, ktorú si štát stanoví vo vybraných oblastiach ako napríklad v rámci ochrany vnútorného trhu, sociálnej ochrany alebo environmentálnych cieľov, goldplating môže za istých okolností mať pozitívny význam. V týchto prípadoch je však nevyhnutné a musí byť jasne zdôvodnené, že jeho pridaná hodnota alebo spoločenský význam prevyšujú náklady, ktoré sú s ním v danom prostredí spájané.

Záver

Považovať goldplating automaticky za negatívny jav nie je správne, na čo poukazujú nielen niektorí autori, ale aj auditné správy či výsledky realizovaných štúdií v členských štátoch, vrátane Slovenskej republiky.³⁰ Tie v rámci hodnotenia neopodstatnenosti goldplatingu ako negatívneho javu konštatujú potrebu, aby časť analyzovaných ustanovení legislatívnych noriem, ktoré idú nad rámec minimálnych požiadaviek práva EÚ boli označované vždy ako goldplating, ktorý je nevyhnutný odstraňovať z dôvodu neopodstatnenej záťaže. Zároveň bolo preukázané, že zdôvodnená pridaná hodnota existujúceho goldplatingu a teda požiadavku na sprísnenie legislatívy EÚ pri transpozícií do národnej legislatívy, nie je možné automaticky považovať za negatívum. Môžeme súhlasiť s tým, že goldplating nepredstavuje zásadu práva EÚ zaväzujúcu členské štáty k implementácii smerníc a ponechávaní si slobodne vybrať najvhodnejšie prostriedky na dosiahnutie zamýšľaného výsledku. Goldplating nemôžeme považovať ani za nezákonný či dokonca ani za akýsi prameň práva v meniacom sa legislatívnom prostredí práva EÚ. Napriek tomu, že sa prezentuje ako zlá prax spojená so zvyšovaním nákladov, nadbytočnou byrokraciou či s ďalšími nežiadúcimi účinkami, faktom ostáva, že goldplating nie je možné ani zovšeobecňovať. To znamená, že je dôležité, aby bol posudzovaný zakaždým individuálne od prípadu k prípadu, keďže za istých okolností predstavuje zdôvodnenú pridanú hodnotu. Platí to najmä v určitých právnych odvetviach, kde v rámci tvorby legislatívy môže pri sledovaní verejného záujmu mať pozitívne vplyvy, čo znamená, že v takých prípadoch nie je ani žiadúce aby bol odstraňovaný. Taktiež nie je prípustné, aby za goldplating bola považovaná akákoľvek legislatívna aktivita vzdiaľujúca sa od obsahu pôvodného právneho aktu. Vhodným príkladom je označovanie nesúladu textu smernice a príslušnej vnútroštátnej normy napriek tomu, že smernica obsahuje doložku zákazu zníženia úrovne ochrany.

³⁰Audit legislatívy z pohľadu goldplatingu predložený vláde Slovenskej republiky v rámci uznesenia vlády SR č. 32 z 2. januára 2018 (LP/2018/837).

Rozhodnutie európskych inštitúcií zmierňovať tvorbu goldplatingu či dokonca snaha o jeho úplné odstránenie často odráža hlbší ideologický postoj, ktorý uprednostňuje regulačný minimalizmus pred širšími sociálnymi alebo inými, napríklad environmentálnymi ambíciami. A aj keď dôvody vzniku goldplatingu sú rôzne a v súčasnosti môžeme konštatovať, že dochádza úspešne k jeho znižovaniu, naďalej absentuje väčšia inštitucionalizácia pri riešení tohto problému. Preto považujeme za vhodné, aby vývoj spojený s odstraňovaním tohto nežiadúceho javu pokračoval naďalej. Navrhované iniciatívy v podobe pridania nových požiadaviek do článkov v rámci transpozície smerníc vyžadujúce od členských štátov systematické posudzovanie vplyvov transpozičných opatrení s použitím rovnakej metodiky ako inštitúcie EÚ, považujeme za prínosné. Pozitívne vnímame aj snahu o zverejňovanie tohto procesu, čo by prispelo k reálnemu odstraňovaniu nežiadúcich účinkov pri prijímaní európskych aktov. Okrem toho, vhodný spôsob znižovania goldplatingu predstavuje prechod od smerníc o minimálnej harmonizácii k smerniciam či nariadeniam o úplnej harmonizácii. V konečnom dôsledku už len samotná širšia diskusia a výmena informácií o tejto problematike v podobe usmerňovania zákonodarcov zo strany európskych orgánov by určite prispela ku transparentnosti znižovania tohto javu tam, kde je nežiadúci.

Zoznam použitej literatúry

1. ATTHOFF, Karin – WALLGREN, Mia: Clarifying Gold-Plating: Better Implementation of EU Legislation. In: Board of Swedish Industry and Commerce for Better Regulation (NNR). Stockholm: Swedish Better Regulation Council, Roč. 6, č. 1, 2012, s. 8 - 14. Dostupné online na: https://nnr.se/wpcontent/uploads/Clarifying_gold_plating_november_2012.pdf.
2. CRAIG, Paul - De BÚRCA, Gráinne: EU Law: Text, Cases and Materials. Oxford: Oxford University Press, 7th edition, 2020. 1219 s. ISBN 978-0-19-885664-1.
3. DI FRANCO, Eleonora: Gold-plating: How EU States over-regulate themselves and then blame Brussels. 2018. Dostupné online: <https://mycountryeurope.com/politics/european-union/gold-plating-regulate-blame-brussels/>.
4. DZURJANÍKOVÁ, Zuzana: Goldplating. In: Zo súdnej praxe, Wolters Kluwer, Roč. 15, č. 6 (2023), s. 6 – 13.
5. FALKNER, Gerda - HARTLAPP, Miriam – TREIB, Oliver: Worlds of compliance: Why leading approaches to European Union implementation are only sometimes-true theories. In: European Journal of Political Research, Roč. 46, č. 4 (2009). s. 395 - 416. Doi: <https://doi.org/10.1111/j.1475-6765.2007.00703>.

6. FUNTA, Rastislav – JURIŠ, Filip – KLÍMEK, Libor: Európske právo. Bratislava: Wolters Kluwer, 3. doplnené a rozšírené vydanie, 2023. 512 s. ISBN: 978-80-571-0662-3.
7. JANS, H. Jan - SQUINTANI, Lorenzo – ARAGAO, Alexandra - MACRORY, Richard – WEGENER, Bernhard: Gold-Plating of European Environmental Measures? In: Journal for European Environmental and Planning Law, Roč. 8, č. 2 (2009). s. 23 – 36. Doi: 10.2139/ssrn.1485386.
8. MASTENBROEK, Ellen: Surviving the Deadline: The Transposition of EU Directives in the Netherlands. In: SAGE Publications, Roč. 4, č. 4 (2003), s. 371 – 395. Doi: 10.1177/146511650344001.
9. MICKUTE, Karolina: How to identify and avoid gold-plating EU regulations. In: Center for Liberal Studies, 2021. s. 2 - 6. Dostupné online: How-to-identify-avoid-gold-plating.pdf
10. RADAELLI, Claudio: Europeanisation: Solution or problem? In: European Integration online Papers (EIoP), Roč. 8, č. 16 (2004), s. 56 – 76. Dostupné online: <https://ssrn.com/abstract=601163>
11. SCHAEFER, Sarah - YOUNG, Edward: Burdened by Brussels or the UK? Improving the Implementation of EU Directives. London: A joint publication by the Foreign Policy Centre and the Federation of Small Businesses, 2006. S. 12 – 51. ISBN: 1-905833-04-0.
12. SQUINTANI, Lorenzo - RAKIPI, Jon: Beyond minimum harmonisation. Cambridge: Cambridge University Press, 2019. 341 s. ISBN: 9781108481007.
13. SQUINTANI, Lorenzo: Gold-plating: A misleading overarching concept: Beyond minimum harmonisation. Cambridge: Cambridge University Press, 2019. s. 13 – 71. ISBN: 9781108646055.
14. TICHÝ, Luboš a kolektív: Evropské právo. Praha: C. H. Beck, 5 prepracované vydanie, 2014. 756 s. ISBN: 978-80-7400-546-6.
15. TOSHKOV, Dimiter: Public opinion and policy output in the European Union: A lost relationship. In: SAGE Publications, Roč. 12, č. 2 (2011), s. 169-191. Doi:org/10.1177/1465116510395043.
16. VOERMANS, Wim: Gold-Plating and Double Banking: An Overrated Problem?, In: SNIJDER, Henk – VOGENAUER, Stefan: Content and Meaning of National Law in the Context of Transnational Law. Munich: Sellier European Law Publishers, 2021. 221 s. ISBN: 978-3-86653-127-7.
17. ZHELYAZKOVA, Asya – CANSARP, Kaya – REINI, Schrama: When Practice Goes beyond Legislators' Expectations: Analysis of Practical Implementation Exceeding Legal Compliance with EU Directives. In: Journal of Common Market Studies, Roč. 56, č. 3 (2018), s. 520-538. Doi: 10.1111/jcms.12637.

18. ZHELYAZKOVA, Asya – THOMANN, Eva: I did it my way: Customisation and Practical Compliance With EU Policies. In: Journal of European Public Policy, Roč. 29, č. 3 (2021), s. 427 - 447. Doi: 10.1080/13501763.2020.1859599.
19. Rozhodnutie Najvyššieho súdu Talianskej republiky z 27. mája 2020 (Supreme Italian Court, JUDGMENT NO. 100 of 2020).
20. The future of European competitiveness Part A | A Competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 70 ISBN 978-92-68-22716-9.
21. The future of European competitiveness Part B | B Competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union, 2025. S. 326. ISBN 978-92-68-22715-2.

Kontaktné údaje

JUDr. Martin Šimkovič

simkovic22@uniba.sk

Právnická fakulta UK v Bratislave, Ústav Európskeho práva

Sekcia cudzojazyčnej právnej komunikácie
Digitálne technológie a právna lingvistika:
implikácie pre výučbu právneho jazyka a výskum
právnej terminológie

VYUŽITIE DIGITÁLNYCH NÁSTROJOV PRI REŠERŠI CUDZOJAZYČNEJ PRÁVNEJ TERMINOLÓGIE. AKO MÔŽU POMÔČ PRÁVNE TEXTY

USING DIGITAL TOOLS TO RESEARCH FOREIGN-LANGUAGE LEGAL TERMINOLOGY. HOW LEGAL TEXTS CAN HELP

Jarmila Pátková¹

Abstrakt: V prostredí globálneho sveta sú právnici konfrontovaní s terminológiou cudzojazyčných právnych systémov, ktorá je osobitná pre každé odvetvie práva. Rešerš môže byť zameraná na vyhľadanie zoznamu termínov v konkrétnej oblasti alebo sa môže týkať vybraných termínov z titulu právno-komparatistického výskumu. Spoľahlivá rešerš termínov je podmienená výberom spoľahlivého a pojmovo reprezentatívneho textového korpusu, akým sú napríklad právne normy alebo súdne rozhodnutia. Spracovanie prirodzeného jazyka (*Natural Language Processing*) je odvetvím umelej inteligencie, ktoré učením sa prirodzenému jazyku dáva technológii schopnosť rozpoznávať, analyzovať, spracúvať a extrahovať z textov rozmanité dáta vrátane termínov. Cieľom tohto príspevku je priblížiť existujúce terminologické zdroje cudzojazyčných právnych pojmov, možnosti rešerše pomocou generatívnej umelej inteligencie a pomocou analytických nástrojov, akým je Sketch Engine, ktoré slúžia na jazykovú analýzu textových korpusov, terminologickú extrakciu, zobrazovanie vetného kontextu a poskytujú bibliografické referencie potrebných na objasňovanie významu termínov. Zároveň upozorňujeme na limity matematicko-štatistických výstupov, ktoré je potrebné korigovať aplikovaním odborno-jazykovej kompetencie a kvalitatívno-analytickými postupmi.

Kľúčové slová: termín, rešerš, extrakcia, kľúčové slovo, právne texty

Abstract: In today's globalized legal environment, practitioners frequently encounter terminology from foreign legal systems, each characterized by domain-specific language. Terminological research may target comprehensive term lists within a legal field or focus on selected terms for comparative legal analysis. The reliability of such research depends on the selection of a

¹ Právnická fakulta Univerzity Komenského v Bratislave, Ústav cudzojazyčnej právnej komunikácie

conceptually representative and authoritative text corpus, such as legal statutes or judicial decisions.

Natural Language Processing (NLP), a subfield of artificial intelligence, enables machines to learn and process human language, facilitating the extraction and analysis of legal terminology from textual data. This paper explores existing terminological resources for foreign-language legal terms and examines the potential of generative AI and corpus-based tools — particularly Sketch Engine — for linguistic analysis, term extraction, contextual visualization, and bibliographic referencing.

Furthermore, the paper addresses the limitations of statistical outputs generated by computational tools, emphasizing the need for expert linguistic competence and qualitative analytical methods to ensure accurate interpretation and validation of legal terms.

Key words: term, research, extraction, keyword, legal texts

Úvod

Tento článok je určený predovšetkým právnikom a študentom práva, ktorí prichádzajú do styku s cudzojazyčnými právnymi textmi. Rešeršná činnosť je vlastná všetkým intelektuálnym činnostiam. Je to schopnosť získavať a ďalej spracúvať informácie, schopnosť efektívne nadobúdať doplnkové jazykové a odborné znalosti, ktoré sú nevyhnutné na pochopenie textu.² Terminologická rešerš na účely vlastného právneho výskumu si vyžaduje jazykovú kompetenciu (znalosť jazyka), odbornú kompetenciu (právnická erudícia) i digitálnu gramotnosť. Pod rešeršou máme na mysli vyhľadávanie súboru termínov z istej tematickej oblasti alebo skúmanie konkrétneho termínu či termínov s cieľom pochopiť príslušný pojem patriaci do cudzej kultúry. V rámci právnej komparatistiky môže vzniknúť potreba excerpovať pre špecifickú oblasť práva zoznam pojmov, z ktorého by bolo možné získať predstavu o systéme právneho odvetvia, o previazanosti a význame týchto pojmov. Porozumenie si vyžaduje interpretáciu, ktorá sa odvíja od sémantickej roviny. Výklad cudzieho slova či výrazu ide ruka v ruku s prekladom. V takomto rámci je nevyhnutné termínom venovať pozornosť z hľadiska jazyka, nielen z hľadiska dát. Terminologická rešerš znamená tiež v úvodnej fáze odpovedať si na otázku, kde hľadať cudzie termíny a aké kritériá pritom držať na zreteli. S vedomím rizík, ktoré so sebou nesie nekritické spoliehanie sa na výsledky získané prostredníctvom plnoautomatizovaných digitálnych nástrojov vrátane tých, ktoré podporuje generatívna umelá inteligencia, je naším zámerom priblížiť možnosti skúmania

² ŠTEFKOVÁ, Marketa: Právny text v preklade. Translatologické aspekty právnej komunikácie v kombináciách málo rozšírených jazykov. Bratislava: Iura Edition, 2013, s. 127

odborných termínov pomocou dostupných zdrojov a digitálnych nástrojov opierajúc sa o poznatky lingvistiky a o znalosť typov právnych textov ako terminologického zdrojového materiálu.

V prvej časti článku špecifikujeme, čím sa vyznačujú právne termíny, následne uvádzame stručný prehľad možností terminologickej rešerše na účely štúdia cudzej právnej kultúry s využitím manuálnych, poloautomatických a plnoautomatických zdrojov a nástrojov. V poslednej časti ilustrujeme možné prínosy extrakcie termínov z korpusu francúzskych pracovnoprávných textov pomocou softvéru Sketch Engine v kombinácii s lingvistickou analýzou právnych termínov.

Termín a terminologické zdroje

„Termín je pomenovanie pojmu vymedzeného definíciou a miestom v systéme pojmov daného vedného odboru“.³ (Masár 1991, s. 19) Terminológia ako názvoslovie vedného odboru je výsledkom činnosti odborníkov, ktorí pojmy, s ktorými vo svojej špecializácii pracujú, pomenúvajú jednotne a konvenčne. Za vznikom termínov je teda potreba vedeckej obce alebo komunity odborníkov zabezpečiť bezproblémové dorozumievanie sa pomocou presných, systémových, významovo priezračných slov a slovných spojení viazaných na konkrétny odbor. Termíny sú usporiadané v systémovej štruktúre⁴ tak, aby boli zabezpečené vzťahy nadradenosti, podriadenosti, príbuznosti tak, aby termíny viažuce sa k jednému javu, boli zoskupené na tom istom mieste systému. V oblasti práva termíny označujú právne reality, právne úkony a výsledky úkonov, právny stav a deje smerujúce k vzniku, zániku, zmenám práv a povinností a podobne. Zákonodarca má za povinnosť zjednocovať názvy pojmov v podobe legálnych definícií, určujúcich obsah a rozsah pojmu. Cudzí termín je lexikálnym prvkom cudzieho jazyka, je utvorený podľa slovotvorných a gramatických pravidiel tohto jazyka, a označuje cudzí pojem, ktorý patrí do špecifickej oblasti práva. Právne termíny sú často viacslovné. Spojením viacerých lexém sa otvára možnosť spojiť viacero pre právo významných obsahov do jedného termínu (zložené právne výrazy).⁵ Najčastejšie vznikajú determinatívnou syntagmatickou väzbou, spojením podstatného mena s jeho prívlastkom. Vo francúzštine je prívlastkom prídavné meno alebo ďalšie podstatné meno spájajúce sa pomocou predložky. Ďalšou možnosťou tvorby pomenovaní je kompozícia, kedy sa spájajú dve slová (prevažne substantíva) pomocou spojovníka.

³ MASÁR, Ivan: Príručka slovenskej terminológie. Bratislava: VEDA, 1991, s. 19.

⁴ CABRÉ, María Teresa: La terminología. Teoría, metodología, aplicaciones. 1. edícia. Barcelona: Empúries, 1993, s. 170.

⁵ ABRAHÁMOVÁ, Eva: Základy právnej komunikácie. Šamorín: Heuréka, 2012. s. 40

Termíny používajú predovšetkým odborníci príslušného vedného odboru v komunikácii, ktorá sa týka predmetu ich špecializácie. Ako výsledky vedeckého poznania aj normalizované termíny sa sústreďujú v koncentrovanej podobe v špecializovaných informačných zdrojoch. Za všetky spomenieme odborné slovníky, terminologické databázy a odborné tezaury. Terminológie právnych odvetví sú zachytené vo výkladových **slovníkoch** právnych pojmov, ktorých prínosom je široký rozsah termínov celého odboru práva, prehľadné abecedné zobrazenie hesiel s uvedením lingvistickej informácie (slovnodruhovú kategóriu, pôvod slova/súčasti viacslovného pomenovania), výklad pojmu, prípadne príklady použitia termínu v textoch. Pri heslovom slove viažucom sa na viaceré pojmy (interná polysémia) sa vyznačujú jednotlivé oblasti (pododvetvie, subsystém) a príslušné významy. Slovníky sú výsledkom systematickej lexikografickej a terminografickej práce. Tieto reprezentatívne diela bývajú v papierovej podobe, v ktorej sú terminologické jednotky zachytené v podobe platnej k dobe edície. Odborné slovníky môžu byť tiež prekladové, dvoj i viacjazyčné. Uvádzajú iba prekladový ekvivalent, nie podrobný výklad pojmu. Terminologické glosáre sú slovníkmi malého rozsahu uvádzajúce prehľad pojmov z užšie vymedzenej odbornej oblasti.

Možnosť dynamickej aktualizácie a implementácie neologizmov dávajú **terminologické databázy**, prevažne pôsobiace v online priestore.⁶ Terminologická databáza je „súbor odborných terminológií uchovávaný v počítači, zahŕňajúci nomenklatúry, štandardizované termíny a lexikalizované syntagmy spolu s identifikačnou informáciou ich zdroja“. ⁷ Takou databázou je interaktívna databáza *IATE*, s ktorou pracujú inštitúcie a orgány EÚ a ktorá slúži na „zber, šírenie a manažment terminológie“⁸. Okrem normalizovaných termínov špecifikuje aj odporúčané, neodporúčané i zastarané termíny a odkazuje na textový zdroj termínu (z úradného vestníka Európskej únie), informuje o zdrojovej inštitúcii, okrem definície objasňuje obsah pojmu a pripája použitie termínu v kontexte. Každý termín je zaradený do špecifickej podoblasti (napr. Právo všeobecne – Sociálne veci – správne právo (politika)). Podrobná kategorizácia napomáha orientácii a výberu prekladového ekvivalentu cudzojazyčného termínu. V zhode s multilingválnou politikou Únie je možné vyhľadávať termíny v 24 jazykoch členských štátov a zároveň si z rovnakého počtu zvoliť cieľový jazyk. Databáza *IATE* obsahuje termíny práva EÚ, mnohé termíny národných právnych systémov v nej absentujú. Užitočným zdrojom právnych termínov sú kanadské terminologické databázy *TERMIUM Plus* a *Grand*

⁶ LEVICKÁ, Jana: Terminologické implikácie štruktúrnej a kontextovej analýzy francúzskej a slovenskej stavebnej lexiky, diz.p., Univerzita Komenského v BA, Filozofická fakulta, 2006, s. 51.

⁷ SAGER, Juan-Carlos: A Practical Course in Terminology Processing. Amsterdam-Philadelphia: John Benjamins, 1990, s. 169

⁸ <https://iate.europa.eu/about>

dictionnaire terminologique. Obsahujú heslá odkazujúce na konkrétne právne špecializácie spolu s definíciami.

Tezaurus (z lat. *thesaurus* poklad) je „riadený a štruktúrovaný slovník obsahujúci pojmy reprezentované termínmi s explicitne vyjadrenými vzájomnými vzťahmi“⁹, ktoré môžu byť vzťahmi hierarchickej nadradenosti a podriadenosti, ekvivalencie (synonymné a kvázi-synonymné) a asociácie. Cieľom takto nastavenej skladby hesiel je objasniť sémantický obsah pojmov a ich významové vzťahy, čo zodpovedá koncepcii Tezauru slovenského práva tak, ako ho nájdeme na portáli SLOV-Lex.¹⁰ Tezaurus slovenského práva SLOV-Lex uvádza k pojmom legálnu definíciu, doktrínalnu definíciu spolu s odkazom na zdroj, použitie v právnych predpisoch a judikátoch a tzv. previazané termíny.

Výhodou aktuálnych terminologických databáz a tezaurov je ich online dostupnosť, ergonómia užívateľského rozhrania, priebežné dopĺňanie a aktualizácia. Akokoľvek kvalitné sú tieto terminologické zdroje, nemôžu zachytávať všetky pojmy z právnych odvetví a špecifických tém národných právnych systémov.

Právne texty ako zdroje právnych termínov

Pri úvahách o vyhľadávaní termínov v rámci špecifickej právnej oblasti je vhodné položiť si otázku, kde sa príslušné termíny objavujú, v akých textoch. Je v tejto súvislosti typológia textov relevantná? Okrem toho uvedomujúc si aktuálne trendy rastúceho využívania umelej inteligencie na účely exploatácie dát nás zaujíma, či a aké kritériá uplatniť pri terminologickej rešerši vzhľadom na možnú chybovosť umelej inteligencie, ktorá si ešte stále vyžaduje dohľad človeka.¹¹ Na tomto mieste pokladáme za potrebné pripomenúť, že počítač vyťažujúci textové dáta z korpusov nemá lingvistickú predreceptnú prípravu (nevie urobiť lingvistickú analýzu textu), nerozlišuje v lexikálnej rovine termín od netermínu, substantívum osobitne využívané v odbornej problematike od substantíva všeobecného významu.

Právne termíny sú v prvom rade obsiahnuté v tematicky zodpovedajúcich právnych predpisoch, v ktorých obsah a rozsah pojmu je definovaný zákonodarcom. V tej istej formálnej jazykovej podobe sa jednotne ďalej používajú v odborných textoch príslušného právneho odvetvia. Ide o texty právnej vedy a texty aplikácie práva, kam patria súdne rozhodnutia, rozhodnutia orgánov štátnej a verejnej správy, zmluvy, dohody a mnohé iné textové dokumenty. Jazykovedci prítomnosť slova (i slovných

⁹ ŠPÁNIOVÁ, Marta: Význam terminológie pre informačnú činnosť: Terminologické princípy tvorby tezaurov a interoperabilita s inými slovníkmi. In: Zborník Filozofickej fakulty Univerzity Komenského, Knižničná a informačná veda XXVI (2016), s. 45-68.

¹⁰ <https://www.slov-lex.sk/tezaury/terminy>

¹¹ CLÉMENT-WILZ, Laure et al.: Translation in the European Union: Navigating Technical and Legal Issues in the Light of Artificial Intelligence - Conclusions. In: International Journal of Language and Law, Vol. 14 (2025), Special Issue: Artificial Intelligence and the Language of Law, s. 240.

spojení) v texte nazývajú distribúcia. Podľa Zipfovho zákona¹² majú najvyššiu distribúciu v texte (akomkoľvek) najbežnejšie slová, z ktorých sú tvorené vety, nasledujú ostatné slová, ktorých frekvencia závisí predovšetkým od témy (oblasti). Slová svoj význam nadobúdajú v súvislostiach a tie vyplývajú z kontextu, čo platí ešte väčšmi pre právo, ktoré svoje odborné pomenovania čerpá zo všeobecnej slovnej zásoby. Tie isté slová všeobecného jazyka nadobúdajú v právnom kontexte špecifický význam a stávajú sa termínmi. Ak chce právny interpret porozumieť významu cudzieho pojmu, mal by zohľadniť nielen najbližšie jazykové okolie slova/výrazu (cca 5 slov pred a za slovom/výrazom), ale zamerať sa i na vzdialenejšie okolie (kontext), ktorým je paragraf zákona, sudcovské objasnenie aplikácie právnej normy v rozhodnutí súdu, doktrínálna definícia či právny komentár.¹³ Zákony, súdne rozhodnutia, texty právnej vedy tak poskytujú prirodzený odborný kontext termínu, ktorý vrhá svetlo na obsah a rozsah pojmu, a sú zároveň spoľahlivým materiálom na terminologickú rešerš. Texty práva sú čiastočne verejne dostupné (právne normy, súdne rozhodnutia), čiastočne sú neverejné (zmluvy, dohody). Dostupnosť textov je dôležitým faktorom pri zostavovaní textových korpusov.

Korpus je tematicky zameraná zbierka textov vytvorená na účely lingvistického bádania podľa princípov dokumentárnosti a úplnosti.¹⁴ V prípade právneho jazyka môže byť textový korpus dostatočne reprezentatívny i pri menšom rozsahu, a to z dôvodu konzervatívnosti právneho jazyka, ktorá sa prejavuje schematickými koreláciami medzi formou a funkciou jazykových prvkov.¹⁵

Prirodzený jazyk a jeho počítačové spracovanie

Analýza veľkých textových korpusov pomocou počítačových programov sa používa na extrakciu rozmanitých dát (Text Mining Tools),¹⁶ informácií, slov, názvov, obrázkov, typov dokumentov a pod. Jazykové jednotky vrátane termínov v textoch identifikujú nástroje na spracovávanie prirodzeného jazyka NLP (Natural Language Processing). NLP ako odvetvie umelej inteligencie využíva poznatky lingvistiky na analýzu textu, frekventovaných slov a slovných spojení, obvyklých a charakteristických výrazov, kombinácií slov. Aktuálne softvéry pracujúce na báze NLP narábajú s významom a kontextom slov tak, že stanovujú vektorové

¹² MISTRÍK, Jozef: Lingvistický slovník. Bratislava: SPN, 2002, heslo *Zipfov zákon*

¹³ CVRČEK, František: Právní informatika a lingvistika. In: *Jurisprudence*, Roč. 2, č. 6 (2016), s. 50-51

¹⁴ Slovník francúzskeho jazyka francúzskeho CNRS *Trésor de la langue Française informatisé (TLFi)*, heslo *corpus A Ling (prekl. JP)*.

¹⁵ BHATIA, Vijay – LANGTON, Nicola N. – LUNG, Jane: Legal discourse: Opportunities and threats for corpus linguistics. In: *Discourse in the Professions. Perspectives from corpus linguistics*. Amsterdam: John Benjamins, 2004, s. 207

¹⁶ TALIB, Ramzan et al.: Text Mining: Techniques, Applications and Issues. In: *International Journal of Advanced Computer Science and Applications (IJACSA)*, Roč. 7, č.11 (2016), s. 414.

reprezentácie slov, tzv. *embeddings*.¹⁷ Znamená to zachytenie slova v jeho najbližšom uzuálnom kontexte, teda v tom, do čoho býva „ponorené“. To je dôležité pri rozlišovaní významu slova, ktorý je determinovaný kontextom, čiže slovami, s ktorými sa bežne spája. Aj v prípade slov, ktoré vstupujú do mnohých rozmanitých kontextov, počítač tieto spojenia načíta okamžite a „naučí sa ich“. V lingvistike sa štúdiu spojení slov – kolokácií - venuje významná pozornosť. Využitie strojov v lingvistike sa v priebehu vývoja profilovalo smerom k automatickému učeniu sa stroja jazyku v podobe, v akej sa reálne používa (jazykový úzus/jazykové úzy). Výsledok počítačom automatizovanej analýzy, a teda aj extrahovaná terminológia, závisí od toho, aké textové korpusy sa použijú. Aktuálne veľké jazykové modely (LLM) fungujúce vďaka neurónovým sieťam a využívajúce rozsiahle dáta prístupné na webe, ktoré ľudský výskumník nedokáže v podobnom objeme a podobnou rýchlosťou spracovať, sa „učia“ ľudskému jazyku a vďaka tomu dokážu dáta analyzovať a interpretovať. Automatické rozpoznávanie termínov (ATR) a automatická extrakcia termínov (ATE) sú špecializácie, ktorým sa venujú vývojári softvéru určeného pre všetkých, ktorí potrebujú vyhľadávať, získavať a systematicky spracovať terminológiu nielen v akademickej sfére.¹⁸ Je nepochybné, že v tomto smere technológia ustavične napreduje k cieľu, ktorým je uspokojenie dopytu po informáciách.

Virtuálni asistenti generatívnej umelej inteligencie

Automatická extrakcia termínov patriacich ku konkrétnemu odvetviu práva v cudzom jazyku je úlohou, ktorú virtuálni asistenti generatívnej umelej inteligencie (genAI), ako ChatGPT, OpenAI, Gemini, Claude, dokážu vo veľmi krátkom čase (v sekundách) splniť vygenerovaním zoznamu vďaka informáciám z verejne dostupných právnych portálov krajiny alebo krajín hovoriacich týmto jazykom. Terminológiu získavajú tak, že prehľadávajú príslušné právne predpisy, tematicky ohraničené judikáty, texty právnej vedy, informácie zverejnené štátnymi inštitúciami v príslušnom rezorte. Iným zadaním rešerše môže byť objasniť význam konkrétneho termínu. Asistentovi GenAI poskytneme informácie o odvetví práva, o konkrétnej podobe či kontexte. Uspokojivosť odpovede závisí predovšetkým od primeranosti špecifikácie zadania v konverzácii (tzv. prompt) a od zdroja/ov informácií, ktorý/é virtuálny asistent preskúma.

¹⁷ XU, Kang - FENG, Yifan – LI, Quiandi et al.: Survey on terminology extraction from texts. In: Journal of Big Data, roč. 12, č. 29 (2025), s. 16-17

¹⁸ WISSIK, Tanja: Impact of automatic term extraction on terminology work. A qualitative interview study in institutional. In: Terminology, International Journal of Theoretical and Applied Issues in Specialized Communication, roč. 31, č. 1 (2025), s. 110.

Na tomto mieste uvedieme príklad terminologickej rešerše v komunikácii s chatbotom Copilot, ktorého sme sa opýtali na význam francúzskeho jednoslovného termínu *astreinte* s upresnením oblasti pracovné právo. Chatbot vypísal význam „pokuta, penále“, ale opomenul význam „pracovná pohotovosť“, ktorý má v pracovnom práve dôležité miesto. Ide o prípad internej synonymie, kedy sa význam právneho termínu mení v závislosti od právnych odvetví a predovšetkým v závislosti od bezprostredného vetného kontextu, tzv. *co-textu*¹⁹. Je nesporné, že efektívnosť rešerše závisí od verzie konkrétneho chatbotu.

Vzhľadom na to, že aktuálne nie je možné zabezpečiť stopercentnú bezchybnosť plnoautomaticky generovanej rešerše asistentmi genAI, používatelia vyžadujúci spoľahlivosť sa pravdepodobne aj naďalej budú obracať na terminologické zdroje a na poloautomatické riešenia. Navyše právo je špecifické tým, že niektoré témy nemusia byť zachytené vo verejne prístupných textových korpusoch, napríklad také, o ktorých hovoria súkromnoprávne dokumenty.²⁰ V takom prípade bude potrebné manuálne spracovať špeciálny textový korpus pre následnú analýzu.

Automatická extrakcia termínov

Na rešeršu a extrakciu terminológie boli vyvinuté digitálne nástroje, ktoré spracúvajú vložené textové korpusy, napríklad TermSuite, TermoStat, TerMine, Sketch Engine.²¹ Tieto nástroje sú ponúkané tiež v ekonomickej sfére spoločnostiam, ktoré si zabezpečujú terminologický manažment. Extrakcia termínov pomocou ATE softvérov je proces, ktorý je sčasti manuálny, pretože korpus na analýzu a extrakciu termínov volí a do softvéru nahráva človek – zadávateľ rešerše. Korpusom môže byť tematicky príslušná právna norma. V takom prípade po nahratí textového súboru softvér pripraví texty na analýzu, o čom si povieme nižšie. Korpus si však môžeme zostaviť z vlastného výberu textov. Reprezentatívnosť korpusu závisí od správnej voľby textov tak, aby pokrývali tematickú oblasť výskumu. Napríklad pojmy špecifickejšie späté s výkonom a odmeňovaním práce v pracovnom práve sú zastúpené v kolektívnych zmluvách, v pracovných zmluvách a v odborných textoch tematicky súvisiacich s upravením práv zamestnancov. Výhodou odbornej kompetencie právnikov je, že sa vedia orientovať medzi právne relevantnými textami.

¹⁹ CVRČEK, Václav: Kvantitativní analýza kontextu. Praha: Lidové noviny, Ústav Českého národního korpusu, 2013, s. 23

²⁰ BIEL, Łucja. Corpus-Based Studies of Legal Language for Translation Purposes: Methodological and Practical Potential. In: *Reconceptualizing LSP*. Online proceedings of the XVII European LSP Symposium 2009. Aarhus, 2010. s.4

²¹ WISSIK, Tanja: Impact of automatic term extraction on terminology work. A qualitative interview study in institutional. In: *Terminology, International Journal of Theoretical and Applied Issues in Specialized Communication*, roč. 31, č. 1 (2025), s. 112-113.

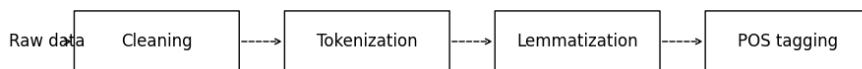
Podľa zvoleného metodologického prístupu k princípom činnosti delíme ATE nástroje do troch skupín, ktoré sa opierajú o:

1. Lingvistický prístup
2. Štatistický prístup
3. Hybridný prístup²²

Systémy využívajúce lingvistické princípy vychádzajú z gramatických pravidiel, syntagmatických konštrukcií a zo slovnej zásoby daného jazyka. Nástroje nastavujú odborníci podľa morfosyntaktických a sémantických vlastností termínov. Štatisticky orientované systémy vychádzajú z údajov o frekvencii a spoločnom výskyte (kookurencii) skúmaných prvkov (slov alebo kombinácií slov). Hybridné systémy kombinujú lingvistické postupy a štatistické postupy na zvýšenie presnosti extrakcie termínov.

Korpusová analýza, ktorej výsledkom bude extrakcia termínov, nasleduje po informaticko-lingvistickej príprave textového korpusu, ktorú automaticky vykoná softvér, a to v nasledovných etapách:

1. **Vyčistenie** textu od nepotrebných prvkov pre jazykovú analýzu (čísla, symboly, odrážky,...)
2. **Tokenizácia**, rozdelenie textu na tokeny (základné jednotky, ktorými sú zväčša jednotlivé slová, ale i čísla, alfanumerické reťazce začínajúce číslicou, interpunkčné znamienka, skratky a označenia, ktoré počítač objaví medzi dvomi medzerami textu)
3. **Lemmatizácia**, priradenie lemmy (základného tvaru) ku každému tvaru slova v korpuse
4. **POS tagovanie**, t.zn. opatrenie tokenov značkou podľa slovného druhu spolu s morfológickou a gramatickou informáciou²³



Obr. 1: Postupnosť krokov prípravy korpusu pred analýzou

Extrakcia termínov v nástroji Sketch Engine – výstupy a použitie

V tejto časti by sme chceli stručne predstaviť online nástroj Sketch Engine, ktorý sa od svojho vzniku v r. 2004 masívne používa aj v lexikografii.²⁴ (Kilgarriff 2014, s. 1)

²² XU, Kang - FENG, Yifan – LI, Quiandi et al.: Survey on terminology extraction from texts. In: Journal of Big Data, roč. 12, č. 29 (2025), s. 2

²³ Glosár Sketch Engine, heslá *token*, *lemmatization*, *POS tagger*.

²⁴ KILGARRIFF, Adam et al. The Sketch Engine : Ten years on. In: Lexicography, roč. 1, č. 1 (2014), s. 7

Umožňuje nahráť vlastné textové súbory, ktorými môžu byť napríklad vybrané právne predpisy alebo texty súdnych rozhodnutí týkajúce sa konkrétnej témy. Sketch Engine skompiluje texty a pripraví ich na analýzu. Na základe vykonanej analýzy generuje výstupy slúžiace na skúmanie rôznych vlastností a jazykových prvkov korpusových textov. Na účely terminologickej rešerše môžeme nechať vytvoriť zoznam termínov alebo môžeme skúmať konkrétne termíny v texte s cieľom pochopiť ich význam, jednotlivé sémantické obsahy, nájsť v zobrazenom širšom kontexte prípadné definície termínu alebo asociované pojmy. Termíny pomenúvajúce súvisiace alebo príbuzné pojmy si môžeme zaznačiť v podobe stromu, ktorý je súčasťou pojmovej sústavy právneho odvetvia.

Na extrakciu termínov slúži funkcia *Keywords*, ktorá generuje zoznam kľúčových slov v jednoslovnej a viacslovnej forme. Poradie termínov vo výstupe závisí od tzv. relatívnej početnosti, ktorá je stanovená porovnaním početnosti (frekvencie) termínu v cieľovom korpuse s jeho frekvenciou v komparatívnom (referenčnom) korpuse.²⁵ Týmto referenčným korpusom je korpus všeobecného jazyka. Majúc na zreteli, že právne výrazy bývajú zložené (pozri časť Termín), termíny nájdeme predovšetkým vo viacslovnom výstupe *Keywords multiword*. Kľúčové slovo je podstatným menom, ktoré je ďalej rozvíjané vo viacslovnom pomenovaní. Mnohé právne termíny sú vytvorené z toho istého kľúčového slova (napr. *contrat*, zmluva). Výstup zobrazuje všetky viacslovné kombinácie kľúčového slova v samostatných riadkoch, čo môže poslúžiť ako základ pre zostavenie poľa asociovaných termínov: Príklad termínov tvorených s kľúčovým slovom *contrat* v podobe, v akej sa objavujú vo výstupe *Keywords*²⁶:

1. *Contrat de travail* (pracovný pomer)
2. *Contrat de travail à durée déterminée* (pracovný pomer na dobu určitú)
3. *Contrat de mission* (zmluva o dočasnom pridelení uzatváraná so zamestnancom)
4. *Contrat de professionnalisation* (zmluva na dobu získania odbornej kvalifikácie)
5. *Contrat de mise à disposition* (zmluva o dočasnom pridelení uzatváraná s užívateľským zamestnávateľom)
6. *Contrat initiative-emploi* (zmluva na podporu zamestnávania)

Zoznam viacslovných pomenovaní, ktoré označujú právne pojmy a sú tvorené pomocou toho istého kľúčového slova, predstavuje súbor príbuzných pojmov, ktoré

²⁵ Glosár Sketch Engine, heslo *frequency* (*frequency per million*)

²⁶ PÁTKOVÁ, Jarmila: Korpusová analýza pracovnoprávných textov v jazykovej kombinácii francúzština-slovenčina so zameraním na ustálené slovné spojenia a terminológiu, diz. p. Univerzita Komenského v BA, Filozofická fakulta, 2025, s. 56.

je možné usporiadať do hierarchickej štruktúry pojmov skúmaného odvetvia. Takáto štruktúra by mohla odrážať vzťahy:

1. nadradenosti a podriadenosti:

contrat de travail (zastrešujúci pojem) a

contrat de travail à durée déterminée (podriadený pojem)

2. rovnocennosti:

contrat de professionnalisation a

contrat initiative-emploi (dva typy špeciálnych zmlúv sledujúcich osobitné ciele

3. komplementárnosti:

contrat de mission (právny úkon vykonaný s jednou stranou (agentúrnym zamestnancom) trojstranného vzťahu) a

contrat de mise à disposition (právny úkon vykonaný s druhou stranou trojstranného vzťahu, s užívateľským zamestnávateľom)

Diferenciáciu pojmov zo zoznamu uľahčuje znalosť cudzieho jazyka. Rozvíjajúci člen viacslovného pomenovania *à durée déterminée* (na dobu určitú) zužuje rozsah nadradeného pojmu a naznačuje, že ide o hyponymický prvok triedy *contrat de travail* (pracovný pomer formalizovaný pracovnou zmluvou). Pri ostatných termínoch so slovom *contrat* z nášho príkladu prívlastky kľúčového slova určujú význam toho-ktorého pojmu tak, že pripájajú ďalšiu sémantickú zložku termínu. Tou je iný významný pojem pracovného práva (napr. *mise à disposition*, dočasné pridelenie).

Určujúce prvky viacslovného termínu, ktoré Sketch Engine nazýva modifikátory, tento nástroj vizualizuje pomocou funkcie *Word Sketch*. Po zadaní kľúčového slova termínu získame prehľad slov, s ktorými sa viaže v kolokáciách a v poradí, ktoré zodpovedá frekvencii spojení. *Word Sketch* zobrazuje tabuľkový prehľad štatisticky najvýznamnejších kolokácií slova (t.j. obvyklé a významovo kompatibilné spojenia slov) podľa jednotlivých gramaticko-syntaktických väzieb, do ktorých slovo vstupuje, akými sú väzba s priamym a nepriamym predmetom, s prívlastkom (modifikátorom resp. determinantom), predikatívna väzba (spojenie so slovesom), väzba s predložkou pred i za slovom. Ak do vyhľadávania zadáme jednoslovný termín (napr. *entrepreneur*, podnikateľ), nástroj nám v tejto funkcii nájde medzi najčastejšími kolokátmi slovo *salarié* (poberajúci mzdu). *Entrepreneur salarié* je pojem neznámy v slovenskom systéme pracovného práva, toto dvojslovné pomenovanie znamená „samostatne zárobkovo činný člen družstva²⁷“. *Word Sketch* dokáže odhaliť aj málo frekventované zložené termíny.

Funkcia *Concordance* (konkordancia) vizualizuje hľadané slovo/viacslovné pomenovanie vo vetnom kontexte a je cenná pri overovaní formálneho ohraničenia viacslovného termínu, ako aj absolútnej početnosti výskytu v korpuse. Zobrazuje

²⁷ Tento typ družstva má vo Francúzsku skratku CAE (Coopérative d'activité et d'emploi).

vetný kontext (co-text) a po rozkliknutí konkrétneho výskytu aj širší kontext, ktorým môže byť segment legislatívneho textu, ktorý vysvetľuje pojem. Ak rešeršujeme vo verejne dostupnom korpuse (napr. korpusy európskeho práva), konkordancia uvádza informáciu o zdrojovom dokumente. V tejto funkcii sa po zadaní slova zobrazia všetky výskyty slova v korpuse v rôznych tvaroch (vďaka lemmatizácii), a tak prezeraním konkordancie môžeme objaviť nové termíny, napríklad *contrat de mission à l'exportation* (zmluva o vyslaní do zahraničia), ku ktorému nás privedie konkordančné zobrazenie termínu *contrat de mission* (pozri tu vyššie). Z prekladu vyplýva, že ide o odlišné zmluvy. V podobných prípadoch k objasneniu významu oboch termínov prispieva poznanie cudzieho jazyka a cudzej kultúry.

Vo francúzskom právnom jazyku termíny najčastejšie vznikajú nominalizáciou (slovnodruhovú transformáciu, ktorej výsledkom je podstatné meno): napr. *dédit* (nedodržanie zmluvy - termín) utvorené od slovesa *dédire* (odvolať). Po zadaní slovesného tvaru konkordancia zobrazí podstatné meno. Uvedený príklad odhaľuje, ako jazyková kompetencia, teda poznanie významu slovesa ozrejmuje to, čo terminológovia nazývajú motiváciou, čiže súvislosť medzi podobou designátora (slova) a právnym pojmom, ktorá stála za zrodom termínu (motivovala ho). Z nášho pohľadu je takéto lingvistické skúmanie cudzieho termínu prínosné i pre právne analýzy.

Nástroj Sketch Engine ponúka aj ďalšie funkcie na podrobnejšiu lingvistickú analýzu, ktorú je možné zamerať na slovnú zásobu vo všeobecnosti, gramatické tvary, syntaktické konštrukcie, štylistické prvky.

Záver

Rešerš termínov na účely právneho výskumu môže byť manuálna, poloautomatická i plnoautomatická. Osvedčené terminologické zdroje, ako slovníky, terminologické databázy, glosáre a tezaury, sú plodom práce terminografov a lexikografov. Ich výhodou je robustnosť a dôslednosť terminologickej práce. Virtuálni asistenti generatívnej umelej inteligencie (genAI) nie sú nastavení na vykonanie právno-komparatistického zadania, v rámci ktorého by plnohodnotne porovnali podobné pojmy patriace do odlišných právnych kultúr. Právna komparácia zohľadňuje nielen právny systém, ale i právnú kultúru, ktorá pojmom vtlačá významové nuansy. Odborník v oblasti práva tieto nuansy vníma okrem iného ako súčasť svojej vedomostnej a skúsenostnej výbavy. Pri plnoautomatickej rešerši termínov s podporou genAI závisí od expertne zadefinovaných zadaní zo strany človeka, či digitálny asistent poskytne uspokojivú odpoveď. Nástroje na automatickú extrakciu termínov (ATE) kombinujú princípy korpusovej lingvistiky s frekvenčno-štatistickými metódami. Jazyková kompetencia a lingvistické nazeranie na skúmaný termín otvárajú možnosti hlbšieho porozumenia obsahu a rozsahu pojmu, ktorý je

termínom označovaný. Tento aspekt môžu oceniť právni interpreti, ktorých zaujímajú sémantické znaky pomenovania právneho pojmu, vďaka ktorým je možné prehĺbiť poznanie nielen pojmu, ale i jeho miesta v cudzom právnom systéme.

Dôležitým faktorom ovplyvňujúcim relevantnosť, úplnosť a spoľahlivosť získanej terminológie je reprezentatívnosť textového korpusu. Pod týmto pojmom lingvisti rozumejú taký rozsah a kvalitu textov, ktoré poskytujú celkový a vyvážený obraz o (odbornom) jazyku.²⁸ V odbore právo sú reprezentatívnymi korpusmi legislatívne texty, texty právnej vedy, súdne rozhodnutia a rozhodnutia štátnych orgánov, texty zmlúv a dohovorov písané právnikmi, v ktorých sa termíny objavujú vo svojom prirodzenom kontexte určujúcim význam pojmov.

Zoznam použitej literatúry

1. ABRAHÁMOVÁ, Eva: Základy právnej komunikácie. Šamorín: Heuréka, 2012. 128 s. ISBN 978-80-89122-81-3
2. BHATIA, Vijay – LANGTON, Nicola N. – LUNG, Jane: Legal discourse: Opportunities and threats for corpus linguistics. In: Discourse in the Professions. Perspectives from corpus linguistics. Amsterdam: John Benjamins, 2004. 333 s. ISBN 90-272-2287-8
3. BIEL, Łucja. Corpus-Based Studies of Legal Language for Translation Purposes: Methodological and Practical Potential. In: HEINE, C.; ENGBERG, J. (ed.). *Reconceptualizing LSP*. Online proceedings of the XVII European LSP Symposium 2009. Aarhus, 2010. s. 4. Dostupné na: <https://bcom.au.dk/fileadmin/www.asb.dk/isek/biel.pdf> [zobrazené 2022-11-04]
4. CABRÉ, María Teresa: La terminología. Teoría, metodología, aplicaciones. 1. edícia. Barcelona: Empúries, 1993. 529 s. ISBN 84-7596-405-2
5. CVRČEK, Václav: Kvantitativní analýza kontextu. Praha: Lidové noviny, Ústav Českého národního korpusu, 2013, 283 s. ISBN 978-80-7422-264-1
6. CVRČEK, František: Právní informatika a lingvistika. In: Jurisprudence, Roč. 2, č. 6 (2016), s. 49-53
7. ČERMÁK, František. Korpus a korpusová lingvistika. Praha: Karolinum Press, 2017. <https://ebookcentral.proquest.com/lib/uniba-ebooks/detail.action?docID=5325775> [zobrazené 2023-03-24].
8. CLÉMENT-WILZ, Laure - DE LAFORCADE, Agata — CENNAMO, Ilaria: Translation in the European Union: Navigating Technical and Legal Issues in the Light of Artificial Intelligence - Conclusions. In: International Journal of Language and Law (JLL), roč. 14, Special Issue: Artificial Intelligence and the Language of

²⁸ ČERMÁK, František. Korpus a korpusová lingvistika. Praha: Karolinum Press, 2017, s. 28

- Law (2025), s. 240-255. ISSN: 2194-7414. Dostupné na: <https://www.languageandlaw.eu/jll/issue/view/14> [zobrazené 2025-09-09].
9. KILGARRIFF, Adam et al. The Sketch Engine : Ten years on. In: Lexicography. Online. roč. 1, č. 1 (2014), s. 7–36. Dostupné na: <https://doi.org/10.1007/s40607-014-0009-9> [zobrazené 2022-03-22].
 10. LEVICKÁ, Jana: Terminologické implikácie štruktúrnej a kontextovej analýzy francúzskej a slovenskej stavebnej lexiky, diz.p., Univerzita Komenského v BA, Filozofická fakulta, 2006. 221 s.
 11. LEVICKÁ, Jana: Slovenská terminologická databáza. In: Kultúra slova, roč. 42, č. 3 (2008), s. 139-157
 12. ŁUKASIK, Marek: Corpus linguistics and generative AI tools in term extraction: a case of Kashubian – a low-resource language. In: Applied Linguistics Papers, Roč. 27, č. 4 (2023), s. 34-45 Dostupné na: http://alp.uw.edu.pl/wp-content/uploads/sites/315/2024/02/5-ALP_Lukasik-Marek.pdf [zobrazené 27.09.2025]
 13. MARÍN PÉREZ, María José. "Automatic term recognition and legal language: A shorter path to the lexical profiling of legal texts?". *Handbook of Terminology: Volume 3. Legal Terminology*, edited by Łucja Biel and Hendrik J. Kockaert, John Benjamins Publishing Company, 2023, s. 511-541. <https://doi.org/10.1075/hot.3.aut2> [zobrazené 2025-09-29].
 14. MASÁR, Ivan: Príručka slovenskej terminológie. Bratislava: VEDA, 1991, 192 s. ISBN 80-224-0341-5
 15. MISTRÍK, Jozef: Lingvistický slovník. Bratislava: SPN, 2002. 294 s. ISBN 80-08-02704-5
 16. PÁTKOVÁ, Jarmila: Korpusová analýza pracovnoprávných textov v jazykovej kombinácii francúzština-slovenčina so zameraním na ustálené slovné spojenia a terminológiu, diz. p. Univerzita Komenského v BA, Filozofická fakulta, 2025. 192 s.
 17. SAGER, Juan-Carlos: A Practical Course in Terminology Processing. Amsterdam-Philadelphia: John Benjamins, 1990. 252 s.
 18. ŠALING, Samo et al.: Veľký slovník cudzích slov. Veľký Šariš: Samo – AAMM, 1997. 1310 s. ISBN 80-967524-0-5
 19. ŠPÁNIOVÁ, Marta: Význam terminológie pre informačnú činnosť: Terminologické princípy tvorby tezaurov a interoperabilita s inými slovníkmi. In: Zborník Filozofickej fakulty Univerzity Komenského, Knižničná a informačná veda XXVI (2016), s. 45-68. ISBN 978-80-223-4252-0 s. 48
 20. ŠTEFKOVÁ, Marketa: Právny text v preklade. Translatologické aspekty právnej komunikácie v kombináciách málo rozšírených jazykov. Bratislava: Iura Edition, 2013, 222 s. ISBN 978-80-8078-681-6

21. TALIB, Ramzan et al.: Text Mining: Techniques, Applications and Issues. In: International Journal of Advanced Computer Science and Applications (IJACSA), Roč. 7, č.11 (2016), s. 414-418. <http://dx.doi.org/10.14569/IJACSA.2016.071153>
22. WISSIK, Tanja: Impact of automatic term extraction on terminology work. A qualitative interview study in institutional. In: Terminology, International Journal of Theoretical and Applied Issues in Specialized Communication, roč. 31, č. 1 (2025), s. 110-135. ISSN 0929-9971 E-ISSN 1569-9994
23. XU, Kang - FENG, Yifan – LI, Quiandi et al.: Survey on terminology extraction from texts. In: Journal of Big Data, roč. 12, č. 29 (2025) <https://doi.org/10.1186/s40537-025-01077-x>

Online slovníky:

SKETCH ENGINE - glosár: <https://www.sketchEngine.eu/guide/glossary/>

TRÉSOR DE LA LANGUE FRANÇAISE INFORMATISÉ (TLFi), Dostupné na: <http://atilf.atilf.fr/>

Kontaktné údaje

Mgr. Jarmila Pátková, PhD.

jarmila.patkova@flaw.uniba.sk

Právnická fakulta UK v Bratislave

Ústav cudzojazyčnej právnej komunikácie

MOŽNOSTI A LIMITY STROJOVÝCH PREKLADAČOV NA BÁZE UMELEJ INTELIGENCIE PRI PREKLADE PRÁVNEJ TERMINOLÓGIE

POSSIBILITIES AND LIMITS OF AI-BASED MACHINE TRANSLATORS IN THE TRANSLATION OF LEGAL TERMINOLOGY

Alexandra Debnárová¹

Abstrakt: Digitálne technológie a ich využitie sú v posledných rokoch čoraz častejšie predmetom skúmania rôznych vedných disciplín a translatológia nie je výnimkou. Zapojenie umelej inteligencie do prekladu otvára nový priestor pre diskusiu a prináša otázky týkajúce sa, okrem iného, spoľahlivosti moderných prekladových nástrojov. Preklad právnych textov a právnej terminológie si navyše vyžaduje špecifický prístup a zvýšenú mieru zodpovednosti za výsledný translát. Predložený príspevok sa zameriava na možnosti, ktoré prinášajú technológie v podobe súčasných strojových prekladačov, ako aj na ich obmedzenia vyplývajúce nielen z povahy právnych textov. Výhody strojových prekladačov, najmä tých na báze neurónových sietí, spočívajú predovšetkým v časovej úspore a efektivite, prípadné limity majú rôznu závažnosť a príčiny. Súčasťou príspevku je porovnanie vybraných pojmov, ktoré sú súčasťou nemeckej právnej terminológie, pričom iba jeden má ustálený ekvivalent v slovenskom jazyku, s pomocou neurónových prekladačov. Zaujímalo nás, ako a či vôbec sa na ich výslednom preklade prejaví zasadenie do kontextu a zmena gramatického rodu.

Kľúčové slová: strojový preklad, neurónový strojový preklad, umelá inteligencia, právna terminológia

Abstract: In recent years, digital technologies and their applications have increasingly become the subject of research across various disciplines, and translation studies is no exception. The integration of artificial intelligence into translation opens up new spaces for discussion and raises questions concerning, among other things, the reliability of modern translation tools. The translation of legal texts and legal terminology, moreover, requires a specific approach and a heightened level of responsibility for the resulting translation. This paper focuses on the possibilities offered by current machine translation

¹ Právnická fakulta Univerzity Komenského v Bratislave, Ústav cudzojazyčnej právnej komunikácie

technologies, as well as on their limitations stemming not only from the nature of legal texts. The advantages of machine translators, especially those based on neural networks, lie primarily in time efficiency and effectiveness, while their limitations vary in degree and cause. The paper also includes a comparison of the translation of selected terms from German legal terminology, of which only one has a fixed equivalent in Slovak, carried out with the help of neural machine translators. We were interested in how and whether their final translation would reflect their context and change in grammatical gender.

Key words: machine translation, neural machine translation, artificial intelligence, legal terminology

Úvod

Keďže vzájomná komunikácia je kľúčovým predpokladom výmeny informácií a nadväzovania spolupráce a medziľudských vzťahov, je prirodzené, že jej zjednodušenie sa stalo jedným z ústredných snažení ľudského spoločenstva aj na medzijazykovej úrovni. Používanie digitálnych technológií na báze AI sa v súčasnosti zrejme najvýraznejšie manifestuje na masívnom využívaní voľne dostupných strojových prekladačov na princípe neurónových sietí. Zaujímalo nás, aké sú možnosti a limity pri ich používaní a to najmä pokiaľ ide o špecifické právne texty. V závere sme analyzovali preklad vybraných termínov nemeckého právneho jazyka prostredníctvom neurónových prekladačov. Prekladače vygenerovali vybraný pojem najskôr izolovane a následne zasadený do reálneho kontextu rozhodnutí súdov jednej zo spolkových krajín.

Umelá inteligencia

Oznámenie Európskej komisie Európskemu parlamentu a ďalším európskym inštitúciám pod názvom *Umelá inteligencia pre Európu* z r. 2018 definovalo vôbec po prvý raz umelú inteligenciu takto: „Umelá inteligencia sú systémy, ktoré vykazujú inteligentné správanie tým, že analyzujú okolité prostredie a podnikajú kroky – s istou mierou samostatnosti – na dosiahnutie konkrétnych cieľov. Systémy umelej inteligencie môžu byť založené výlučne na softvéri a pôsobiť vo virtuálnom svete (napr. hlasoví asistenti, softvér na analýzu fotografií, vyhľadávače, systémy rozpoznávania hlasu a tváre), ale umelá inteligencia môže byť aj súčasťou

hardvérových zariadení (napr. vyspelé roboty, autonómne vozidlá, bezpilotné vzdušné prostriedky alebo aplikácie internetu vecí).²

Definícia bola o rok neskôr prostredníctvom expertnej skupiny zriadenej Európskou komisiou (AI HLEG) zrevidovaná a rozšírená, pričom zúčastnení odborníci zdôrazňovali ako významnú súčasť (do istej miery vágneho) konceptu inteligencie pojem racionality ako schopnosti zvoliť si akciu, ktorá čo najlepšie poslúži dosiahnutiu určitého cieľa.³ Informatik S. Russell, ktorý sa špecializuje na AI, v súvislosti s konceptom inteligencie upozorňuje, že pokiaľ mieru inteligencie človeka odvodzujeme od schopnosti dosahovať vlastné zámery, potom by sme s prívlastkom *inteligentný* v súvislosti s nástrojmi AI mali nárábať opatrne, nakoľko nechceme, aby dosahovali svoje vlastné zámery, ale boli prospešné pre nás - ľudí. Aj on operuje s pojmom racionality, umelá inteligencia sa podľa neho zaoberá detailmi zostrojenia racionálnych strojov.⁴

Aj keď sa odborníci zhodujú, že pojem umelá inteligencia nevystihuje celkom presne jej podstatu, v spoločnosti je natoľko vžitý, že sa stal pevnou súčasťou globálneho komunikačného priestoru.

Umelá inteligencia a preklad

Dokument Európskej komisie s názvom Umelá inteligencia pre Európu uvádza jazykový preklad ako jeden z príkladov každodenného využitia umelej inteligencie, pričom zdôrazňuje zlepšenie výkonnosti plnenia úloh ako je strojový preklad vďaka *hlbokému učeniu* ⁵(*deep learning*).⁶

Russel považuje za tri najdôležitejšie aplikačné oblasti AI rozpoznávanie objektov, rozpoznávanie reči a strojový preklad. Rozpoznávanie objektov na obrázkoch, ktoré testovalo niekoľko výskumných skupín na veľkom množstve cvičných dát, preukázalo zníženie 15 -percentnej strojovej chybovosti v r. 2012 na 2- percentnú chybovosť v roku 2017. Vďaka princípu hlbokého učenia došlo k porovnateľnému progresu aj vo

² Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Umelá inteligencia pre Európu. [cit.1. septembra 2025], dostupné na: https://www.umelainteligenciavpraxi.sk/download_portal_files/onlibai/oznamenie-umela-inteligencia-pre-europu.pdf

³https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf [cit.1. septembra 2025]

⁴ RUSSELL, S.: Jako člověk. Umělá inteligence a problém jejího ovládání. Praha: Dokořán, 2021. s. 15.

⁵ V súčasnosti sa takmer výlučne prekladá ako *hlboké učenie*, v texte budeme preto ďalej používať tento slovenský ekvivalent, hoci v oficiálnom preklade dokumentu sa hovorí o „hlbkovom učení“.

⁶ Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Umelá inteligencia pre Európu. [cit.1.septembra2025] Dostupné na: https://www.umelainteligenciavpraxi.sk/download_portal_files/onlibai/oznamenie-umela-inteligencia-pre-europu.pdf

zvyšných dvoch oblastiach, teda aj v oblasti strojového prekladu.⁷ Výrazné zníženie chybovosti za pomerne krátke obdobie naznačilo perspektívu zlepšovania aj do budúcnosti.

Integrácia UI do prekladového procesu je aktuálnou témou v európskych inštitúciách ako Európska komisia či Súdny dvor EÚ. EK v r.2017 sprístupnila eTranslation, vlastný interný nástroj na neurónový strojový preklad, Súdny dvor EÚ v r.2023 prijal stratégiu na využitie UI a analýzu jeho prípadných rizík aj pri preklade súdnych rozhodnutí, uznesení a ďalších súvisiacich dokumentov.⁸

Výhody nástrojov na báze umelej inteligencie pri preklade

Medzi hlavné výhody strojových prekladačov patrí efektivita, časová a finančná úspora. Strojové prekladače umožňujú za veľmi krátky čas preložiť veľký objem textu. V súčasnosti navyše prekladové nástroje ponúkajú preklad z/do veľkého množstva jazykov. Potrebám bežných užívateľov často postačuje „hrubý preklad“, ktorý umožní transfer kľúčovej informácie východiskového textu do želaného jazyka aj za cenu jeho nižšej kvality tzn. použitia menej vhodných synonym, neprirodzených slovných obrátov, s výskytom štylistických chýb atď. ⁹ Treba však poznamenať, že uvedené bolo skôr doménou starších štatistických prekladačov, a s nástupom neurónových strojových prekladačov sa výrazne zvýšila kvalita ich výstupov.

M. Štefková pri pozitívach využitia nástrojov na strojový preklad uvádza, že „odborná literatúra zdôrazňuje výhodu konzistencie prekladu aj v prípade veľmi špecifickej terminológie.“ ¹⁰ Konzistentnosť strojových prekladačov sa môže ukázať ako výhoda aj v porovnaní s prípadmi, keď zadávateľ v dôsledku časového tlaku musí zákazku rozdeliť medzi viacerých prekladateľov.

Je nepopierateľné, že kvalita výsledného prekladu do značnej miery závisí od kvality zdrojového textu. Uvedené sa týka najmä (no nielen) angličtiny, keď sa do rúk prekladateľa dostane text zhotovený autorom, ktorý ma odlišný materinský jazyk, a východiskový jazyk neovláda na dostatočnej úrovni. Prekladače a chatboty na báze UI môžu nevyhovujúci text upraviť do vyhovujúcej jazykovej podoby štandardného

⁷ RUSSEL, S.: Jako člověk. Umělá inteligence a problém jejího ovládání. Praha: Dokořán, 2021. s. 220-222

⁸ WRIGHT, S: Artificial Intelligence in Legal Translation at the Court of Justice of the European Union. In: International Journal of Language and Law. Vol.14. 2025. s.127

⁹ „Uplatnenie týchto technológií v súčasnosti stále smeruje k prekladu jednoduchých textov bez typických črt autentického, živého jazyka, bez typických lexikálnych vzťahov v slovnej zásobe, ako metafora, metonymia, homonymia, kontextová viazanosť pojmov a pod.“ In: ŠTEFKOVÁ: M.:Právny text v preklade. Translatologické aspekty právnej komunikácie v kombináciách málo rozšírených jazykov. Bratislava: IURA EDITION, spol.s.r.o. 2019. s. 153

¹⁰ Tamže s.154

jazyka, a uľahčiť tým prekladateľovi prácu, vykonávajúc tak úlohu prvého editora textu.

Prekladateľská činnosť dominuje prostrediu orgánov EÚ, v ktorej s každým rozšírením narastá počet úradných jazykov. V záujme väčšej efektivity dochádza často k nepriamym prekladom prostredníctvom piatich pivotných jazykov. Využitím spoľahlivých prekladových nástrojov, v súlade s Aktom o UI, by mohlo dôjsť k zvýšeniu kvality prekladov v európskych inštitúciách a predísť stratám, ku ktorým nevyhnutne dochádza pri preklade z druhej ruky.

Nedostatky prekladových nástrojov na báze umelej inteligencie

Oznámenie Komisie o umelej inteligencii adresované európskym inštitúciám uvádza ako jej nedostatok absentovanie kľúčových zručností vlastných ľuďom, ako sú kreativita a kritické myslenie.¹¹ Odkazujúc na terminologický aparát Antona Popoviča¹² možno pri prekladových nástrojoch využívajúcich umelú inteligenciu hovoriť aj o absencii skúsenostného komplexu prekladateľa, ktorý „zahŕňa spoločenské, filozofické, psychologické a iné názory a individuálne skúsenosti osvojené prekladateľom, slúžiace ako pozadie pri komunikačnej, semiotickej a štylistickej realizácii prekladu“¹³. Aj keď sú mantinely, v ktorých sa môže prekladateľ odborného resp. právneho textu pohybovať, omnoho užšie ako u prekladateľa literárneho textu, jeho skúsenostný komplex zohráva pri tvorbe východiskového textu nezanedbateľnú úlohu. Zatiaľ čo prekladateľ pri tvorbe výsledného textu prechádza rozhodovacím procesom, nástroje na preklad pri tvorbe textu rozhodovací proces nahrádzajú výberom ekvivalentu z dostupnej databázy. Hoci sa v súvislosti so systémami UI niekedy hovorí o rozhodovaní, v skutočnosti takýto systém *iba* „automatizuje procesy, ktoré sa tradične vykonávajú na základe ľudského úsudku“.¹⁴ D. Munková pomenúva niekoľko problémov, ktoré sú príčinami chybovosti strojového prekladu. Ide o problém analýzy (neporozumenie východiskového textu v dôsledku jeho nižšej kvality), problém transferu (nesúlady vo forme a obsahu), problém syntézy (príliš veľa možností na vyjadrenie toho istého obsahu) a problém medzijazykovej rozdielnosti (neschopnosť preložiť lexémy neštandardného jazyka).

¹¹ Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Umelá inteligencia pre Európu. [cit.1.septembra2025] Dostupné na: https://www.umelainteligenciavpraxi.sk/download_portal_files/onlibai/oznamenie-umela-inteligencia-pre-europu.pdf

¹² Popovič nadviazal na pojem *skúsenostný komplex* Františka Mika.

¹³ POPOVIČ, A.: Originál/Preklad. Bratislava: Tatran. 1983. s. 164

¹⁴ Commission_Guidelines_on_the_definition_of_an_artificial_intelligence_system_established_by_Regulation_EU_20241689_AI_Act_Slovak_zCilj9dxjfiBU3mXnEPl15Vb64_118637.PDF [cit.1.septembra2025]

Tie sa manifestujú v doslovnosti prekladu, v použití nesprávneho synonyma, nesprávnom slovoslede a pod.¹⁵

Pri otázke negatív nástrojov umelej inteligencie sa možno stretnúť s názorom, že ich použitie môže viesť k prehlbovaniu nežiaducich stereotypov a diskriminácie, a to napríklad pri virtuálnych asistentkách s prevažne ženskou identitou, pri rozpoznávaní tváří iba určitej farby pleti, pri nastavovaní kritérií vo výberových konaniach a pod.¹⁶ Dáta, na ktorých sú trénované strojové prekladače, môžu obsahovať diskriminatívne vzorce, ktoré sa následne premietnu do prekladov a generovaných textov.¹⁷

Pri prekladateľských programoch vidia niektorí autori problém v zvolení pohlavia podľa kontextu pri spätnom preklade z jazyka, ktorý pohlavie nerozlišuje.¹⁸ V prípade prekladu do iného jazyka navyše nemusí prekladový nástroj zohľadniť prítomnosť gramatického rodu, a to ani pri jazykových kombináciách, kde oba jazyky touto kategóriou disponujú. Kľúčovým zdrojom dát pre prvú verziu Google prekladača, pričom jedným z jeho zdrojov je dodnes, bol korpus Europarl založený na prepisoch schôdzí Európskeho parlamentu. Percentuálny podiel viet vyslovených ženskými hovoriacimi bol v závislosti od skúmaných datasetov 32-33%, čo svedčí o jeho rodovej nevyrovnanosti,¹⁹ ktorá sa môže odraziť aj vo výslednom preklade.²⁰

Ak sme pri výhodách použitia prekladových nástrojov na báze UI hovorili o rýchlosti, je potrebné podotknúť, že pri použití nesprávneho algoritmu, nedostatočne kvalitného zdrojového textu alebo tréningových dát môže byť výstupom síce rýchlo dodaná, no nesprávna informácia.²¹ Tá si bude v lepšom prípade vyžadovať dôkladnú posteditáciu, v horšom bude výstup nepoužiteľný.

Aj Nemecký Spolkový zväz tlmočníkov a prekladateľov²² upozorňuje na riziká používania prekladačov a pripomína, že humánny prekladateľ v určitom zmysle vykonáva dodatočnú kontrolu kvality textu a môže si všimnúť nedostatky, ktoré UI

¹⁵ MUNKOVÁ, D.: Strojový preklad a translatológia. Nitra: Univerzita Konštantína Filozofa v Nitre. 2020.s. 27

¹⁶ KOLAŘÍKOVÁ, L., HORÁK, F: Umělá inteligence a právo. Praha: Wolters Kluwer ČR. 2020. s. 115-124

¹⁷ <https://bdue.de/mdue-online/vorsicht-uebersetzen-mit-chatgptco> [cit. 10.septembra 2025]

¹⁸ „Podobným problémem jsou například překladatelské programy, které při zpětném překladu z jazyka nerozlišujícím pohlaví toto zvolí dle kontextu, což opět může vést k posilování předsudků.“ S-111

¹⁹ VANMASSENHOVE, E., HARDMEIER, CH., WAY, A.: Getting Gender Right in Neural Machine Translation. 2018 S. 3003

²⁰ Tamže. Skupina výskumníkov z univerzít v Dubline a v Uppsale uskutočnila zaujímavý experiment, keď v súvislosti s databázou Europarl do NMT nástroja integrovala informáciu o rode hovoriaceho, čím vo väčšine prípadov dosiahla presnejší preklad na úrovni gramatického rodu, výsledky sa však líšili v závislosti od jednotlivých jazykových kombinácií.

²¹ RUSSEL, S.: Jako člověk. Umělá inteligence a problém jejího ovládní. Praha: Dokořán, 2021. s.36

²² Bundesverband der Dolmetscher und Übersetzer

ignoruje, napr. obsahové nezrovnalosti, duplicitný či multiplicitný výskyt slov alebo slovných spojení v dôsledku kopírovania či nesprávne uvedené interpunkčné znamienka. Zväz pripomína aj fakt, že čím plynulejšie a prirodzenejšie preklad znie, tým ľahšie možno prehliadnuť chyby strojového prekladača.²³

Špecifiká prekladu právnych textov pri využití prekladových nástrojov na báze UI

Právne texty v tejto súvislosti chápeme v širšom zmysle, teda ako súbor všetkých textov právnej povahy bez špecifikácie právnej oblasti alebo zložky štátnej moci, pod ktorú spadá. V právnom texte prevažuje vysoký štýl, no v závislosti od konkrétneho typu sú jeho súčasťou aj výpovede zachytávajúce autentický prejav hovoriacich. Právne texty obsahujú jednotlivé termíny, ale aj väčšie textové celky pochádzajúce z iných vedných odborov (zákony so špecifickou terminológiou, konkretizovanie predmetu zmluvy, súdne spisy so znaleckými posudkami atď.)²⁴ Ak prekladač nedokáže detegovať ten-ktorý štýl, nedôjde k dosiahnutiu štylistickej ekvivalencie, ktorá je jedným z indikátorov kvality prekladu, a výsledkom je štylistická nivelizácia.²⁵

Možným argumentom v neprospech prekladových nástrojov by mohol byť fakt, že tento nemá informácie o koncovom užívateľovi prekladu. Poznanie cieľového recipienta sa tradične považuje za dôležitý činiteľ, na ktorý prekladateľ berie ohľad pri kreovaní translátu. Pri právnych typoch textov je dôležité poznať účel, na ktorý má preklad slúžiť, aby bolo zrejmé, či má ísť o právne záväzný dokument alebo je jeho úloha iba informatívna, a či je recipientom laik alebo odborník v oblasti. S výnimkou prekladov pre štátne inštitúcie či prekladov, ktoré si zabezpečujú spoločnosti z interných zdrojov, však aj prekladateľom nezriedka chýbajú informácie o zadávateľovi zákazky. Týka sa to najmä prekladov zadávaných prostredníctvom agentúr. Výskum na vzorke 303 prekladateľov právnych textov zo 41 krajín ukázal, že 26% z nich informáciou o koncovom užívateľovi prekladu nedisponuje nikdy, ďalších 34% uviedlo, že ňou disponuje iba zriedka. Niekedy zadávateľ (agentúra) tento údaj neposkytuje zámerne z dôvodu zachovania dôvernosti.²⁶

Dôležitou požiadavkou na výsledný translát, navyše s ohľadom na možné právne následky, je presnosť, spoľahlivosť a spomínané zachovanie dôvernosti. Rizikom pri používaní online prekladačov je únik dôverných informácií napr. v prípade

²³ <https://bdue.de/mdue-online/vorsicht-uebersetzen-mit-chatgptco>

²⁴ ĎURICOVÁ, A.: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Bellianum. Vydavateľstvo UMB v Banskej Bystrici. 2016. s.27

²⁵ RAKŠANYIOVÁ, J.: Sociálny priestor súčasného právneho prekladu na Slovensku In: *Úradný prekladateľ v slovenskom a európskom sociálnom priestore*. Bratislava: Vydavateľstvo univerzity Komenského v Bratislave, 2015. s. 36

²⁶ SCOTT, R.J.: Legal Translation Outsourced Oxford: Oxford University Press, 2019. s. 133-136

nedôslednej anonymizácie dokumentov, ani tá však nemusí zaručiť, že nebude odhalená identita zúčastnených strán, prípadne iný typ údajov.²⁷

Špecifikom právnych textov sú vnútrojazykové rozdiely vyplývajúce z existencie rôznych právnych systémov, ktoré spája jeden jazyk. Jeden právny dokument môže zasahovať do viacerých jurisdikcií,²⁸ v ktorých sú prítomné rozdiely na rovine legislatívy, terminológie²⁹, ale aj názvoslovia a kompetencií inštitúcií. Otázkou je, či a do akej miery dokáže strojový prekladač identifikovať krajinu/y pôvodu príslušného dokumentu a aplikovať príslušnú terminológiu, najmä ak sa vyskytnú v jednom texte. Zaujímavý výsledok v tejto súvislosti priniesol terénny výskum J. Rakšányiovej, z ktorého vyplýva, že dve tretiny oslovených respondentov z radov slovenských prekladateľov vnútrojazykové terminologické rozdiely nezohľadňujú a používajú vždy rovnaké ekvivalenty.³⁰

Právne texty v slovenčine charakterizuje častý výskyt bohemizmov. K. Hegerová poukazuje, že jazyková stránka legislatívnych textov „významnou mierou ovplyvňuje jazykové vedomie používateľov jazyka“, a že napriek desaťročiam upozornení zo strany jazykovedcov sa nielen v legislatívnych textoch, ale aj v písomných a ústnych prejavoch objavujú nevhodné a nespisovné slová a slovné spojenia. Ide napr. o pojmy ako prejednávať, obdržaný, závierka, zahájiť a pod.³¹ M. Štefková upozorňuje, že „nedostatok pozornosti venovanej jazykovej kultúre primárnych legislatívnych textov sa následne odráža v jazykovej úrovni aktov aplikácie práva, ktoré sú často predmetom prekladu“³². Tieto lapsusy sa pri vytváraní databáz/korpusov autentických právnych textov pre potreby strojového prekladu môžu preniesť do koncového prekladu a spolupodieľať sa na zachovávaní nežiaduceho status quo.

²⁷ Viac o kryptografických metódach slúžiacich na zachovávanie dôvernosti informácií aj prostredníctvom fragmentácie textu a označovania vybraných segmentov textu (tzv. tagging) pozri: BISAZZA, A., KIM.S., TURKMEN, F.: Using Confidential Data for Domain Adaptation of Neural Machine Translation. In: Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics. 2020. s. 46-52

²⁸ Napr. v prípade nemčiny do jurisdikcií NSR, Rakúska, Švajčiarska, Belgicka a Lichtenštajnska.

²⁹ Téma rozličných právnych systémov v nemecko-jazyčnom prostredí sa venuje pozri: WREDE, O. Právny preklad a jeho translačné modely – teória a prax. Nitra: Univerzita Konštatntína Filozofa v Nitre, 2021. s. 16 -21

³⁰ RAKŠANYIOVÁ, J.: Sociálny priestor súčasného právneho prekladu na Slovensku In: *Úradný prekladateľ v slovenskom a európskom sociálnom priestore*. Bratislava: Vydavateľstvo univerzity Komenského v Bratislave, 2015.s. 47

³¹ HEGEROVÁ, K. O jazykovej kultúre v právnických textoch In: *Kultúra slova*. 1995. č.6, s. 334-335

³² ŠTEFKOVÁ, M.: Právny text v preklade. Translatologické aspekty právnej komunikácie v kombináciách málo rozšírených jazykov. Bratislava: IURA EDITION, spol.s.r.o., 2019. s. 61

Prekladače

Pre potreby analýzy sme použili dostupné strojové prekladače fungujúce na princípe umelých neurónových sietí (NMT³³). Tie na rozdiel od pôvodných, štatistických automatizovaných nástrojov určených na strojový preklad (MT³⁴), ktoré izolovane prekládali jednotlivé slová, berú do úvahy aj kontext v rámci prekladaného textu či isté významové nuansy. Zvolili sme si najznámejší voľne dostupný prekladač Google Prekladač (Google Translate) s najväčším množstvom jazykových kombinácií, prekladač DeepL, poskytujúci údajne najadekvátnejšie preklady, najstarší prekladač Systran a napokon konverzačného robota ChatGPT.

Google Prekladač (2016) vznikol ako nástroj na štatistický strojový preklad (SMT³⁵). Ten najskôr preložil východiskový text do angličtiny, aby ho následne previedol do zvoleného jazyka. V prípade slovenčiny ako východiskového jazyka bola ďalším sprostredkujúcim jazykom okrem angličtiny čeština, išlo teda o preklad z druhej ruky. Transfer do cieľového jazyka a výber použitých slov prebiehal na základe štatistickej pravdepodobnosti, pričom čerpal primárne z databázy transkripcií, ktoré vznikli na základe schôdzí Európskeho parlamentu a dokumentov OSN. Ako uvádzajú D. Munková a P. Petráš: „Strojový preklad je schopný vytvoriť niekoľko prekladov k jednej východiskovej vete a aplikovaním štatistického prístupu vyberie najpravdepodobnejší preklad. Pri tomto prístupe k prekladu sa nevyužívajú rozsiahle jazykové znalosti, ale jazykové korpusy a algoritmus založený na pravdepodobnosti.“³⁶

V r. 2017 začal Google prekladač využívať princíp hlbokého učenia na báze umelých neurónových sietí.³⁷ „Neurónový strojový preklad chápe vetu ako celok a vytvára asociácie medzi frázami aj v dlhších vetách, t.j. prečíta si všetky východiskové slová až po koniec vety a až potom naraz začne *vysielať* jedno cieľové slovo.“³⁸

Tieto princípy využíva aj prekladač DeepL (2017) tvorcov paralelného korpusového slovníka Linguae, ktorý je zároveň významným zdrojom jeho dát. DeepL ponúka menej jazykových kombinácií a vychádza z menšej databázy.

³³ Neural Machine Translation

³⁴ Machine Translation

³⁵ Statistical Machine Translation

³⁶ D. MUNKOVÁ, P. PETRÁŠ: Strojový preklad založený na neurónových sieťach – sľubná cesta prekladu z analytických jazykov do flektívnej slovenčiny?. In: Slovenská reč: Nitra: Univerzita Konštantína Filozofa v Nitre, 2017. s. 76

³⁷ K metóde učenia pozri viac: VÉGH, P. Neurónové a fuzzy systémy (základy umelej inteligencie). Bratislava: Slovenská technická univerzita v Bratislave, 2014. s. 68-69 a RUSSEL.: Jako člověk. Umělá inteligence a problém jejího ovládní. Praha: Dokořán, 2021. s. 218-225

³⁸ D. MUNKOVÁ: Strojový preklad a translatológia. Nitra: Univerzita Konštantína Filozofa v Nitre. 2020. s.22

Jedným z najstarších strojových prekladačov je systém Systran (1964), ktorý pôvodne fungoval ako prekladač založený na pravidlách (RBMT³⁹) a neskôr ako hybridný nástroj, ktorý kombinoval vlastnosti pravidlového a štatistického prekladu. V súčasnosti aj on využíva princíp umelých neurónových sietí.

Posledným prekladovým nástrojom, hoci naň nie je primárne určený, je konverzačný robot ChatGPT (2022). Pri ChatGPT bola využitá technológia RLHF⁴⁰, ktorá pracuje s využitím ľudskej spätnej väzby a je naprogramovaná tak, aby rozpoznávala negatívnu („tresty“) a pozitívnu spätnú väzbu („odmeny“).

Komparatívna analýza

Nakoľko slovenčina aj nemčina sú flektívne jazyky, pri transfere sémantickej informácie pri tejto jazykovej kombinácii „odpadá“ problém, ktorý je pri súčasnej dominancii anglického jazyka spôsobený jeho analytickou povahou. Oba jazyky disponujú gramatickými kategóriami ako rod či pád podstatných mien, navyše sú oba právne systémy – slovenský aj nemecký, súčasťou kontinentálneho práva.

Hlavnými kritériami pri manuálnom (ľudskom) hodnotení toho-ktorého prekladového riešenia sú najčastejšie plynulosť a adekvátnosť.⁴¹ Adekvátnosť⁴² sa orientuje na východiskový jazyk, teda zachovanie zmyslu originálu, pričom plynulosť je kvalita orientovaná na cieľový jazyk translátu. Adekvátnosť prekladu do cieľového jazyka je u súčasných prekladačov do veľkej miery závislá od kontextu aj vzhľadom na polysémiu, pričom v niektorých jazykoch sú viacvýznamové slová zastúpené veľmi výrazne. V nemčine jestvuje skupina slov, ktorá nesie istý význam v bežnom jazyku a odlišný význam v právnom jazyku (napr. *ausschlagen* ako vykopnúť resp. odmietnuť), ale stretávame sa aj s termínmi, ktoré majú viacero funkčných významov (napr. *Gewalt* ako *moc* a *Gewalt* ako *násilie* resp. *Leistung* ako výkon či *Leistung* ako *plnenie*) aj v rámci právnej terminológie.

Stredobodom našej analýzy je preklad trojice nemeckých lexém, sústredených okolo termínu *Zeuge* v zmysle slovenského *svedok*. Konkrétne ide o termíny *Augenzeuge*, *Ohrenzeuge* a *Knallzeuge*. S výnimkou prvého pojmu *Augenzeuge* tzn. očitý *svedok*, nemajú v slovenskom jazyku ustálený ekvivalent. Zákon nedisponuje ich presnou definíciou, možno sa však s nimi stretnúť napr. v textoch súdnych rozhodnutí nemeckých súdov. Pojem *Ohrenzeuge* označuje osobu, ktorá podáva svedectvo o niečom, čo počula. Pojem *Knallzeuge* označuje zväčša osobu, ktorá počula náraz

³⁹ Rule Based Machine Translation

⁴⁰ Reinforcement Learning from Human Feedback

⁴¹ Problematike hodnotenia kvality strojového prekladu sa vyčerpávajúco venuje D.Munková. In: *Strojový preklad a translatológia*. Nitra: Univerzita Konštantína Filozofa v Nitre. 2020.S.24-26

⁴² Pojem adekvátnosť sa používa pri hodnotení kvality výstupov moderných strojových prekladačov, v našom kultúrnom prostredí je zaužívaný termín ekvivalencia.

v dôsledku dopravnej nehody, no nebola jej očitým svedkom. Čerpali sme z databázy rozsudkov spolkové krajiny Severné Porýnie-Vestfálsko, išlo o novšie rozhodnutia vynesené po r. 2020.

V prvom rade nás zaujímalo, ako si dostupné strojové prekladače poradia s prekladom izolovaných termínov bez bližšieho kontextu, teda v prípade, že by sme ich použili ako slovník. Zároveň sme chceli zistiť, ako ovplyvní výsledok zmena mužského rodu na ženský. Následne sme chceli vyskúšať, ako sa zmení preklad termínov pri ich zasadení do kontextu.

Tab. č. 1

VT ⁴³	Augenzeuge/A ugenzeugin	Ohrenzeuge/Oh renzeugin	Knallzeuge/Knallzeu gin
Google prekladač	očitý svedok/očitý svedok	svedok/svedok	petardy/svedok
Systran	očitý svedok/očitý svedok	ušný svedok/ušný svedok	výbušný svedok/lupič
DeepL	svedok/svedky ňa alt. očitá svedkyňa	svedok/svedkyň a	výbušniny/svedkyňa výbuchu
ChatGPT	očitý svedok/očitá svedkyňa	svedok podľa sluchu/svedok, ktorý niečo počul /sluchová svedkyňa (svedkyňa, ktorá niečo počula)	svedok výstrelu/rachotu/nárazu resp. zvukový svedok /svedkyňa nárazu/"buchu" (osoba, ktorá pri nehode či udalosti nevidela priebeh, ale počula náraz alebo výbuch)

Východiskový termín *Augenzeuge* v mužskom rode všetky prekladače okrem DeepL nahradili správnym slovenským ekvivalentom *očitý svedok*. Na druhej strane, DeepL bol jediný nástroj, ktorý našiel vhodný ekvivalent v ženskom rode. Ženský tvar v pojmoch *Ohrenzeugin* a *Knallzeugin* identifikoval iba DeepL a ChatGPT. Je

⁴³ Východiskový termín

pozoruhodné, ako zmena gramatického rodu v niektorých prípadoch v pozitívnom zmysle ovplyvnila výsledok prekladových výstupov.

Následne sme pre zasadenie termínu (viď. Tab.2) do kontextu uviedli celú vetu, ako bola uvedená v rozsudku. Vyskytujú sa v nej dva zo skúmaných termínov.

Tab. č. 2

VT ⁴⁴	Infolgedessen saß das Opfer recht wehrlos am Frühstückstisch der abgeschiedenen Wohnung (ohne Augen- und Ohrenzeugen), was der Angeklagte zur Tat ausnutzte.
Google prekladač	V dôsledku toho obeť sedela úplne bezbranná pri raňajkovom stole v odľahlom byte (bez očitých svedkov), čo obžalovaný využil na spáchanie trestného činu.
Systran	V dôsledku toho bola obeť skôr bezbranná pri raňajkovom stole v oddelenom byte (bez očných a ušných svedkov), ktorý žalovaný využil.
DeepL	V dôsledku toho obeť sedela celkom bezbranná pri raňajkovom stole v odľahlom byte (bez svedkov, ktorí by ju videli alebo počuli), čo obžalovaný využil na spáchanie činu.
ChatGPT	V dôsledku toho sedela obeť dosť bezbranne pri raňajkovom stole v odľahlom byte (bez očitých a ušných svedkov), čo obžalovaný využil na spáchanie činu.

Z hľadiska adekvátnosti možno za najuspokojivejší považovať prekladový výstup konverzačného robota ChatGPT. Ten okrem prekladu vety uvádza aj vysvetlivku pojmu *Ohrenzeugen*, - tí, ktorí počuli, čo sa stalo. Humánný prekladateľ by vetu mohol s použitím vysvetlivky s minimálnym zásahom preformulovať tak, aby čo najlepšie spĺňala požiadavku ekvivalencie. Pri výstupe druhého najvyhovujúcejšieho prekladu od DeepL by bola takisto nevyhnutná posteditácia humánnym prekladateľom, v tomto prípade výraznejšia, nakoľko sa dopustol významového posunu. Nejde o svedkov, ktorí by počuli alebo videli obeť, ale trestný čin. Za najmenej uspokojivý možno považovať preklad vygenerovaný prekladačom Systran: spojenia očný a ušný svedok v slovenčine neexistujú, prekladač vynechal fakt, že páchatel' situáciu využil na spáchanie činu a navyše nás preniesol z trestného do civilného procesu, keďže zamenil pojem „obžalovaný“ za „žalovaný“. Nahradením vzťažného zámena „was“ zámenom „který“ z prekladu vyplýva, že dotyčná osoba využila na spáchanie činu stôl

⁴⁴ Východiskový text

resp. byť a nie predmetnú situáciu. Požiadavka plynulosti bola zachovaná vo všetkých sledovaných prípadoch.

Tab. č. 3

VT ⁴⁵	Eine solche Schilderung erinnert unwillkürlich an sogenannte "Knallzeugen" bei Verkehrsunfällen.
Google prekladač	Takýto opis nám mimovoľne pripomína takzvaných „svedkov bzučania“ pri dopravných nehodách.
Systran	Takýto opis nedobrovoľne pripomína tzv. "popových svedkov" pri dopravných nehodách.
DeepL	Takýto popis pripomína takzvané „svedectvá výbuchu“ pri dopravných nehodách.
ChatGPT	Takéto líčenie mimovoľne pripomína takzvaných „zvukových svedkov“ pri dopravných nehodách.

V poslednej tabuľke (Tab.č.3) je uvedená východisková veta v nemčine s posledným sledovaným termínom a príslušné preklady vytvorené strojovými prekladačmi. Najuspokojivejšie, hoci stále nie celkom adekvátne, je pretlmočenie ChatuGPT, jeho opisný preklad sledovaného termínu má najbližšie k požiadavke zrozumiteľnosti. Ostatné sledované preklady zvoleného pojmu nie sú adekvátnym slovenským ekvivalentom ani v kontexte celej vety. Požiadavka plynulosti bola zachovaná vo všetkých sledovaných prípadoch.

Záver

V r. 2014 a 2015 sa uskutočnil výskum J. Rakšányiovej mapujúci sociálny priestor právneho prekladu. Medzi zverejnenými výsledkami možno nájsť aj odpovede respondentov na otázku „Ako odhadujete budúcnosť právnych prekladov?“. Až 54%⁴⁶ respondentov z radov zadávateľov a 45% respondentov z radov prekladateľov uviedlo, že „úradné preklady možno vyhotovovať len v dnešnej, klasickej podobe“. Približne 20% respondentov z oboch skupín uviedlo ako odpoveď, že texty sa budú prekladať pomocou počítačových programov a ďalších 26% resp. 20% sa domnieva, že „prekladateľ bude doplnkovým korektorom strojových prekladov“. ⁴⁷ Hoci sa prieskum uskutočnil tesne pred nástupom neurónových prekladačov, domnievame sa, že má stále vysokú výpovednú hodnotu.

⁴⁵ Východiskový text

⁴⁶ Autorka upozorňuje, že respondenti si mohli zvoliť viac odpovedí a nemuseli označiť ani jednu, preto počet percent udáva frekvenciu jednotlivých odpovedí.

⁴⁷ RAKŠÁNYIOVÁ, J. Sociálny priestor súčasného právneho prekladu na Slovensku. In: *Úradný prekladateľ v slovenskom a európskom sociálnom priestore*. Bratislava: Vydavateľstvo univerzity Komenského v Bratislave, 2015. s.32

Navzdory nepomerne väčšej stati opisujúcej nevýhody a riziká použitia nástrojov na báze UI pri preklade právnych textov nebolo naším cieľom spochybňovať preukázateľné možnosti, ktoré prinášajú, ani obhajovať (oprávnené nespochybniteľnú) opodstatnenosť profesie prekladateľa. Moderné prekladové nástroje majú potenciál stať sa významným pomocníkom pri procese translácie u humánnych prekladateľov, chceli sme však upozorniť na ich limity, najmä pokiaľ ide o preklad špecifických právnych textov. Prekvapilo nás, ako významne môže uvedenie/zmena gramatického rodu pozmeniť výsledný translát, keď zadanie substantíva v ženskom rode vygenerovalo presnejší preklad. Možno konštatovať, aj na základe porovnania prekladov vybraných nástrojov na strojový preklad, že hoci prekladačom nemožno autonómne zveriť preklad právneho textu, užívateľovi, ktorý sa orientuje vo východiskovom i cieľovom jazyku a má vyššie právne povedomie, môže pri práci s daným typom textov priniesť nezanedbateľné benefity.

Zoznam použitej literatúry

1. BISAZZA, Arianna, KIM Sohyung, TURKMEN, Fatih: Using Confidential Data for Domain Adaptation of Neural Machine Translation. In: *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*. 2020. s. 46-52 ISSN 0736-587X
2. ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Bellianum. Vydavateľstvo UMB v Banskej Bystrici. 2016. 146 s. ISBN 978-80-557-1170-6
3. HEGEROVÁ, Katarína: O jazykovej kultúre v právnických textoch. In: *Kultúra slova*. 1995. č.6, s. 332-337.[cit. 10. septembra 2025] Dostupné na: <https://www.juls.savba.sk/ediela/ks/1995/6/ks19956.html#id3>
4. KOLAŘÍKOVÁ, Linda, HORÁK, Filip: Umělá inteligence a právo. Praha: Wolters Kluwer ČR. 2020. 216 s. ISBN 978-80-7598-783-9
5. MUNKOVÁ, Daša, PETRÁŠ, Patrik: Strojový preklad založený na neurónových sieťach – sľubná cesta prekladu z analytických jazykov do flektívnej slovenčiny? In: *Slovenská reč*. 2023. č.1, s. 74-89
6. MUNKOVÁ, Daša, VAŇKO, Juraj a kol.: Mýliť sa je ľudské (ale aj strojové). Nitra: Univerzita Konštantína Filozofa v Nitre, 2017. 260 s. ISBN 978-80-558-1255-7
7. MUNKOVÁ, Daša.: Strojový preklad a translológia. Nitra: Univerzita Konštantína Filozofa v Nitre, 2020. 36 s. ISBN 978-80-558-1510-7
8. POPOVIČ, Anton: Originál/Preklad. Interpretačná terminológia. Bratislava: Tatran, 1983. 362 s. Pzn. aut. V publikácii absentuje ISBN.
9. PIKUS, Miroslav, HRABOVSKÝ, Richard: Umělá inteligencia na Slovensku: využitie, dosah na trh práce a etické aspekty. Bratislava: exe, a.s., 2020. 63 s. ISBN 978-80-974509-0-8

10. RAKŠÁNYIOVÁ, Jana et al.: Sociálny priestor súčasného právneho prekladu na Slovensku. In: *Úradný prekladateľ v slovenskom a európskom sociálnom priestore*. Bratislava: Vydavateľstvo univerzity Komenského v Bratislave, 2015. s. 7-55. ISBN 978-80-223-4034-2
11. RUSSEL, S.: Jako člověk. Umělá inteligence a problém jejího ovládání. Praha: Dokořán, 2021. 271 s. ISBN 978-80-7363-810-8
12. SCOTT, R. Juliette: Legal Translation Outsourced. Oxford: Oxford University Press, 2019. 216 s. ISBN 978-0-19-090000
13. ŠTEFKOVÁ, Marketa: Právny text v preklade. Translatologické aspekty právnej komunikácie v kombináciách z málo rozšírených jazykov. Bratislava: IURA EDITION, spol. s.r.o., 2013. 221 s. ISBN 978-80-8078-681-6
14. VANMASSENHOVE, E., HARDMEIER, CH., WAY, A.: Getting Gender Right in Neural Machine Translation. In: *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing* Brussel: Association for Computational Linguistics 2018. s. 3003-3008 [cit. 11. Septembra 2025]Dostupné na: <https://aclanthology.org/D18-1334.pdf>
15. VÉGH, Peter: Neurónové a fuzzy systémy (základy umelej inteligencie). Bratislava: Slovenská technická univerzita v Bratislave, 2014. 164 s. ISBN 978-80-227-42227-6
16. WRIGHT, Susan: Artificial Intelligence in Legal Translation at the Court of Justice of the European Union. In: *International Journal of Language and Law*. Vol.14. 2025. s.120-142. [cit. 15. Septembra 2025] Dostupné na : <http://www.languageandlaw.eu/jll/article/view/216/103>
17. WREDE, Oľga : Právny preklad a jeho translačné modely – teória a prax. Nitra: Univerzita Konštantína Filozofa v Nitre, 2021. 34 s. ISBN 978-80-558-1691-3

Odkazy na internetové zdroje

Rozhodnutia súdov spolkovej krajiny Severné Porýnie-Vestfálsko:

https://nrwe.justiz.nrw.de/lgs/kleve/lg_kleve/j2024/140_Ks_507 Js_734_22_1_23_Urteil_20231016.html [cit. 11. septembra 2025]

https://nrwe.justiz.nrw.de/arbg/duesseldorf/lag_duesseldorf/j2021/NRWE_LAG_D_sseeldorf_3_Sa_646_20_Urteil_20210427.html [cit. 11. septembra 2025]

Ostatné:

1.
https://www.umelainteligenciavpraxi.sk/download_portal_files/onlibai/oznamenie-umela-inteligencia-pre-europu.pdf [cit. 1. septembra 2025]
<https://bdue.de/mdue-online/vorsicht-uebersetzen-mit-chatgptco> [cit. 1. septembra 2025]

2.
 Commission_Guidelines_on_the_definition_of_an_artificial_intelligence_system_e

stablished_by_Regulation_EU_20241689_AI_Act_Slovak_zCiljgdxjf6iBU3mXnEPl1
5Vb64_118637.PDF [cit. 1. septembra 2025]

3.

<https://bdue.de/mdue-online/vorsicht-uebersetzen-mit-chatgptco>

[cit.

10.septembra 2025]

Kontaktné údaje

Mgr. Alexandra Debnárová, PhD.

alexandra.debnarova@flaw.uniba.sk

Ústav cudzojazyčnej právnej komunikácie

Právnická fakulta UK, Bratislava

USE OF CHATGPT IN TEACHING AND LEARNING LEGAL ENGLISH – FRIEND OR FOE?

Lucia Smolková¹

Abstract: Artificial intelligence (AI) has had a significant impact on English language teaching and learning. English for Specific Purposes (ESP), including Legal English, is no exception to that. Unlike Medical English or Business English, Legal English, as a type of ESP, is characterized by distinct features stemming from the legal system in which it operates. Differences between common law and civil law traditions, as well as concepts and terms with no direct equivalents across systems, make this variety of English particularly complex. The objective of this paper is to examine the impact of AI, in particular the ChatGPT, on the teaching and learning of Legal English by identifying some of the multiple opportunities it offers and some of the challenges it presents. It also aims to explore the evolving role of the Legal English teacher in the era of ChatGPT. The methodological approach of this paper is based on a review of selected scholarly papers and studies addressing the use of AI in English language education, and English for Specific Purposes (ESP) contexts and subsequent analysis of its application to Legal English teaching and learning to explore the implications for this specific branch of ESP.

Key words: ELT/L (English Language Teaching and Learning), ESP (English for Specific Purposes), Legal English, AI, ChatGPT

Introduction

AI has greatly affected the entire world of English language teaching and learning through various applications and tools that can be used both by learners and teachers. Studies conducted into the use of AI indicate that the use of AI in English language teaching is more prevalent than in any other taught subject.² A total of 76 per cent of English language teachers who participated in a global survey (including

¹ Univerzita Komenského v Bratislave, Právnická fakulta

² CROMPTON, Helen – EDMETT, Adam – ICHAPORIA, Neenaz – BURKE, Diane: AI and English language teaching: Affordances and challenges. In: British Journal of Educational Technology, Vol. 55 (2024), p. 2523.

1,348 teachers from 118 countries) report already using AI-powered tools for a range of tasks.³

Teaching English for Specific Purposes (ESP) is defined by its focus on catering to the students' specific linguistic needs. According to Boeru, a significant portion of the teaching content is either teacher-developed or adapted, posing a definite strain on the teacher to find and adapt current and relevant input which addresses both the lexical particularities of the students and their general language proficiency requirements.⁴ The impact of AI on ESP has also been explored and there are a number of studies that indicate the positive affect of AI in teaching and learning ESP, e.g. the improvement of students' English writing skills associated with improved self-efficacy and self-regulated learning, significant improvement in speaking, listening and reading after being exposed to AI technology, guiding teachers towards new creative opportunities and encouraging them to create personalised teaching activities, thus better addressing their learners' individual needs.

The learners of Legal English, as a type of ESP, require specialized language proficiency to navigate the complex and precise terminology used in legal texts and to be able to understand and use legal language accurately for successful communication within the legal profession.⁵ Legal English is also adapting as the technology that assists lawyers to do their jobs more efficiently is developing and growing in importance. Canham and Mason claim that it is no longer possible to learn Legal English effectively without keeping a close watch on developments in legal technology.⁶

ChatGPT, a general-purpose conversation chatbot released on November 30, 2022, by OpenAI, is the fastest-growing consumer internet application in the history.⁷ It has been acknowledged to positively impact the teaching and learning of ESP. ChatGPT emerges as a digital language learning assistant that supports language acquisition through personalised interactions and real-time feedback.⁸ Teachers and students increasingly recognize the complex opportunities and challenges associated with ChatGPT, its transformative impact on education is becoming more evident and it is

³ EDMETT, Adam - ICHAPORIA, Nikhil - CROMPTON, Helen - CRICHTON, Ronald: Artificial Intelligence and English Language Teaching: Preparing for the Future (2nd edition). British Council, 2023, p. 10.

⁴ BOERU, Mariana: Exploring the Use of AI Tools in Teaching English for Specific Purposes (ESP). In: Scientific Bulletin of Naval Academy, Vol. XXVII (2024), p. 93.

⁵ XATAMOVA, Nodiraxon - ASHUROV, Jahongir: The Future of Legal English Learning: Integrating AI into ESP Education. In: SPAST Reports, Vol. 1, Issue 7 (2024).

⁶ CANHAM, Natalie – MASON, Catherine: Advanced Legal English. Oxford: Routledge, 2017. p. 10.

⁷ CROMPTON, Helen - BURKE, Diane: The Educational Affordances and Challenges of ChatGPT: State of the Field. In: TechTrends, Vol. 68, Issue 2 (2024), p. 380.

⁸ SLAMET, Joko: Potential of ChatGPT as a digital language learning assistant: EFL teachers' and students' perceptions. In: Discover Artificial Intelligence, Vol. 4, Issue 46 (2024), p. 2.

believed that ChatGPT has the potential to revolutionize ELT/L through its advanced features, including personalization, instant feedback, and human-like conversational abilities. Generative AI models, such as ChatGPT, are also instrumental in redefining teacher roles and making student learning more interactive and personalised. ChatGPT can undoubtedly likewise promote teaching and learning Legal English in many ways. What role can ChatGPT play in Legal English teaching and learning and what are the challenges it poses? Due to the limited scope of this paper, we will restrict our analysis to selected opportunities and challenges.

Some opportunities ChatGPT provides in Legal English teaching and learning

Creating educational content

Despite the fact that Legal English textbooks are undoubtedly an important resource for Legal English teachers allowing them to easily design a syllabus with a clear organization and division into units or sections with the continuity of the units making the course of Legal English classes or courses well-organized, integrated and coherent,⁹ ChatGPT is considered to be an effective tool for developing instructional materials in English language education through generating high-quality dialogue materials suitable for English students.¹⁰

Similarly, Legal English teachers can use ChatGPT for generating educational materials, such as vocabulary-building exercises, namely gap-fill, error-correction, matching, multiple choice, word-derivation, synonym/paraphrasing exercises, etc. using authentic legal contexts which could otherwise be difficult to procure, especially in situations in which the Legal English teacher is not a lawyer himself/herself and thus does not have access to such authentic legal texts, and which the Legal English teacher would otherwise have to spend time designing himself/herself. Instructional materials for Legal English classes are often highly specific. For teachers/learners from civil law systems, this presents a challenge, as most textbooks are based on the common law system and are not always directly relevant for them to teach/practise the legal vocabulary that they need. Developing tailor-made materials that address their specific needs is therefore a time-consuming task for Legal English teachers.

However, a Legal English teacher should always carefully and critically evaluate any ChatGPT outputs used as educational content, especially when exact information (e.g. up-to-date statutory requirements) is required to be incorporated into the

⁹ LIUOLIENĖ, Alvyda - METIŪNIENĖ, Regina: Legal English and Adapted Legal Texts. In: SANTALKA: Filologija, Edukologija, 1 (2012), p. 57.

¹⁰ YOUNG, Julio Christian – SHISHIDO, Makoto: Investigating OpenAI's ChatGPT Potentials in Generating Chatbot's Dialogue for English as a Foreign Language Learning. In: *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 14, Issue 6 (2023), p. 66.

teaching materials, given the fact that ChatGPT tends to simplify its outputs. Law students and practising lawyers attending Legal English classes frequently expect, and sometimes explicitly request, that their Legal English classes also cover the realia specific to their own national legal system and not the legal system of common law countries. Therefore, translation of legal concepts or terms required by students does not have to be accurate when performed via ChatGPT given the differences between common law and civil law systems.

For example, in a speaking activity where Legal English students are asked to describe the statutory requirements for becoming an attorney in Slovakia, if using ChatGPT only to find this information,¹¹ and after comparing the chatbot's answer with the actual provisions of the Slovak Legal Profession Act, it becomes clear that the response is incomplete, and omits some statutory requirements. Consequently, neither the Legal English learner nor the teacher can rely solely on the chatbot and must verify the accuracy of the output.

Adapting educational content to Legal English learners' proficiency level and expertise

Creation of customized educational content by ChatGPT has also been explored. Bonner et al. stated that ChatGPT can be highly beneficial as it is capable of producing personalised learner-centered content by drawing on its extensive linguistic knowledge, thereby enabling teachers to deliver more targeted and effective instruction.¹² Koraishi also explored how ChatGPT can be used to streamline the creation of engaging and contextually appropriate learning materials tailored to individual learner needs, referring to the fact that such materials can be created in accordance with a specific Common European Framework of Reference for Languages (CEFR) proficiency level. Furthermore, he also highlighted the possibility of effortless adaptation of an already created text for use with a different CEFR proficiency level by simply prompting ChatGPT with different parameters or providing additional guidance, thus maximizing the utility of the generated content.¹³

Legal English learners often have varying levels of general English proficiency, ranging from A2 to C1. Legal English teachers can use ChatGPT to easily customize

¹¹ The following prompt has been used in this respect: "What are the exact statutory requirements for becoming an attorney in Slovakia under the current law?"

¹² BONNER, Euan et al.: Large Language Model-Based Artificial Intelligence in the Language Classroom: Practical Ideas for Teaching. In: *Teaching English with Technology*, Vol. 23, Issue 1, (2023), p. 23.

¹³ KORAISHI, Osama: Teaching English in the Age of AI: Embracing ChatGPT to Optimize EFL Materials and Assessment. In: *Language Education & Technology (LET Journal)*, Vol. 3, Issue 1 (2023), p. 56.

the educational content to target the relevant proficiency level, for example by: (i) adjusting vocabulary complexity by using simpler or more advanced legal terminology (e.g. for lower levels, replacing *null and void* with *not legally valid*), (ii) modifying sentence structure by using shorter and simpler sentences, or by abridging authentic legal documents for lower levels, and by using longer, more complex sentences mirroring authentic legal texts for higher levels, (iii) controlling exercise difficulty (e.g. gap-fill exercise with word banks for lower levels and open-ended gap-fill exercise for higher levels), (iv) selecting contexts (e.g. lower levels can deal with easy everyday legal scenarios whereas higher levels can deal with more complex areas like case law, interpreting contractual provisions, drafting court submissions, etc.).

As for expertise, many Legal English learners, especially legal practitioners, often request that the syllabus focus exclusively on a limited range of legal topics reflecting their area of expertise. ChatGPT can likewise adapt to such needs by generating materials, exercises, and examples tailored to specific fields of law, such as contract law, intellectual property, or criminal procedure.

More accessible Legal English terminology – no need for dictionaries anymore?

In a study conducted by Lew, Ptasznik and Wolfer, the results showed that ChatGPT is a viable alternative to traditional dictionaries in both production and reception tasks in English. In particular, the results indicate that ChatGPT was significantly more effective than monolingual and bilingual dictionaries in productive tasks, i.e. tasks requiring learners to generate and use target items in context. In receptive tasks, focused on comprehension, ChatGPT outperformed the monolingual dictionary but did not surpass the bilingual dictionary.¹⁴

ChatGPT has proven to be a great tool in identifying different contexts in which Legal English terminology is used. Furthermore, it provides several possible translations of legal terms, so that there is actually no need to consult a dictionary. Legal English terminology becomes more accessible, and Legal English learners can understand the usage of legal terms in different legal settings and avoid any possible mistranslation.

For example, when exploring how the frequently used Slovak legal term *výkon* can be translated into English,¹⁵ ChatGPT provided a number of contexts, such as *výkon rozhodnutia*, *výkon funkcie*, *výkon práv*, *výkon trestu odňatia slobody*, *výkon*

¹⁴ LEW, Robert – PTASZNIK, Bartosz – WOLFER, Sascha: The effectiveness of ChatGPT as a lexical tool for English, compared with a bilingual dictionary and a monolingual learner's dictionary. In: Humanities and Social Sciences Communications, 11, 1324 (2024), p. 8.

¹⁵ The following prompt: *How do you translate the Slovak legal term "výkon" into English?* has been used.

vlastníckeho práva, výkon verejnej moci and corresponding translation solutions *enforcement/execution of a decision, performance/discharge of duties, exercise of rights, imprisonment, exercise of ownership rights, exercise of public authority/powers*. ChatGPT thus has the ability to provide context-sensitive legal terminology by analysing the source legal term within its legal context and by selecting the most appropriate English equivalent, including recognising the nuances between similar terms. This is particularly valuable in translating where a single legal term, such as *výkon*, may have multiple meanings ranging from enforcement of court decisions to the exercise of rights or the performance of duties.

Furthermore, ChatGPT can be a valuable tool for identifying English legal terminology in cases where the exact term for a particular legal concept is not known or cannot be found in a legal dictionary. By providing a description of the concept and its context, ChatGPT can suggest an existing or appropriate English equivalent, often offering several alternatives with explanations of their nuances. This process facilitates the quick identification of the corresponding legal term—especially when legal dictionaries do not contain the term in question—or confirms that such a term does not exist within the legal system of common law countries.

For example, during a Legal English class for legal practitioners specializing in criminal law, the Slovak legal term *dozorový prokurátor* in the context of prisons needed to be translated as part of a speaking activity. The legal dictionary did not provide a suitable translation.¹⁶ In the search for an adequate equivalent, we provided ChatGPT with the legal definition of the concept of *dozorový prokurátor* stemming from Slovak Act No. 153/2001 Coll. on Prosecution “*this prosecutor exercises supervision over the observance of the law in places where persons deprived of their liberty are held, or where persons whose personal freedom is restricted based on a court decision or by another competent state authority are detained*” to try to match it to the corresponding concept in the UK Prison Act 1952.¹⁷ After conducting research into the concept of *dozorový prokurátor* in the UK Prison Act 1952, it was found that the prison oversight of lawfulness under the Prison Act 1952 is not conducted by a prosecutor but there are different inspection mechanisms. ChatGPT offered several explanatory translation solutions (e.g. prosecutor exercising supervisory functions over places of detention, prosecutor responsible for overseeing lawfulness in detention facilities, public prosecutor with oversight of detention conditions) noting that no single, universally standardized English term exists. Subsequently, after being instructed to provide a short, formal term, it proposed a concise option - *detention oversight prosecutor*. As we can see in the aforementioned example,

¹⁶ CHROMÁ, Marta: Česko-anglický právnický slovník. Praha: Leda, 2011. 488 s.

¹⁷ UK Prison Act 1952. Available online at: <https://www.legislation.gov.uk/ukpga/Geo6and1Eliz2/15-16/52/contents>.

ChatGPT has the ability to recognize when a direct translation is unavailable and to provide function-based paraphrases conveying the legal role. It is also able to move from descriptive to terminologically efficient phrasing while preserving the legal accuracy.

Better comprehension of complex and overcomplicated Legal English texts

The use of authentic legal text in a Legal English classroom can significantly contribute to the learning experience.¹⁸ However, the language used in them is many times too complicated with too much legalese making it thus harder for learners to decipher the exact meaning.

ChatGPT can easily convert legalese used in many Legal English texts into a plain English text. Mason, a popular proponent of plain English, often refers to the fact that in today's world, legalese is completely unnecessary in many instances.¹⁹ In order to avoid contracts in English that "look as if they were possibly drafted by Shakespeare when he was having a bad day,"²⁰ Legal English learners can easily employ ChatGPT to help them understand difficult legal texts – ChatGPT can easily convert complex, incomprehensible, and overcomplicated texts with too much legalese into plain English after using the prompts for ChatGPT, such as (i) avoid legal Latin, (ii) use the active voice and not the passive, (iii) do not use archaic words like *heretofore*, etc., (iv) do not use list of synonyms in one sentence that mean the same thing, e.g. *alter, amend, vary, modify*, (v) keep your sentences short.²¹

Furthermore, ChatGPT could be used to summarize a complicated Legal English text quickly and efficiently and, as Bonner suggests, give learners not only a model of a well-written summary, but also provide Legal English learners with a level-appropriate text. At the same time, this capability of ChatGPT could also be used to check Legal English learners' summarization skills by comparing their summaries to the ChatGPT-generated ones.²²

Assisting Legal English learners in developing their writing skills

The potential of ChatGPT to improve the writing skills of English language learners has been highlighted in numerous studies. ChatGPT helps in planning by aiding

¹⁸ LIUOLIENĖ, Alvyda - METIŪNIENĖ, Regina: Legal English and Adapted Legal Texts. In: SANTALKA: Filologija, Edukologija, 1 (2012), p. 5.

¹⁹ CANHAM, Natalie – MASON, Catherine: Advanced Legal English. Oxford: Routledge, 2017.p. 8.

²⁰ CANHAM, Natalie – MASON, Catherine: Advanced Legal English. Oxford: Routledge, 2017.p. 8.

²¹ CANHAM, Natalie – MASON, Catherine: Advanced Legal English. Oxford: Routledge, 2017. p.9.

²² BONNER, Euan et al.: Large Language Model-Based Artificial Intelligence in the Language Classroom: Practical Ideas for Teaching. In: *Teaching English with Technology*, Vol. 23, Issue 1 (2023), p. 30.

students think deeply, generate ideas, and organize them coherently. During revision, it helps to produce polished writing. Students also reported enhanced creative thinking and improved essay coherence and readability.²³ Similarly, it has also been found that AI tools in general significantly enhanced students' writing proficiency and motivation through its ability to efficiently and effectively identify and correct grammatical errors, awkward sentence structures, stilted syntax, and incorrect punctuation or spelling. ChatGPT can also be used to brainstorm writing topics and content to help facilitate the writing process.²⁴

Given the fact that writing is central to legal communication, practising writing skills in Legal English classes is crucial. Lawyers spend much of their professional life writing contracts, pleadings, memos, client letters, emails, judgements or various reports. Legal writing is built on precision and clarity and ChatGPT can be a very useful tool in this regard by providing students with instant feedback on grammar, coherence, and style, generating model texts for comparison, or assisting learners in revising their drafts for greater clarity and accuracy. Moreover, ChatGPT can simulate authentic legal communication tasks, such as drafting a client letter or summarising a case, thereby enabling students to practise writing in a safe, low-stakes environment. Such practice helps learners refine their ability to convey complex legal ideas in clear and professional English.

Some challenges associated with the use of ChatGPT in Legal English teaching and learning

According to the study conducted by Crompton et al., when it comes to challenges of using AI in English language teaching and learning, such challenges do not appear to be well reported, and there is more focus on affordances of AI systems in English language teaching and learning.²⁵ While ChatGPT is being championed as a tool that has the potential to transform and revolutionize education, including English language teaching and learning, there are several concerns and risks involved in its use, also with respect to Legal English.

²³ For example YANG, Yang: An Empirical Study on the Impact of ChatGPT on Writing Proficiency in Chinese EFL Learners. In: Curriculum and Teaching Methodology, Vol. 7 (2024), p. 176.

²⁴ ZHAI, Xiaoming: ChatGPT User Experience: Implications for Education. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4312418.

²⁵ CROMPTON, Helen – EDMETT, Adam – ICHAPORIA, Neenaz – BURKE, Diane: AI and English language teaching: Affordances and challenges. In: British Journal of Educational Technology, Vol. 55 (2024), p. 2522.

ChatGPT literacy and keeping up-to date with frequent changes

Technological advancements are occurring at such a rapid pace that the primary challenge lies not in a lack of tools or resources for improving the educational system, but in the difficulty of keeping up with constant innovations.²⁶ Crompton et al. also claim that the rapid development of the technology will provide a constant challenge for up-to-date AI literacy.²⁷ According to the global teacher survey very few teachers report having had enough training on how to incorporate AI into teaching.²⁸ This concern also applies to tools such as ChatGPT, which are updated frequently and whose capabilities, limitations, and usage policies develop rapidly. For teachers, this means that effective integration of ChatGPT into teaching requires not only language-pedagogical expertise but also continuous monitoring of how the tool changes over time.

There is a need for developing ChatGPT literacy among both teachers and learners. Ma et al. introduced the concept of ChatGPT literacy within language education stating that by exploring the appropriate use, potential pitfalls, and pedagogical integration of ChatGPT, teachers can harness its benefits while mitigating its limitations.²⁹ Ma et al. state that ChatGPT literacy should involve critically evaluating the response provided by ChatGPT, designing effective prompts, adopting it for assessment, and ensuring its ethical use.

ChatGPT literacy of a Legal English teacher could, in light of the aforementioned definition, translate as having the ability to use ChatGPT to enrich Legal English teaching while maintaining professional accuracy and ethical standards. This includes knowing how to design precise prompts to generate authentic legal texts, critically evaluating ChatGPT's outputs for accuracy and appropriateness, especially in cases of translation of legal texts, and integrating the tool into lessons and assessments in ways that support student learning without leading to their over-reliance on ChatGPT. Therefore, it is crucial to prioritize professional development programs that would equip teachers, including Legal English teachers, with not only technical understanding but also pedagogical strategies for integrating ChatGPT effectively into curricula.

²⁶ DUBOVYK, Olena: Innovations in ESP Teaching and Learning Practices. In: Humanities Studios: Pedagogy, Psychology, Philosophy, Vol. 12, Issue 4 (2024), p. 2.

²⁷ CROMPTON, Helen – EDMETT, Adam – ICHAPORIA, Neenaz – BURKE, Diane: AI and English language teaching: Affordances and challenges. In: British Journal of Educational Technology, Vol. 55 (2024), p. 2523.

²⁸ EDMETT, Adam - ICHAPORIA, Nikhil - CROMPTON, Helen - CRICHTON, Ronald: Artificial Intelligence and English Language Teaching: Preparing for the Future (2nd edition). British Council, 2023. p. 11.

²⁹ MA, Qing et al.: Exploring ChatGPT Literacy in Language Education: A Global Perspective and Comprehensive Approach. In: Computers and Education: Artificial Intelligence, 7 (2024), p.3.

For a Legal English student, ChatGPT literacy means being able to use ChatGPT as a supportive learning tool to practice Legal English while developing critical thinking and professional responsibility. This involves designing clear prompts to get useful practice materials, assessing the reliability and accuracy of ChatGPT-generated legal texts, and using ChatGPT for feedback on writing or simulations such as client consultations. It also requires ethical awareness—recognising when ChatGPT support is appropriate, and when authentic work is essential.

Need for new roles and competencies of Legal English teachers in the ChatGPT era

According to UNESCO's AI competency framework for teachers, it is teachers who are the primary users of AI in education, and who are expected to be the designers and facilitators of students' learning with AI, the guardians of safe and ethical practice across AI-rich educational environments, and who act as role models for lifelong learning about AI.³⁰

Deng also notes that English educators in general face unprecedented challenges in terms of the diversity of teaching resources and the adoption of new teaching models. He emphasizes that ignoring these challenges or clinging rigidly to old methods risks falling behind and remaining passive, whereas exploring new approaches in English classroom teaching can provide a breakthrough to move beyond traditional practices.³¹

Therefore, what we see as one of the challenges of using ChatGPT in teaching and learning Legal English is for the Legal English teachers to embrace their new roles and competencies. One such competence is prompt engineering, which is pivotal for effective interaction with ChatGPT in educational contexts, given the fact that the core function of ChatGPT lies in supplying input or posing questions to elicit useful responses.³² It is therefore important for Legal English teachers to become familiar with the prompt design strategies that can draw out the most pertinent replies from ChatGPT and effectively interact with it.

In practice, in Legal English classes, effective prompt designing could be "Draft a simple lease agreement between a landlord and a tenant for a one-year rental of an apartment in London. Include clauses on rent, repairs, and termination" instead of "Write a contract." Another example could be "Explain the tort of trespass to land in

³⁰ UNESCO. *AI competency framework for teachers*. 2024. p. 3. Available online at: <https://unesdoc.unesco.org/ark:/48223/pf0000391104>.

³¹ DENG, Yongping: Challenges of College English Teaching in the AI Era. In: *Sino-US English Teaching*. Vol. 22, Issue 4 (2025), p. 130.

³² MA, Qing et al.: Exploring ChatGPT Literacy in Language Education: A Global Perspective and Comprehensive Approach. In: *Computers and Education: Artificial Intelligence*, 7 (2024), p.3.

English law in simple terms suitable for first-year law students. Provide one short real-life example and one case reference” instead of “Explain trespass”, etc. It is crucial to choose the right words to yield the desired outcome.

Due to the specific nature of Legal English, in particular the significant differences between common law and civil law, we could expect that a very important role of a Legal English teacher will be mainly to correct inaccurate translations generated by ChatGPT. In practice, this is currently quite a frequent phenomenon witnessed by Legal English translators. In cases where there is not an equivalent legal term due to different legal systems, ChatGPT-generated translation is often inaccurate and need to be corrected. However, we could wonder whether, with the constantly developing technologies, this problem will also be solved.

Furthermore, another Legal English teacher's role will be to motivate and encourage students to complete their assignments without using ChatGPT, or with only limited use of it, so as not to deteriorate in terms of creativity, critical thinking, concentration, and determination. Reading, understanding, and interpreting Legal English texts can be challenging on the one hand, but a great practice of a number of skills on the other hand. Overuse of ChatGPT and overreliance on it has the potential to hinder the development of students' critical thinking. Teachers should be able to guide their students towards a “healthy use” of ChatGPT such as using it to gather preliminary information that they would have to cross-check with statutes, case law, and commentary to verify accuracy, critically evaluate sources, and identify gaps or contradictions, or consider alternative interpretations. Encouraging students to use ChatGPT as an assistant rather than a generator of their work helps maintain the balance between technological support and the development of essential skills. When learners rely on ChatGPT to generate full assignments, they risk bypassing critical processes such as formulating arguments, practicing legal vocabulary, and structuring texts logically. This kind of overreliance may diminish creativity, critical thinking, and the ability to work independently—all of which are necessary for legal professionals.

Finally, Legal English teachers will have to make a great effort to identify any work generated by ChatGPT. It is becoming more difficult to distinguish between ChatGPT-generated and learner-generated content, which consequently complicates assessment. Therefore, teachers must consider new strategies for assessment, such as designing tasks which encourage demonstration of critical thinking and legal reasoning in ways that are less easily replicated by ChatGPT.

Conclusion

The incorporation of ChatGPT in English teaching and learning processes has become inevitable. The opportunities that ChatGPT brings into Legal English

teaching and learning are wide-ranging: from generating authentic and level-appropriate teaching materials, through better comprehension of complex legal texts, to improving access to legal terminology and enhancing legal writing. Its ability to adapt resources to different learner needs and legal contexts makes it a valuable tool in modern Legal English pedagogy.

The role of Legal English teachers has changed dramatically in the ChatGPT era and they are facing the challenges of their role transformation in order to adapt to these new developments. We believe that their expertise remains vital in clarifying legal concepts and correcting inaccurate information provided by ChatGPT. Another important role that they will have to embrace is guiding their Legal English learners toward critical, responsible, and balanced use of ChatGPT so that their Legal English learners will not become heavily reliant on its outputs and thus have their creativity and critical thinking deteriorated.

ChatGPT cannot replace the Legal English teacher's human role as motivator and facilitator. The challenge—and opportunity—for Legal English teachers in the AI era is therefore not to compete with ChatGPT, but to use it as a supportive tool. It should therefore be regarded not as a substitute for teachers, but as a helpful tool that, when used critically and responsibly, can contribute to the learning process and make Legal English education more efficient, flexible, and engaging.

As for Legal English learners, their ChatGPT literacy should primarily focus on using the tool as a supportive aid for practice and learning, critically evaluating generated legal content for accuracy and reliability, and developing the knowledge when their authentic and independent work is necessary because if learners depend on ChatGPT excessively for translating or generating legal texts, or examples, they may fail to develop critical skills such as legal writing, vocabulary acquisition, and understanding of legal reasoning necessary for their legal profession.

Bibliography

1. BOERU, Mariana: Exploring the Use of AI Tools in Teaching English for Specific Purposes (ESP). In: Scientific Bulletin of Naval Academy, Vol. XXVII (2024), p. 91 – 96. DOI:10.21279/1454-864X-24-l1-013.
2. BONNER, Evan et al.: Large Language Model-Based Artificial Intelligence in the Language Classroom: Practical Ideas for Teaching. In: *Teaching English with Technology*, Vol. 23, No. 1, (2023), p. 23-41. DOI: 10.56297/BKAM1691/WIEO1749.
3. CANHAM, Natalie – MASON, Catherine: Advanced Legal English. Oxford: Routledge, 2017. 272 p. ISBN-13: 978-1789267112.
4. CHROMÁ, Marta: Česko-anglický právní slovník. Praha: Leda, 2011. 488 p. ISBN 978-80-7335-249-3.

5. CROMPTON, Helen - BURKE, Diane: The Educational Affordances and Challenges of ChatGPT: State of the Field. In: *TechTrends*, Vol. 68, Issue 2 (2024), p. 380-392. <https://doi.org/10.1007/s11528-024-00939-0>.
6. CROMPTON, Helen – EDMETT, Adam – ICHAPORIA, Neenaz – BURKE, Diane: AI and English language teaching: Affordances and challenges. In: *British Journal of Educational Technology*, Vol. 55 (2024), p. 2503-2529. <https://doi.org/10.1111/bjet.13460>.
7. DENG, Yongping: Challenges of College English Teaching in the AI Era. In: *Sino-US English Teaching*. Vol. 22, Issue 4 (2025), p. 129–132. <https://doi.org/10.17265/1539-8072/2025.04.002>.
8. DUBOVYK, Olena: Innovations in ESP Teaching and Learning Practices. In: *Humanities Studios: Pedagogy, Psychology, Philosophy*, Vol. 12, Issue 4 (2024), p. 23-33. DOI: 10.31548/hspedagog/4.2024.23.
9. EDMETT, Adam - ICHAPORIA, Nikhil - CROMPTON, Helen - CRICHTON, Ronald: Artificial Intelligence and English Language Teaching: Preparing for the Future (2nd edition). British Council, 2023. <https://doi.org/10.57884/78EA-3C69>.
10. KORAISHI, Osama: Teaching English in the Age of AI: Embracing ChatGPT to Optimize EFL Materials and Assessment. In: *Language Education & Technology (LET Journal)*, Vol. 3, No. 1 (2023), p. 55-72. https://langedutech.com/letjournal/index.php/let/article/view/48?utm_source=chatgpt.com.
11. LEW, Robert – PTASZNIK, Bartosz – WOLFER, Sascha: The effectiveness of ChatGPT as a lexical tool for English, compared with a bilingual dictionary and a monolingual learner's dictionary. In: *Humanities and Social Sciences Communications*, 11, 1324 (2024). <https://doi.org/10.1057/s41599-024-03775-y>.
12. LIUOLIENĖ, Alvyda - METIŪNIENĖ, Regina: Legal English and Adapted Legal Texts. In: *SANTALKA: Filologija, Edukologija*, 1 (2012), p. 56 – 64. ISSN 1822-430X print/1822-4318 online.
13. MA, Qing et al.: Exploring ChatGPT Literacy in Language Education: A Global Perspective and Comprehensive Approach. In: *Computers and Education: Artificial Intelligence*, 7 (2024), p. 1-10. DOI:10.1016/j.caeai.2024.100278.
14. NAZEER, Imran – YASMIN, Saima – KHAN, Nida Mushtaq: English Language Acquisition through ChatGPT: A Study on Personalised Conversational Practice and Feedback. In: *Journal of Applied Linguistics and TESOL*, Vol. 7, Issue 4 (2024), p. 1076 – 1088. <https://doi.org/10.2139/ssrn.5079704>.
15. SLAMET, Joko: Potential of ChatGPT as a digital language learning assistant: EFL teachers' and students' perceptions. In: *Discover Artificial Intelligence*, Vol. 4, Issue 46 (2024), p. 1-15. <https://doi.org/10.1007/s44163-024-00143-2>.

16. SUN, Grace - HOELSCHER, Stephanie: The ChatGPT Storm and What Faculty Can Do. In: *Nurse Educator*, Vol. 48, Issue 3 (2023), p. 119-124. <https://doi.org/10.1097/NNE.0000000000001390>.
17. TOPSAKAL, Oguzhan - TOPSAKAL, Elif: Framework for a Foreign Language Teaching Software for Children Utilizing AR, Voicebots and ChatGPT (Large Language Models). In: *The Journal of Cognitive Systems*, Vol. 7, Issue 2 (2022), p. 33 - 38. <https://doi.org/10.52876/jcs.1227392>.
18. UK Prison Act 1952. Available online at: <https://www.legislation.gov.uk/ukpga/Geo6and1Eliz2/15-16/52/contents>.
19. UNESCO. AI competency framework for teachers. 2024. p. 3. Available online at: <https://unesdoc.unesco.org/ark:/48223/pf0000391104>.
20. XATAMOVA, Nodiraxon - ASHUROV, Jahongir: The Future of Legal English Learning: Integrating AI into ESP Education. In: *SPAST Reports*, Vol. 1, Issue 7 (2024). <https://doi.org/10.69848/sreports.v1i7.5081>.
21. YOUNG, Julio Christian – SHISHIDO, Makoto: Investigating OpenAI's ChatGPT Potentials in Generating Chatbot's Dialogue for English as a Foreign Language Learning. In: *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 14, Issue 6 (2023), p. 65-72. DOI: 10.14569/IJACSA.2023.0140607.
22. ZHAI, Xiaoming: ChatGPT User Experience: Implications for Education. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4312418.

Contact details

JUDr. Lucia Smolková, PhD.

lucia.smolkova@flaw.uniba.sk

Faculty of Law, Comenius University in Bratislava

AI PODPORENÉ PRÍSTUPY K UČENIU SA ANGLICKÉHO JAZYKA PRE ŠPECIFICKÉ ÚČELY: ZAMERANIE NA PRÁVNÚ TERMINOLÓGIU

AI-ENHANCED APPROACHES FOR LEARNING ENGLISH FOR SPECIFIC PURPOSES: A FOCUS ON LEGAL TERMINOLOGY

Iva Dudášová¹

Abstrakt: Rozvoj umelej inteligencie predstavuje míľnik v oblasti učenia sa odborného anglického jazyka. Vo výučbe právneho jazyka sa otvárajú nové dimenzie didaktiky, ale aj možnosti objavovania a precvičovania právneho jazyka a terminológie, ktoré presahujú rámce tradičných prístupov v jeho osvojovaní. Príspevok analyzuje potenciál umelej inteligencie pri učení sa anglického jazyka pre špecifické účely so zreteľom na efektivitu a personalizáciu učenia sa právnej terminológie, špecifické lingvistické využitia jazykových modelov v právnom diskurze a predstavenie možností a nástrojov učenia sa, ktoré ponúka generatívna umelá inteligencia cez adaptívne AI platformy. Prínosom článku je aj identifikácia negatívnych dopadov využívania AI zo strany študentov od prílišného spoliehania sa na výsledky ponúkané AI, cez množiace sa otázky ohľadom etického využívania umelej inteligencie až po potenciálne zásahy do kreativity študentov učiacich sa aplikovať a používať právnu terminológiu v rámci právneho diskurzu. Článok ponúka nový pohľad na kľúčový význam správneho načasovania využívania umelej inteligencie v kreatívnom procese učenia sa každého študenta a upresní vhodné a nevhodné časové okná na jej využitie.

Kľúčové slová: anglický jazyk pre špecifické účely, umelá inteligencia, právna terminológia, právny diskurz

Abstract: The development of artificial intelligence represents a milestone in the field of learning professional English. New dimensions of didactics are opening up in the teaching of legal language, as well as opportunities for discovering and practicing legal language and terminology that go beyond the scope of traditional approaches to its acquisition. This article analyses the potential of artificial intelligence in learning English for specific purposes with regard to the effectiveness and personalisation of acquiring legal terminology,

¹ Ústav cudzojazyčnej právnej komunikácie, PraF UK.

specific linguistics uses of language models in legal discourse, and the presentation of learning opportunities and tools offered by generative artificial intelligence through adaptive AI platforms. The article also identifies the negative impacts of AI use by students, ranging from over-reliance on AI results, to growing questions about the ethical use of artificial intelligence, to potential interference with the creativity of students learning to apply and use legal terminology in legal discourse. The article offers a new perspective on the key importance of the right timing for using artificial intelligence in the creative learning process of each student and specifies appropriate and inappropriate timeframes for its use.

Key words: English for specific purposes, artificial intelligence, legal terminology, legal discourse

Úvod

Učenie a učenie sa sú dve strany jednej mince. V prípade právnej terminológie stojí na jednej strane pedagóg lingvista, ktorý sa musí moderne vysporiadať s výučbovým procesom a s novými možnosťami, ktoré prináša umelá inteligencia a na druhej strane sú študenti, ktorí sa pripravujú na budúce právnické povolanie v kritických časoch. Tie sa podľa väčšiny prognóz týkajú právnickej profesie ako takej,² ale aj právnického vzdelávania³ zásadne ovplyvneného umelou inteligenciou (AI), ktorá je vnímaná ako prísľub, ale aj ako hrozba. Akokoľvek je však AI vnímaná, už je tu prítomná a je potrebné sa adaptovať. Úvodnou otázkou tohto článku je, akým spôsobom je možné vyrovnať sa so zmenami v čase, kedy sa stáva efektívna integrácia technológií pri učení sa nevyhnutnou a to pri zachovaní (alebo zvýšení) integrity, etiky a dôvery.

V rámci článku zúžime pole záujmu na tú stranu mince, ktorá patrí prístupu študentstva a stratégie učenia sa s podporou AI určíme zodpovedaním na otázky **pre**

² Medzinárodná advokátska komora (IBA) vydala v septembri 2024 správu s názvom *The Future is now: Artificial Intelligence and the Legal Profession*, kde zdôraznila nevyhnutnosť analyzovať dopady AI na právnickú profesiu s ohľadom na to, že je prvýkrát dostupná technológia, ktorá okrem iného umožňuje asistovať pri príprave komplexných právnych dokumentov a právnej rešerši. Dostupné na: <https://www.ibanet.org/document?id=The-future-is-now-AI-and-the-legal-profession-report>.

citované dňa 10.09.2025. Podobne sa vyjadrili aj v Law Society of England and Wales, kde uviedli, že AI dotvára budúcnosť právnej praxe cez transformatívnu úlohu v právnych operáciách, rešerši, dostupnosť cez tzv. chatbots, analýzy rizík a prediktívne analýzy. Dostupné na <https://www.lawsociety.org.uk/topics/ai-and-lawtech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>.

³ Viac v DILIDZE, Tatia: *The Evolving Role of Artificial Intelligence in Legal Education and Research*. In: Law and World, 2025, Roč. 11 č.33, s. 92-93.

koho sú tieto moderné stratégie určené, **aké jazykové osobitosti** je možné a užitočné precvičovať s AI, **s akými nástrojmi** vieme splniť účel týchto stratégií a zodpovedať otázku **ako neohýbať** stratégie a nevystavovať sa rizikám, ktoré existencia AI priniesla do vysokoškolského procesu nabierania nových vedomostí a aktívneho učenia sa.

Navrhujeme AI podporené prístupy a stratégie k učeniu sa anglického jazyka pre špecifické účely so zameraním na právnu terminológiu. Nadchádzajúce časti prezentujú v prvom rade adaptívne platformy na učenie sa v kontexte reality univerzitných štúdií a to v mnohopočetných skupinách študentov, kde je individualizovaný prístup vyučujúceho často nemožný. V ďalšej časti uvedieme možnosti špecifických oblastí, kde AI nástroje môžu uľahčiť osvojovanie si terminológie z rôznych oblastí práva a systémov, kontextové učenie s právnymi zdrojmi a práce s korpusom textov. Posledná časť sa bude venovať stratégiám prevencie negatívnych dopadov využívania AI študentmi (pokles kritického myslenia, falošný pocit porozumenia, strata kreativity či strata schopnosti pamätať si).

Lingvistické využitia jazykových modelov v právnom diskurze

Umelá inteligencia umožnila a zároveň si vyžiadala, aby sa výučba práva aktualizovala a bola v súlade s celospoločenskými zmenami. Aj študenti majú v úmysle a záujem prispôbiť sa a zapojiť sa do vývoja nových metód hodnotenia s cieľom podporiť samostatné štúdium práva, a v tomto smere by učitelia mali podniknúť všetky možné kroky, aby študenti mohli plne zažiť právo prostredníctvom technológií alebo umelej inteligencie v každodennej práci akademických činností.⁴

Využitie umelej inteligencie v právnej oblasti zlepšuje učenie sa študentov prostredníctvom niektorých špecifických konverzačných chatbotov, ako je napr. ChatGPT, ktorý umožňuje alebo podporuje rozvoj určitých právnych zručností ako je argumentácia.⁵ Ak aj chceme nájsť prepojenie medzi tradičným učením postavenom na Sokratovej metóde, ktorá je založená na dialógu medzi učiteľom a študentom v cieľom stimulovať ich schopnosti analyzovať právne prípady, objasňovať svoje uvažovanie a obhajovať svoje argumenty a kritické myslenie, tak aj v situácii prevrátených rolí môže študent využiť AI ako osobného Sokratovského tútora a pomyselného nesúdiaceho učiteľa, ktorý bude kriticky analyzovať právne

⁴ WU, Junyan – TANG, Wenjun: *Reform Method of University Legal Education Based on Artificial Intelligence and Wireless Communication*. In: *Wireless Communications and Mobile Computing*, 2022. číslo článku 2574911. s. 5.

⁵ AGUILAR, Héctor González: *Some Trends on Artificial Intelligence in Legal Education*. In *Proceedings of the 22nd LACCEI International Multi-Conference for Engineering, Education and Technology (LACCEI 2024): Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0*, Latin American and Caribbean Consortium of Engineering Institutions, (2024), s.6.

uvažovanie študenta bez spoločenských brzd. Môže tak robiť ako osoba, ktorá sa učí klásť dostatočne presné a trefné otázky smerujúce na AI, viesť dialóg a v procese ujasňovať, čo mu osobne nie je zrejmé a trénovať sa v argumentácii.

Argumentácia nie je jedinou oblasťou, kde je umelá inteligencia využiteľná. Z hľadiska učenia sa právnického anglického jazyka je uplatniteľná v najmenej štyroch kľúčových oblastiach. Právny jazyk je známy svojimi osobitnými **lexikálnymi štruktúrami** (ustálenými jazykovými spojeniami známymi ako *collocations* a polysémiou), pričom AI môže na vyžiadanie študentom generovať glosáre a opakovacie karty na precvičovanie slovnej zásoby v kontexte rôznych oblastí práva (zmluvné právo, trestné právo, občianske právo a iné).⁶

Ďalším znakom odborného právneho jazyka sú **morfosyntaktické štruktúry**: komplexné vetné štruktúry so včlenenými vetami, s využitím trpného rodu alebo podmieňovacieho spôsobu. Výskum uskutočnený na sto štyridsiatich siedmich študentoch práva v druhom a treťom ročníku preukázal mieru subjektívnej náročnosti v pochopení viet so zvyšujúcim sa počtom včlenených podradovacích viet v rámci dlhých súvetí vyselektovaných z autentických právnych textov pracovných a nájomných zmlúv. Napriek tomu, že cieľom výskumu bolo porovnať vnímanie náročnosti študentov druhého ročníka (ktorí ešte prevažne neboli vystavení práci s reálnymi zmluvami, ale učili sa terminológiu rôznych oblastí práva) so študentmi tretieho ročníka (ktorí mali za sebou 2 semestre prekladového semináru a kontaktu s reálnymi zmluvami), z výskumu vzišlo, že študenti ako nerodení hovoriaci potrebujú pomoc s orientáciou v rámci komplexných vetných štruktúr, ktoré majú často v sebe viac ako 6 včlenených, navzájom prepojených a podmienených štruktúr. Študenti tretieho ročníka vykazovali subjektívne vyššiu mieru porozumenia pri všetkých vetách rôznej komplexnosti a zároveň nižšiu mieru chybovosti pri kontrolných otázkach⁷ a so správnym používaním techník učenia sa, sa dá tento progres znásobiť. Umelá inteligencia im môže v prípade potreby pomôcť analyzovať a rozobrať dlhé ustanovenia, ktoré majú potenciál viesť k nedorozumeniam, uľahčiť pochopenie významu a poukázať na výzvy pri právnom písaní zmlúv tzv. *drafting*.

Ďalšími jazykovými aspektami, ktoré sú relevantné z hľadiska naberania anglickej právnickej terminológie sú **pragmatické funkcie**, ako je voľba vhodného registra jazyka pričom umelá inteligencia vie dať študentovi spätnú väzbu ohľadom tónu jeho textu, aby sa vyhol prílišnému neformálnemu registru vzhľadom na jeho neskúsenosť a taktiež vie pomôcť s lepším napĺňaním **funkcií diskurzu**, ako je napríklad kohézia textu. Umelá inteligencia môže navrhnúť spôsoby ako zlepšiť prúdenie informácií cez

⁶ Ako napríklad ChatGPT, Quizlet, LingQ, Memrise, WordUp AI Vocabulary. Dané platformy umožňujú nahrať súbory, z ktorých si následne program vytvorí špecializovaný glosár na precvičovanie podľa potrieb študenta.

⁷ Vid' DUDAŠOVÁ, Iva: *Coordination vs. Subordination in Selected Legal Contracts*. Diplomová práca. 2025. s. 35-53.

písaný text prostredníctvom spojok a iných spojovacích prostriedkov ako napríklad „*whereas, therefore, notwithstanding*“.

Adaptívne AI platformy

Adaptívne AI platformy majú potenciál pretvoriť tradičné učenie sa založené na Sokratovej metóde učenia na nový štýl, ktorý dokáže sústrediť pozornosť na praktické zručnosti nevyhnutné pre modernú právnu prax po štúdiách.

AI podporené nástroje sú dnes využívané pre úlohy ako je právna rešerš, príprava podkladov na návrhy zmlúv a môžu automatizovať opakujúce sa úkony, ktoré umožňujú študentom zefektívniť prípravu na výučbový proces. AI algoritmy umožňujú analýzy rozsiahlych textov pre identifikáciu pre študenta užitočných bodov, čím sa stierajú limity, ktoré kedysi študenti mali: obmedzené kognitívne možnosti a obmedzený čas.

GenAI, tzv. generatívna umelá inteligencia, ako podskupina umelej inteligencie, dokáže generovať nové dáta na základe vzorcov, extrapolovaných z pôvodne zadaného veľkého množstva tréningových dát, kým tradičná AI sa zameriavala na klasifikáciu a odporúčania. Inými slovami GenAI, ako napr. ChatGPT, Claude a iné nachádzajú vzorce na porozumenie a vytvárajú nové výstupy, ktoré napodobňujú ľudskú kreativitu a uvažovanie.⁸

Generatívna umelá inteligencia vyniká svojou rýchlosťou a môže byť skvelým nástrojom pre skúsených riešiteľov problémov. Pre tých, ktorí sú ešte len v procese rozvíjania divergentného myslenia (to je štádium prichádzania so širším okruhom myšlienok a nápadov), čiže aj pre študentov, a nemajú ešte dostatočne vytvorenú kreatívnu sebadôveru, existuje riziko toho, že umelá inteligencia bude brániť rozvoju ľudského myslenia. V rámci štúdie vedenej kolektívom S. Habib niektorí účastníci uviedli, že vnímali ťažkosti s prichádzaním s nápadmi nad rámec toho, čo ponúkala umelá inteligencia, čo môže napovedať aj o prílišnej fixácii na ponúknuté riešenia.⁹ Dá sa povedať, že prítomnosť iného generatívneho zdroja môže spôsobiť spomalenie efektívnosti pôvodného generatívneho zdroja, ktorý by mal byť tým primárnym. Študent by mal totiž vedieť posúdiť ponúknutý preklad alebo nájsť riešenie dilemy ohľadom právnej terminológie a preukázať flexibilitu pri vnímaní rôznych perspektív. Moderné AI platformy navyše ponúkajú špecializované režimy, ktoré sú optimalizované pre vzdelávacie účely, takzvané **"learning mode"** alebo **"study mode"** funkcie. Sú dostupné v platformách ako ChatGPT Plus, Claude, či Gemini

⁸ ALIER, Marc – GARCÍA-PEÑALVO, Francisco – CAMBA, Jorge D.: *Generative Artificial Intelligence in Education: From Deceptive to Disruptive*. In: International Journal of Interactive Multimedia and Artificial Intelligence, Roč. 8, č. 1 (2024), s. 9.

⁹ HABIB, Sabrina a kol.: *How Does Generative Artificial Intelligence Impact Student Creativity?* In: Journal of Creativity, Roč. 34, č. 1 (2024). s. 5.

Advanced a umožňujú študentom vytvárať personalizované učebné plány, ktoré môžu byť presne prispôsobené kurikulu. Systém dokáže analyzovať sylabus predmetu a na jeho základe vytvoriť detailný časový harmonogram učenia, ktorý zohľadňuje postupnosť tém, ich vzájomnú prepojenosť a nároky na osvojenie si právnej terminológie. Študent môže do systému nahráť učebný plán predmetu a AI vie automaticky rozdeliť materiál do logických celkov s odporúčaným časovým rozložením.

Jednou z kľúčových výhod *learning* režimu je **schopnosť generovania dodatočných cvičení**, ktoré sú zamerané na špecifické potreby študenta. Na základe identifikovaných slabých miest v porozumení právnej terminológie dokáže AI vytvoriť ciele úlohy na precvičovanie. Napríklad, ak študent má problémy s rozlišovaním medzi "*authority*" a "*competence*" v rôznych kontextoch, systém vygeneruje sériu cvičení, ktoré postupne budujú porozumenie týchto pojmov prostredníctvom autentických právnych situácií. Tieto cvičenia môžu mať formu doplňovacích úloh, výberu z možností, alebo tvorby vlastných viet s použitím daných termínov v správnom kontexte. *Learning* režim sa osvedčuje aj pri vyhľadávaní a kategorizácii najvýznamnejších právnych textov pre jednotlivé témy. AI dokáže na požiadanie študenta **identifikovať kľúčové precedensy**, legislatívne texty alebo odborné články, ktoré sú relevantné pre aktuálne preberanú problematiku. Pri štúdiu zmluvného práva môže systém navrhnúť štúdium konkrétnych prípadov, pričom súčasne poskytne zjednodušené vysvetlenie právnych princípov v anglickom jazyku prispôbomom jazykovej úrovni študenta, ktorú mu na počiatku špecifikuje. *Learning* režim umožňuje aj **adaptívne opakovanie**, kde AI sleduje pokrok študenta a automaticky navrhuje opakovanie materiálu na základe krivky zabúdania. Termíny, ktoré študent nepoužil určitý čas, alebo s ktorými mal v minulosti problémy, sa automaticky zaraďujú do opakovaných blokov.

Integrácia *learning* režimu do univerzitného kurikula vyžaduje iniciatívnu spoluprácu medzi vyučujúcimi a študentmi. Vyučujúci môžu poskytovať AI systémom štruktúrované vstupy o cieľoch predmetu, očakávaných výstupoch a špecifických požiadavkách na terminológiu, zatiaľ čo študenti aktívne využívajú tieto nástroje na doplnenie a prehĺbenie svojich vedomostí získaných na hodinách. Takýto hybridný prístup maximalizuje efektívnosť učebného procesu pri zachovaní kvality vzdelávania a rozvoji kritického myslenia študentov.

Stratégie prevencie negatívnych dopadov AI

Stratégie prevencie predpokladajú, že negatívne dopady umelej inteligencie sú už identifikované a uvedenému sa v posledných rokoch venovala pozornosť akademickej obce, pričom bolo identifikovaných viacero problematických oblastí. Medzi nimi prehnané spoliehanie sa na výsledky, ktoré ponúka umelá inteligencia

študentom, zásahy do kreativity a edukačná etika.¹⁰ V tomto ohľade sa aj fakulty a univerzity snažia reagovať na využívanie AI a formovať využívanie generatívnej umelej inteligencie cez novovytvorené predmety ako je napríklad *Právo a umelá inteligencia* na Právnickej fakulte UK, kde sa cez zadania študenti učia zadávať príkazy na vytvorenie právnej analýzy, ktorú musia skorigovať a nesú zodpovednosť za výsledok právnej analýzy a taktiež cez normatívne interné predpisy fakúlt/univerzít, ktoré majú za cieľ vytvoriť rámec jej využívaniu.

V súvislosti s prehnaným spoliehaním sa na výsledky, ktoré ponúka AI sa môžeme dotknúť konceptu autonómie učiaceho sa študenta, ktorému sa venovali H. Holec a D. Little. Holec ho definoval ako „*schopnosť prevziať zodpovednosť za vlastné vzdelávanie*“, pričom sa uvádza, že táto schopnosť „*nie je vrodenná, ale musí sa nadobudnúť buď prirodzeným spôsobom alebo (ako sa najčastejšie stáva) formálnym vzdelávaním, t.j. systematickým a zámerným spôsobom*“ a zdôrazňuje sa, že prevziať zodpovednosť za svoje vzdelávanie znamená mať (...) zodpovednosť za všetky rozhodnutia týkajúce sa všetkých aspektov tohto vzdelávania (...).¹¹ Little zase uviedol, že autonómia študenta je „*v podstate otázkou psychologického vzťahu študenta k procesu a obsahu vzdelávania – schopnosťou odstupe, kritického myslenia, rozhodovania a nezávislého konania*“.¹² Práve zodpovednosť, schopnosť odstupe a kritického zhodnotenia ponúknutých foriem riešení zo strany AI by mali byť novými aspektami formálneho vzdelávania budúceho právnik. Na nezávislé rozhodovanie a kritické nazeranie na terminológiu je nevyhnutným predpokladom, že študent už disponuje vedomosťami a zručnosťami súvisiacimi s anglickým jazykom pre špecifické účely, aby vedel náležite zhodnotiť adekvátnosť ponúknutého riešenia zo strany AI platforiem. Rovnakým spôsobom potom dokáže autonómne dohliadať na svoj učebný proces v hraniciach používania, ktoré stanovila univerzita/fakulta/vyučujúci. Implikácie pre študenta sú uvedomenie si vlastnej zodpovednosti za výsledok svojho vzdelávania, pričom by malo prísť k uvedomeniu, že AI nie je náhradou vzdelávania, ale prostriedkom. Rezonujú názory ohľadom budúcej relevantnosti a uplatnenia prekladateľov, pričom pôvodné predikcie ohľadom skorého nahradenia sa preklopili do hodnotenia kolaboratívneho

¹⁰ V rámci štúdie, keď študentom bola adresovaná otázka ohľadom ich závislosti na nástrojoch umelej inteligencie, viac ako 50 percent účastníkov uviedlo, že si uvedomuje, že tieto nástroje im zhoršuje kritické myslenie pri písaní a približne 15 percent z nich považuje za náročné prekonať svoju závislosť od týchto nástrojov, zatiaľ čo ostatní nie. Takisto 15 percent študentov priznalo, že používanie nástrojov umelej inteligencie vystavuje riziku účasti na plagiátorstve. In: PHAM Thi Thuy Dung – LUONG Minh Hieu: *Students' Challenges in Employing AI Tools in Legal Writing*. In: International Journal of TESOL & Education, Roč. 5, č. 2, (2025), s. 82-83.

¹¹ HOLEC, Henri: *Autonomy and Foreign Language Learning*. Oxford: Pergamon. 1981, s. 3.

¹² LITTLE, David: *Learner Autonomy. 1: Definitions, Issues and Problems*. Dublin: Authentik. 1991. s. 4.

potenciálu.¹³ K uvedenému patrí aj uvedenie, že študenti v rámci anglického jazyka pre špecifické účely budú mať za úlohu zhodnotiť predkladané AI riešenia a na to musia disponovať dostatočne vyvinutým kritickým myslením, ktoré by bez predchádzajúcich nadobudnutých vedomostí nebolo možné aplikovať.

Kreativita je definovaná ako schopnosť prichádzať s novými riešeniami, kombináciami myšlienok, ktoré majú hodnotu novoty, užívania a využitia pre široký okruh ľudí.¹⁴ S rozšírením generatívnej AI sa uplatnenie úsudku a kontroly pri používaní systémov a nástrojov umelej inteligencie stávajú nevyhnutnou súčasťou poskytovania najlepších možností vzdelávania pre študentov práva, pričom je nevyhnutné dbať na to, aby AI nezasahovala škodlivo do rozvíjajúcej sa kreativity, ale ju rozvíjala. Morrone a kolektív (2022) sa zaoberal vzťahom medzi kreativitou a AI tým, že viedol monitorované rozhovory so študentmi v Austrálii ohľadom ich skúsenosti s AI. Kolektív zistil, že študenti s vyšším sebahodnotením porozumenia AI uvádzali pozitívnejšie názory na integráciu AI do svojich školských aktivít. Autori navrhli, aby boli aplikácie umelej inteligencie povolené a aby boli študenti povzbudzovaní k používaniu umelej inteligencie vo vzdelávacích prostrediach a to najmä povzbudzovaní vo využití nových spôsobov prístupu k rôznym situáciám.¹⁵

Kvalitatívnemu a kvantitatívnemu výskumu sa venovali aj kolektív okolo Sabriny Habib v článku zameranom na to ako generatívna umelá inteligencia zasahuje do kreativity študentov a zo štúdie vzišlo viacero záverov.¹⁶ Štúdia sa síce zameriavala na to, ako sa umelá inteligencia používa vo fáze divergentného myslenia v tvorivom procese, výsledky potvrdili tvrdenie Vinchona a kol. (2023), že príprava študentov na tvorivú spoluprácu s umelou inteligenciou si vyžaduje rozvoj zručností pre počiatočné fázy (definovanie problému a určenie podnetu pre umelú inteligenciu) a koniec tvorivého procesu (konvergentné myslenie alebo hodnotenie a výber nápadov na implementáciu).¹⁷ Ak uvedené všeobecné zistenia ohľadom kreatívneho procesu aplikujeme na proces učenia sa anglického jazyka pre špecifické účely, tak zistíme, že pre študentov práva, ktorý sa učia cudzí odborný jazyk je základná znalosť stavebných kociek v podobe odbornej terminológie kľúčová a neobíditeľná. Ak má študent posúdiť to, čo mu AI ponúkne musí mať už zvládnuté stavebné kocky

¹³ VIEIRA, Lucas Nunes – ALONSO, Elisa: *Translating perceptions and managing expectations: an analysis of management and production perspectives on machine translation*. In: *Perspectives*, Roč. 28 (2019), s. 163–165.

¹⁴ CHIROCO, Alice a kol.: *Awe Enhances Creative Thinking: An Experimental Study*. In: *Creativity Research Journal*, Roč. 30, č. 2 (2018), s.124.

¹⁵ MARRONE, Rebecca – TADDEO, Victoria – HILL, Gillian: *Creativity and Artificial Intelligence—a Student Perspective*. In: *Journal of Intelligence*, Roč. 10 č. 3 (2022), s. 7.

¹⁶ HABIB, Sabrina a kol.: *How Does Generative Artificial Intelligence Impact Student Creativity?* In: *Journal of Creativity*, Roč. 34, č. 1 (2024). s. 7.

¹⁷ Ref. 16. s. 6.

s ktorými AI pracuje od počiatku. Ak sa študent domnieva, že sa celý proces dá nahradiť umelou inteligenciou, utrpí kvalita a odbornosť výstupu. Rovnako dôležitá a nenahraditeľná úloha je schopnosť študenta skonvergovať, zhodnotiť AI výstup a prispôbiť ho svojim potrebám.

Ako by teda mohol zodpovedný študent používať AI v procese učenia sa? Efektívna stratégia vyžaduje postupné budovanie kompetencií, kde študent najprv zvládne základy právnej terminológie tradičnými metódami, aby získal potrebný základ na kritické hodnotenie AI výstupov. V úvodných fázach štúdia by mal AI využívať predovšetkým na generovanie cvičných úloh, vysvetľovanie komplexných vetných štruktúr a precvičovanie kolokácií, pričom každý AI výstup by mal následne overiť prostredníctvom autentických právnych zdrojov. Kľúčové je dodržiavanie princípu „AI ako nástroj, nie náhrada“, čo znamená, že študent najprv formuluje vlastné riešenia a preklady a až následne konzultuje s AI, čím si zachováva aktívnu úlohu v učebnom procese. Pri práci s AI by si mal študent explicitne a vopred definovať hranice využitia – napríklad AI sa bude používať výhradne na analýzu štruktúry právnych textov, ale vlastná schopnosť argumentácie sa bude budovať výhradne samostatne, alebo využívať AI na generovanie synonym právnych termínov, ale kontextuálne použitie sa bude overovať pomocou reálnych právnych dokumentoch. Zodpovedný prístup zahŕňa aj transparentnosť voči vyučujúcim ohľadom rozsahu využitia AI pri samovzdelávaní, aby bol vyučujúci schopný odhaliť prípadné chyby spôsobené halucináciami jazykových modelov a vedenie záznamov o tom, aké AI nástroje a pre aké účely študent pri samoštúdiu používa, a pravidelné sebareflexné hodnotenie, či využívanie AI nástrojov ešte stále podporuje alebo už nahrádza študentove vlastné myšlienkové procesy. Takto nastavená stratégia umožňuje maximalizovať potenciálne prínosy AI pri minimalizovaní reálnych rizík ohrozenia akademickej integrity a etiky či rozvoja kritického myslenia.

Rozvoj a využívanie umelej inteligencie je potrebné regulovať, aby sa stanovili konkrétne pravidlá jej používania a aby sa tiež identifikovali dôsledky v prípade jej neetického alebo nevhodného používania. Ukazuje sa ako nevyhnutné vytvoriť regulatívny systém s príslušnými sankciami, tak aby boli pravidlá vynútiteľné. Regulácia totiž vie predchádzať určitým etickým rizikám, ktoré môže spôsobiť používanie umelej inteligencie v právnom vzdelávacom systéme.¹⁸ Najmä nerodení hovoriaci ako sú študenti slovenského práva, ktorí pracujú na zlepšení svojich cudzojazyčných kompetenciách znášajú riziko neúmyselného porušenia akademickej integrity používaním AI nástrojov. Tvrdiť, že došlo ku konečnému ustáleniu všetkých etických dilem a etických zneužití vo vzťahu k používaniu umelej

18 FLORES-VIVAR, Jesús – GARCÍA-PEÑALVO, Francisco. *Reflections on the ethics, potential, and challenges of artificial intelligence in the framework of quality education (SDG4)*. In: Comunicar, č. 74, (2023).s. 40.

inteligencie by bolo mylné. Tak ako sa vyvíja AI, tak aj štandardy jej používania a budúcnosť ukáže ako sa etické pravidlá upresnia.

Záver

Nie sme v dobe, kedy by sa AI dala zakázať, ale je na mieste, aby sa študenti pýtali akými spôsobmi sa dá využiť v ich prospech a v prospech, čo najefektívnejšieho procesu učenia sa. Uviedli sme špecifické využitia jazykových modelov v právnom diskurze, ktoré sa dajú prepracovávať s pomocou generatívnej AI, predstavili sme spôsoby ako tak urobiť na adaptívnych AI platformách a nakoniec sme na základe identifikovaných negatívnych vplyvov AI (ktoré sú už predmetom viacerých zahraničných štúdií a priebežne vyhodnocované) navrhli prevencie týchto negatívnych dopadov. Záverom, dôležité je načasovanie využívania generatívnej AI v kreatívnom procese, povedomie o prijatých etických pravidlách využívania AI a nezanedbanie vlastnej intelektuálnej činnosti v procese nadobúdania nových vedomostí. Táto etapa sa totiž nedá nahradiť využívaním AI. Vyučujúci na to majú reflektovať. Ak študenti neuvážene využívajú AI nástroje je aj úlohou vyučujúcich, aby podporili jej etické a efektívne využitie na hodinách a pomimo nich. Cieľom študentov by totiž nemalo byť nájdenie zradných skratiek, kde sa študenti zaujímajú len o výsledok, ale mal by byť zdôraznený aj proces v zmysle ľudovej múdrosti „Cesta je cieľ“. Cesta môže však nabráť iný obohacujúci rozmer s využitím AI možností a dialóg medzi študentmi a vyučujúcimi by mal v tomto ohľade byť otvorený.

Zoznam použitej literatúry

1. AGUILAR, Héctor González: *Some Trends on Artificial Intelligence in Legal Education*. In *Proceedings of the 22nd LACCEI International Multi-Conference for Engineering, Education and Technology (LACCEI 2024): Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0*, Latin American and Caribbean Consortium of Engineering Institutions, (2024), s.9. DOI:10.18687/LACCEI2024.1.1.481.
2. ALIER, Marc – GARCÍA-PEÑALVO, Francisco – CAMBA, Jorge D.: *Generative Artificial Intelligence in Education: From Deceptive to Disruptive*. In: *International Journal of Interactive Multimedia and Artificial Intelligence*, Roč. 8, č. 1 (2024), s. 5–14. DOI: <https://doi.org/10.9781/ijimai.2024.02.011>.
3. CHIROCO, Alice a kol.: *Awe Enhances Creative Thinking: An Experimental Study*. In: *Creativity Research Journal*, Roč. 30, č. 2 (2018), s. 123-131. <https://doi.org/10.1080/10400419.2018.1446491>
4. DILIDZE, Tatia: *The Evolving Role of Artificial Intelligence in Legal Education and Research*. In: *Law and World*, 2025, Roč. 11 č.33, s. 92-105. DOI: <https://doi.org/10.36475/11.1.7>.

5. DUDAŠOVÁ, Iva: *Coordination vs. Subordination in Selected Legal Contracts*. Diplomová práca, 2025. s. 77.
6. FLORES-VIVAR, Jesús – GARCÍA-PEÑALVO, Francisco. *Reflections on the ethics, potential, and challenges of artificial intelligence in the framework of quality education (SDG4)*. In: *Comunicar*, č. 74, (2023).s. 37-47. DOI: <https://doi.org/10.3916/C74-2023-03>.
7. HABIB, Sabrina a kol.: *How Does Generative Artificial Intelligence Impact Student Creativity?* In: *Journal of Creativity*, Roč. 34, č. 1 (2024). str. 7. DOI: <https://doi.org/10.1016/j.yjoc.2023.100072>.
8. HOLEC, Henri: *Autonomy and Foreign Language Learning*. Oxford: Pergamon. 1981. 145 s. ISBN 0-08-025357-1.
9. LITTLE, David: *Learner Autonomy. 1: Definitions, Issues and Problems*. Dublin: Authentik. 1991. 48 s. ISBN 0-08-025110-8.
10. MARRONE, Rebecca – TADDEO, Victoria – HILL, Gillian: *Creativity and Artificial Intelligence—a Student Perspective*. In: *Journal of Intelligence*, Roč. 10 č. 3 (2022), s. 65. DOI: <https://doi.org/10.3390/jintelligence10030065>.
11. PHAM Thi Thuy Dung – LUONG Minh Hieu: *Students' Challenges in Employing AI Tools in Legal Writing*. In: *International Journal of TESOL & Education*, Roč. 5, č. 2, (2025), s. 75-86. DOI: <https://doi.org/10.54855/ijte.25524>.
12. VIEIRA, Lucas Nunes – ALONSO, Elisa: *Translating perceptions and managing expectations: an analysis of management and production perspectives on machine translation*. In: *Perspectives*, Roč. 28 (2019), s.163–184. DOI: <https://doi.org/10.1080/0907676X.2019.1646776>
13. WU, Junyan – TANG, Wenjun: *Reform Method of University Legal Education Based on Artificial Intelligence and Wireless Communication*. In: *Wireless Communications and Mobile Computing*, 2022. číslo článku 2574911. 7 s. <https://doi.org/10.1155/2022/2574911>.
14. Medzinárodná advokátska komora (IBA). *The Future is now: Artificial Intelligence and the Legal Profession*. Dostupné na: <https://www.ibanet.org/document?id=The-future-is+now-AI-and-the-legal-profession-report>. citované dňa 10.09.2025
15. <https://www.lawsociety.org.uk/topics/ai-and-lawtech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>.

Kontaktné údaje

Mgr. et JUDr. Iva Dudášová, PhD.

iva.dudasova@flaw.uniba.sk

Ústav cudzojazyčnej právnej komunikácie, Právnická fakulta UK

ÚRADNÝ PREKLADATEĽ V DIGITÁLNOH PROSTREDÍ: MEDZI TRADÍCIOU A INOVÁCIOU

SWORN TRANSLATOR IN THE DIGITAL ENVIRONMENT: BETWEEN TRADITION AND INNOVATION

Sandra Banková, Sylvia Mičíková¹

Abstrakt: Digitalizácia justičného prostredia sa v posledných rokoch výrazne posunula – od elektronických podaní až po využívanie elektronického podpisu. V tejto dynamike však povolanie úradného prekladateľa zostáva prevažne v analógovej podobe. Príspevok sa zameriava na analýzu súčasného právneho rámca výkonu činnosti úradného prekladateľa na Slovensku s ohľadom na digitalizáciu. Predstavuje kľúčové problémy, ako sú absencia jednotného systému pre elektronické úradné preklady, pretrvávajúca požiadavka fyzickej pečiatky a podpisu, ako aj bezpečnostné riziká spojené s neštandardizovanými elektronickými postupmi. Diskutuje sa aj o možných riešeniach, ako napríklad využívanie zabezpečených komunikačných platforiem. Ďalej sa skúma dopad digitalizácie na efektivitu a dostupnosť úradných prekladov pre jednotlivcov a inštitúcie. Cieľom príspevku je otvoriť odbornú diskusiu o tom, ako nájsť rovnováhu medzi tradíciou a požiadavkami digitalizovaného právneho prostredia, pričom sa berie do úvahy potreba ochrany dôvernosti a integrity prekladov v digitálnom formáte. Zároveň sa kladie dôraz na vzdelávanie a prípravu úradných prekladateľov, aby vedeli efektívne využívať moderné digitálne nástroje a systémy.

Kľúčové slová: ESP, úradný prekladateľ, digitalizácia, elektronický podpis, elektronická pečiatka, bezpečnosť

Abstract: The digitalization of the judicial environment has advanced significantly in recent years – from electronic filings to the use of electronic signatures. However, within this dynamic, the profession of the sworn translator remains largely analog. This paper focuses on analyzing the current legal framework governing the work of sworn translators in Slovakia in the context of digitalization. It highlights key issues such as the absence of a unified system for electronic official translations, the persistent requirement for a physical stamp and signature, as well as security risks associated with non-

¹ Univerzita Komenského v Bratislave, Právnická fakulta

standardized electronic procedures. Possible solutions are also discussed, such as the use of secure communication platforms. The aim of this paper is to initiate a professional discussion on how to strike a balance between tradition and the requirements of a digitalized legal environment, while taking into account the need to protect the confidentiality and integrity of translations in digital form. Emphasis is also placed on the education and training of sworn translators so that they are able to use effectively modern digital tools and systems.

Key words: ESP, sworn translator, digitalization, electronic signature, electronic seal, security

Úvod

Digitalizácia verejnej správy na Slovensku prešla v posledných rokoch výrazným vývojom a stala sa kľúčovým pilierom modernizácie štátnych služieb. Zavedenie elektronických podaní, využívanie občianskeho preukazu s čipom (eID) a kvalifikovaného elektronického podpisu (KEP) umožnilo občanom a právnickým osobám komunikovať s orgánmi verejnej moci efektívne a bezpečne². Uvedené elektronické nástroje predstavujú základné komponenty slovenského eGovernmentu, ktorého cieľom je zjednodušiť administratívne procesy, zvýšiť transparentnosť a znížiť byrokráciu³.

Občiansky preukaz s čipom slúži nielen na identifikáciu osôb, ale aj na vytváranie kvalifikovaného elektronického podpisu, ktorý má rovnakú právnu silu ako vlastnoručný podpis.⁴ V prípade úradných⁵ prekladateľov je nevyhnutné, aby ich KEP obsahoval aj tzv. mandátny certifikát, ktorý potvrdzuje ich oprávnenie vykonávať činnosť podľa zákona č. 382/2004 Z. z.⁶ Pre elektronický úradný preklad je okrem KEP

² TOKOVSKA, Miroslava; FERREIRA, Vanessa Nolasco; VALLUŠOVA, Anna a SEBERÍNI, Andrea. E-Government—The Inclusive Way for the Future of Digital Citizenship. Online. Societies (Basel, Switzerland). 2023, roč. 13, č. 6, s. 141.

³ PISÁR, Peter a HONZOVÁ, Stanislava. E-Government and Economic Growth in the European Union: With a Specific Focus on Slovakia. Online. NISPAcee journal of public administration and policy. 2025, roč. 18, č. 1, s. 164.

⁴ Článok 25 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

⁵ Pojem „úradný prekladateľ“ nie je legislatívne definovaný, avšak v praxi sa využíva najčastejšie pre pomenovanie prekladateľa zapísaného do zoznamu znalcov, tlmočníkov a prekladateľov vedenom Ministerstvom spravodlivosti SR podľa zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch. Z toho dôvodu sme sa rozhodli používať toto pomenovanie v celom texte.

⁶ § 8 zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

potrebná aj časová pečiatka, ktorá zabezpečuje presný čas vyhotovenia dokumentu a garantuje jeho nemennosť⁷.

Tento článok sa preto zameriava na analýzu právneho rámca výkonu činnosti úradného prekladateľa v kontexte digitalizácie a identifikuje kľúčové výzvy a možnosti ďalšieho vývoja tejto profesie.

Európske iniciatívy v oblasti digitalizácie verejnej správy

Digitalizácia verejnej správy a elektronických služieb je prioritou Európskej únie, ktorá prostredníctvom legislatívnych a finančných nástrojov podporuje členské štáty v zavádzaní moderných, bezpečných a interoperabilných riešení.⁸ Tieto iniciatívy majú priamy dopad aj na oblasť úradných prekladov.

Základným právnym rámcem je Nariadenie (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách (eIDAS) pre elektronické transakcie na vnútornom trhu, ktoré stanovuje pravidlá pre kvalifikované elektronické podpisy, pečate, časové pečiatky a elektronické doručovanie. V máji 2024 nadobudla účinnosť jeho aktualizácia: Nariadenie (EÚ) 2024/1183, ktoré zavádza Európsky rámec digitálnej identity a EU Digital Identity Wallet⁹.

Každý členský štát bude povinný do roku 2026 poskytnúť občanom, rezidentom a firmám aspoň jednu verziu digitálnej peňaženky, ktorá umožní bezpečné uchovávanie a zdieľanie digitálnych dokumentov (napr. diplomy, licencie, preklady), vytváranie právne záväzných elektronických podpisov a pečatí, či cezhraničné využívanie elektronických služieb v rámci EÚ. Táto peňaženka bude interoperabilná, bezpečná a plne pod kontrolou používateľa, čo má za cieľ posilniť dôveru v elektronické transakcie a identifikáciu.¹⁰

Pre oblasť úradných prekladov je to relevantné z hľadiska digitálnej dôvery, ktorá je kľúčová pri vytváraní elektronických dokumentov s právnou záväznosťou.

⁷ Článok 3 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

⁸ PROFIROIU, Constantin Marius; NEGOIȚĂ, Ciprian Ionuț a COSTEA, Adrian Vladimir. Digitalization of public administration in EU member states in times of crisis: the contributions of the national recovery and resilience plans. Online. International review of administrative sciences. 2024, roč. 90, č. 2, s. 338.

⁹ ANSAROU DI, Zahra Ebadi; CARBONE, Roberto; SCIARRETTA, Giada; RANISE, Silvio; FERRARA, Anna Lisa et al. Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends. In: Data and Applications Security and Privacy XXXVII. 13942. Switzerland: Springer, 2023, s. 113-114.

¹⁰ KUDRA, Andre; RIEGER, Alexander; SEDLMEIR, Johannes; ROTH, Tamara; FRIDGEN, Gilbert et al. Digital Identity Wallets: A Guide to the EU's New Identity Model. Online. Information systems journal (Oxford, England). 2025, s. 3-5.

Právny rámec výkonu činnosti úradného prekladateľa

Výkon činnosti úradného prekladateľa na Slovensku je upravený zákonom č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov¹¹. Tento zákon stanovuje podmienky výkonu činnosti, práva a povinnosti prekladateľov, ako aj pravidlá pre ich zápis do zoznamu vedeného Ministerstvom spravodlivosti SR, a mnohé iné.

Zákon definuje úradného prekladateľa ako fyzickú osobu, ktorá je zapísaná v zozname prekladateľov a splnila odborné, etické a administratívne požiadavky.¹² Na overenie odbornej spôsobilosti prekladateľa slúži absolvovanie odborného minima a úspešné zvládnutie odbornej skúšky.¹³ Prekladateľ je povinný vykonávať svoju činnosť nestranne, nezávisle a v súlade s právnymi predpismi. Výstupom jeho práce je preklad, ktorý musí byť opatrený prekladateľskou doložkou, podpisom a pečiatkou.¹⁴

Podrobnosti výkonu činnosti upravuje vyhláška č. 228/2018 Z. z., ktorá stanovuje napríklad formálne náležitosti úradného prekladu, spôsob vedenia elektronického denníka, pravidlá odborného minima a vzdelávanie¹⁵. Vyhláška tiež upravuje spôsob zápisu do zoznamu, vedenie evidencie výkonu činnosti a elektronickú komunikáciu s ministerstvom. Stojí za spomenutie, že zákon ani vykonávacia vyhláška však nespomínajú tzv. mäkké zručnosti (soft skills)¹⁶, ktoré sú pritom nevyhnutné pre kvalitný výkon prekladateľskej činnosti, napríklad komunikačné zručnosti, zodpovednosť či zvládanie stresu.

Elektronizácia činnosti úradných prekladateľov

V súvislosti s technologickým rozvojom prekladateľskej praxe sa čoraz častejšie začína zdôrazňovať potreba prekladateľov rozvíjať svoje digitálne a technické kompetencie. V tejto súvislosti vystáva meno Prieto Ramos, ktorý vytvoril štruktúru kompetencií právnych prekladateľov, ktorej súčasťou je aj inštrumentálna kompetencia zahŕňajúca o. i. prácu s CAT nástrojmi či terminologickými

¹¹ Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.

¹² § 2 + § 5 zákona č. 382/2004 Z. z.

¹³ DANKOVČIK, J., JURAN, J. a KOŠUTH, M.: Zákon o znalcoch, tlmočníkoch a prekladateľoch. Komentár. Bratislava: Wolters Kluwer SR s. r. o., 2020, s. 64.

¹⁴ Príloha č. 9 k vyhláške č. 228/2018 Z. z.

¹⁵ Vyhláška č. 228/2018 Z. z. Ministerstva spravodlivosti Slovenskej republiky, ktorou sa vykonáva zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

¹⁶ REIMAN, Cindi. Soft skills. Hoboken, New Jersey: John Wiley & Sons, 2023, s 8-9.

databázami.¹⁷ Zároveň je dôležité, aby prekladateľ dokázal prekladaný výraz a text správne interpretovať a adekvátne ho preniesť do cieľového jazyka s použitím vhodného prekladateľského postupu.¹⁸ Takto chápaný technologický a odborný rozmer je nevyhnutný pre efektívny výkon prekladateľskej činnosti v prostredí postupnej digitalizácie.

Uvedené aspekty a kompetencie sú v slovenskej právnej úprave zastúpené len čiastočne, nakoľko v oblasti digitalizácie sa zameriava predovšetkým na povinnosť prekladateľa viesť elektronický denník a odmeňovanie prekladov v elektronickej forme, pričom ostatné technologické aspekty ostávajú takmer bez úpravy.

Elektronický denník je povinný pre každého úradného prekladateľa zapísaného v zozname Ministerstva spravodlivosti SR, pričom prekladateľ je povinný zapisovať údaje o každom vykonanom úkone do 30 dní od jeho vykonania.¹⁹ Elektronický denník sa vedie prostredníctvom modulu RESS – IS ESS²⁰, ktorý je súčasťou elektronizácie služieb súdnictva. Denník umožňuje zaznamenávať prekladateľské, tlmočnicke a znalecké úkony, odosielať údaje do centrálného úložiska ministerstva, a zjednodušuje vyúčtovanie úkonov. Prístup do systému je zabezpečený cez eID kartu alebo prihlasovacie údaje.

Aj keď elektronický denník predstavuje významný krok v digitalizácii oblasti úradných prekladov, jeho využitie je zatiaľ obmedzené na internú evidenciu. Nie je prepojený s verejnými databázami ani neumožňuje automatizované doručovanie alebo overovanie výstupov.

Osobitnú pozornosť si zaslúži vyhláška č. 491/2004 Z. z. o odmenách, náhradách výdavkov a náhradách za stratu času pre znalcov, tlmočníkov a prekladateľov. V § 14 vyhláška výslovne ustanovuje rozdielnú výšku náhrady hotových výdavkov podľa toho, či je preklad vyhotovený v listinnej alebo v elektronickej podobe. Za listinné vyhotovenie prekladu je stanovená náhrada vo výške 2,66 eura za jedno vyhotovenie, zatiaľ čo pri elektronickej forme patrí prekladateľovi 4,66 eura za prvých sto prekladateľských úkonov v danom kalendárnom roku, a za každé ďalšie vyhotovenie

¹⁷PRIETO RAMOS, Fernando. DEVELOPING LEGAL TRANSLATION COMPETENCE: AN INTEGRATIVE PROCESS-ORIENTED APPROACH. Online. Comparative legilinguistics. 2017, roč. 5, s. 11-13.

¹⁸ WREDE, Oľga. Právny preklad a jeho translačné modely – teória a prax. Nitra: Univerzita Konštantína Filozofa v Nitre, 2021, s. 14-25.

¹⁹ § 2 vyhlášky č. 228/2018 Z. z.

²⁰ MINISTERSTVO SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY. Rozvoj elektronických služieb súdnictva (RESS). Online. Dostupné z: <https://www.justice.gov.sk/agenda-ministerstva/nase-projekty/europske-strukturalne-a-investicne-fondy/rozvoj-elektronickych-sluzieb-sudnictva-ress/>. [cit. 2025-08-26].

2,83 eura.²¹ Už samotné číselné nastavenie poukazuje na snahu zákonodarcu ekonomicky motivovať prekladateľa, aby preferoval elektronickú podobu prekladov. Keďže forma vyhotovenia prekladu je výsledkom dohody medzi prekladateľom a objednávateľom,²² takto nastavené odmeňovanie nepriamo nabáda prekladateľov, aby aktívnejšie presviedčali zadávateľov k využívaniu elektronickej alternatívy.

Takýto prístup zákonodarcu môžeme interpretovať ako legislatívny nástroj na podporu digitalizácie prekladov, zároveň však vyvstáva otázka o jeho účelnosti a spravodlivosti. Je otázne, či je vhodné, aby sa finančné mechanizmy využívali ako nepriamy prostriedok na usmerňovanie vzťahu medzi prekladateľom a zadávateľom. Rovnako vnímame ako problematické, že zákonodarca dal túto „táču“ na prekladateľa, aby kvôli vidine vyššieho zisku nabádal zadávateľov na preferovanú formu prekladu.

Taktiež môžeme namietat, že vyššie odmeny za elektronickú formu nezohľadňujú reálne technické ani časové náklady, ktoré musí prekladateľ vynaložiť na získanie certifikátov, čítačiek či softvéru. Je preto namieste zvážiť, či by nebolo vhodnejšie podporovať digitalizáciu systémovo prostredníctvom štandardizovaných nástrojov a zníženia administratívnych bariér namiesto finančných rozdielov vo výške náhrad. V neposlednom rade stojí za zmienku využívanie CAT nástrojov (Computer-Assisted Translation) a ich nezahrnutie do zákona o znalcoch, tlmočníkoch a prekladateľoch. CAT nástroje sú softvér, pomocou ktorého majú prekladatelia možnosť uchovávať prekladovú pamäť a terminologické databázy.²³ Môžeme teda konštatovať, že hoci zákonodarca prostredníctvom odlišných odmien vyvíja snahu o modernizáciu a digitalizáciu činnosti prekladateľov, absencia komplexnej právnej úpravy, vrátane využívania CAT nástrojov, poukazuje na potrebu systémového prístupu k modernizácii prekladateľskej činnosti. Takýto systematický prístup je dôležitý predovšetkým preto, že v konečnom dôsledku je iba prekladateľ zodpovedný za výsledný text, ktorého kvalita je ovplyvnená mnohými objektívnymi aj subjektívnymi faktormi.²⁴ Ak totiž bude z akéhokoľvek dôvodu vypracovaný nesprávny preklad, môžu z toho vyplývať významné právne následky.²⁵

²¹ § 14 ods. 3 písm. a) vyhlášky č. 491/2004 Z. z. Ministerstva spravodlivosti Slovenskej republiky o odmenách, náhradách výdavkov a náhradách za stratu času pre znalcov, tlmočníkov a prekladateľov.

²² § 23 ods. 1 zákona č. 382/2004 Z. z.

²³ KORNACKI, Michal. Computer-assisted translation (CAT) tools in the translator training process. Berlin: Peter Lang, 2018, s. 102.

²⁴ CHROMÁ, Marta. Právní překlad v teorii a praxi. Nový občanský zákoník. Praha: Nakladatelství Karolinum, 2016, s. 34.

²⁵ PRIETO RAMOS, Fernando. Legal and institutional translator competence: developments and training implications. Online. The interpreter and translator trainer. 2024, roč. 18, č. 2, s. 140.

Technické a bezpečnostné zabezpečenie elektronického úradného prekladu na Slovensku

Úradný prekladateľ, ktorý chce vyhotovovať elektronické úradné preklady, musí disponovať viacerými technickými nástrojmi a právnymi oprávneniami. V súčasnosti neexistuje jednotná štátna platforma, ktorá by tento proces centralizovala, a preto sú prekladatelia odkázaní na individuálne riešenia.

Základným predpokladom je kvalifikovaný elektronický podpis, ktorý je možné získať prostredníctvom občianskeho preukazu s čipom (eID). Pri jeho vydaní si používateľ môže aktivovať kvalifikovaný certifikát. Na podpisovanie dokumentov je potrebná čítačka čipových kariet a softvér, ako napríklad Disig Desktop Signer, D.Signer/XAdES, QSign alebo I.CA Secom.²⁶

Prekladateľ musí ďalej disponovať mandátnym certifikátom, ktorý potvrdzuje jeho oprávnenie konať ako úradný prekladateľ. Tento certifikát sa vydáva na základe zápisu v zozname prekladateľov vedenom Ministerstvom spravodlivosti SR²⁷. Na jeho získanie je potrebné predložiť výpis zo zoznamu prekladateľov, dva doklady totožnosti, výber typu nosiča (čipová karta alebo USB token), softvér k čipovej karte (napr. MONET+ ProID+Q)²⁸.

Časová pečiatka slúži na nezávislé potvrdenie času podpisu dokumentu. Získava sa od akreditovaných certifikačných autorít, ako sú Disig alebo I.CA. Časová pečiatka sa zvyčajne automaticky pripája pri podpisovaní dokumentu cez certifikovaný softvér.²⁹ Elektronický úradný preklad sa zvyčajne vytvára vo formáte ASiC (.asice), ktorý združuje samotný dokument a elektronický podpis. Na jeho vytvorenie sa využívajú softvérové nástroje ako Disig Desktop Signer – umožňuje výber formátu PDF alebo ASiC, D.Suite/eIDAS – obsahuje modul ASiC Factory, D.Viewer – slúži na prezeranie podpísaných kontajnerov.³⁰ Uvedená odkázanosť prekladateľov na individuálne technické riešenia môže viesť k nejednotnosti výstupov a zvyšovať riziko chýb či nekompatibility dokumentov.

Od 1. novembra 2016 je štát povinný vykonávať verejnú moc prednostne elektronicky. Elektronické podania a rozhodnutia sa doručujú do elektronických schránok občanov a podnikateľov, pričom listinná forma sa používa len v prípade výnimiek, ak to výslovne ustanovuje osobitný predpis.

Osobitným aspektom, ktorý nemožno opomenúť, je povinnosť prekladateľa zachovávať mlčanlivosť. Podľa § 13 zákona č. 382/2004 Z. z. je úradný prekladateľ

²⁶ SLOVENSKO.SK. eID karta. Online. Dostupné z: https://www.slovensko.sk/sk/eid/_eid-karta/?utm_source=chatgpt.com. [cit. 2025-08-21].

²⁷ Certifikát je možné získať osobne alebo elektronicky cez portál slovensko.sk.

²⁸ Cena sa pohybuje približne od 65 do 85 EUR bez DPH, pričom certifikát má zvyčajne ročnú platnosť.

²⁹ Ročný poplatok za službu sa pohybuje okolo 30 EUR.

³⁰ Tieto aplikácie sú dostupné na stránke slovensko.sk.

povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel počas výkonu svojej činnosti alebo v súvislosti s ňou, a to aj po skončení výkonu činnosti. Tejto povinnosti ho môže zbaviť len zadávateľ alebo Ministerstvo spravodlivosti SR.³¹ V kontexte digitalizácie však vzniká nové riziko. Keďže neexistuje jednotný a centralizovaný štátny systém pre elektronické úradné preklady, každý prekladateľ musí využívať svoje vlastné technické riešenia a softvéry. To vyvoláva otázku, do akej miery sú tieto individuálne riešenia schopné garantovať bezpečnosť dát a ochranu informácií pred neoprávneným prístupom či únikom. Zachovanie mlčanlivosti tak nie je len otázkou právnej zodpovednosti, ale aj technického zabezpečenia, ktoré by malo byť systematicky štandardizované a kontrolované.

Náklady na technické vybavenie

Problematickým bodom pre výkon prekladateľskej profesie sú náklady na technické vybavenie. Získanie mandátneho certifikátu, čipovej karty, čítačky a potrebného softvéru tak môže predstavovať finančnú záťaž, najmä pre samostatne pracujúcich prekladateľov. Okrem počiatočných nákladov je potrebné počítať aj s pravidelnou obnovou certifikátov a aktualizáciou softvéru, čo môže v konečnom dôsledku viesť až k prehodnoteniu vyhotovovania prekladov v elektronickej podobe.

Právna neistota pri elektronických výstupoch

Právna neistota vzniká najmä pri elektronickej podobe úradných prekladov, pretože zákon o znalcoch, tlmočníkoch a prekladateľoch síce požaduje, aby bol dokument podpísaný kvalifikovaným elektronickým podpisom a opatrený časovou pečiatkou, ale nehovorí, v akom presnom formáte má byť uložený, ako má byť štruktúrovaný, akým spôsobom sa má zabezpečiť integrita príloh a ktoré kontajnery sa majú použiť. V tomto prípade úlohu oficiálnej platformy supľujú súkromné firmy³². Okrem toho zákon predpokladá dohodu medzi prekladateľom a objednávateľom, teda elektronický preklad je možný iba vtedy, ak sa na tom obe strany dohodnú, čo vytvára riziko, že v prípade nesúladu nemusí byť dokument akceptovaný.³³

³¹ § 13 zákona č. 382/2004 Z. z.

³² Pre viac informácií pozri webovú stránku: <https://www.lexika.sk/blog/elektronicky-uradny-preklad-prirucka-pre-prekladatelov/>.

³³ § 23 ods. 1 zákona č. 382/2004 Z. z.

Odporúčania pre implementáciu digitalizácie výkonu činnosti úradného prekladateľa

Na základe identifikovaných problémov môžeme formulovať niekoľko konkrétnych odporúčaní, ktoré by mohli slúžiť ako východisko pre odbornú diskusiu a legislatívne či systémové zmeny:

1. Vytvorenie centralizovanej platformy pre elektronické úradné preklady: zriadenie jednotnej štátnej platformy pre elektronické úradné preklady by umožnilo štandardizované spracovanie dokumentov s právnou záväznosťou.
2. Zavedenie metodických usmernení pre úradných prekladateľov: vzhľadom na absenciu jednotnej platformy a rôznorodosť technických riešení je potrebné zaviesť metodické usmernenia, ktoré by štandardizovali postupy pri vyhotovovaní elektronických úradných prekladov. Tieto usmernenia by mali byť vydané Ministerstvom spravodlivosti SR v spolupráci s odbornými organizáciami.
3. Integrácia elektronického denníka s ďalšími elektronickými službami verejnej správy: elektronický denník úradného prekladateľa predstavuje významný nástroj na evidenciu vykonaných úkonov, no jeho využitie je zatiaľ obmedzené iba na internú administratívu. Pre zvýšenie efektivity, transparentnosti a právnej istoty je potrebné jeho prepojenie s ďalšími elektronickými systémami verejnej správy, ako sú:
 - portál slovensko.sk (pre elektronické podania),
 - register právnických osôb (pre overenie subjektov),
 - systémy súdov a orgánov verejnej moci (pre doručovanie dokumentov),
 - centrálné úložiská dokumentov (pre archiváciu a auditovateľnosť).
4. Vzdelávanie a technická podpora pre úradných prekladateľov v oblasti digitálnych nástrojov: úspešná digitalizácia výkonu činnosti úradného prekladateľa si vyžaduje nielen legislatívne a technické zmeny, ale aj systematické vzdelávanie a technickú podporu. Nakoľko absentujú materiály či usmernenia ohľadom digitalizácie v prekladateľskej profesii, môžeme sa domnievať, že prekladatelia nemajú dostatočné znalosti o používaní nástrojov ako sú kvalifikovaný elektronický podpis (KEP), mandátny certifikát, časová pečiatka, formáty PDF/A a ASiC, či softvéry na elektronické podpisovanie. Preto odporúčame zavedenie pravidelných školení, vytvorenie online vzdelávacích modulov, technickú podporu a konzultácie pre prekladateľov pri implementácii elektronických postupov.
5. Podpora výskumu a vývoja v oblasti právne záväzných elektronických jazykových služieb: digitalizácia úradného prekladu si vyžaduje nielen technickú infraštruktúru, ale aj inovačný výskum, ktorý by umožnil vývoj

nástrojov a metodík pre právne záväzné jazykové služby. V súčasnosti sa čoraz viac využívajú AI nástroje na podporu prekladu, post-editáciu, kontrolu kvality a terminologickú konzistenciu. Tieto technológie však zatiaľ nie sú plne integrované do prostredia úradného prekladu, kde je potrebná vysoká presnosť, právna istota a transparentnosť.

6. Zabezpečenie interoperability medzi národnými a európskymi systémami: v kontexte rastúcej medzinárodnej komunikácie v rámci Európskej únie je kľúčové, aby systémy pre elektronické úradné preklady boli technicky, právne a organizačne interoperabilné. To znamená, že dokumenty vyhotovené v jednom členskom štáte by mali byť uznávané a spracovateľné aj v iných štátoch bez potreby dodatočného overovania či konverzie.

Záver

Digitalizácia justičného prostredia na Slovensku prináša nové príležitosti, ale zároveň aj výzvy pre profesiu úradného prekladateľa. Ako ukazuje uvedená analýza súčasného právneho rámca, významné pokroky už boli dosiahnuté v oblasti elektronickej identifikácie a podpisovania dokumentov, no mnohé praktické aspekty ostávajú nevyriešené. Absencia jednotného systému pre elektronické úradné preklady či neistota pri technických formátoch prekladov oslabujú dôveru v elektronicú podobu prekladu.

Osobitným a diskutabilným krokom je nastavenie náhrad výdavkov podľa vyhlášky č. 491/2004 Z. z., ktoré prostredníctvom finančnej diferenciácie zvýhodňuje elektronicú formu. Zákonodarca týmto spôsobom zjavne sleduje cieľ podporiť digitalizáciu v preklade, avšak tento prístup sa nám javí ako kontroverzný, keďže nepriamo prenáša zodpovednosť za presadzovanie elektronických riešení na samotných prekladateľov.

Ak má byť digitalizácia úradného prekladu vnímaná ako plnohodnotný a dôveryhodný nástroj, je potrebné hľadať rovnováhu medzi technickými, legislatívnymi a etickými požiadavkami výkonu tejto profesie. Riešenie by malo spočívať najmä v systematickej podpore, teda vytvorení centralizovaných platforiem, metodických usmernení, technickej a finančnej pomoci pre prekladateľov, ako aj v budovaní interoperabilných systémov na európskej úrovni. Nazdávame sa, že iba týmto spôsobom je možné zabezpečiť, aby digitalizácia bola vnímaná ako prirodzený nástroj na zvýšenie efektívnosti, transparentnosti a dôveryhodnosti úradného prekladu v 21. storočí.

Zoznam použitej literatúry

1. ANSAROUDI, Zahra Ebadi; CARBONE, Roberto; SCARRETTA, Giada; RANISE, Silvio; FERRARA, Anna Lisa et al. Control is Nothing Without Trust a First Look

- into Digital Identity Wallet Trends. In: Data and Applications Security and Privacy XXXVII. 13942. Switzerland: Springer, 2023, s. 113-132. ISBN 9783031375859. ISSN 0302-9743. Dostupné z: https://doi.org/10.1007/978-3-031-37586-6_7. [cit. 2025-08-15].
2. CHROMÁ, Marta. Právní překlad v teorii a praxi. Nový občanský zákoník. Praha: Nakladatelství Karolinum, 2016. ISBN 978-80-246-2851-6.
 3. DANKOVČIK, J., JURAN, J. a KOŠUTH, M.: Zákon o znalcoch, tlmočníkoch a prekladateľoch. Komentár. Bratislava: Wolters Kluwer SR s. r. o., 2020. ISBN 978-80-571-0255-7.
 4. KORNACKI, Michal. Computer-assisted translation (CAT) tools in the translator training process. Berlin: Peter Lang, 2018. ISBN 978-3-631-77071-9.
 5. KUDRA, Andre; RIEGER, Alexander; SEDLMEIR, Johannes; ROTH, Tamara; FRIDGEN, Gilbert et al. Digital Identity Wallets: A Guide to the EU's New Identity Model. Online. Information systems journal (Oxford, England). 2025. ISSN 1350-1917. Dostupné z: <https://doi.org/10.1111/isj.70009>. [cit. 2025-08-16].
 6. PISÁR, Peter a HONZOVÁ, Stanislava. E-Government and Economic Growth in the European Union: With a Specific Focus on Slovakia. Online. NISPAcee journal of public administration and policy. 2025, roč. 18, č. 1, s. 163-191. ISSN 1337-9038. Dostupné z: <https://doi.org/10.2478/nispa-2025-0008>. [cit. 2025-08-02].
 7. PRIETO RAMOS, Fernando. DEVELOPING LEGAL TRANSLATION COMPETENCE: AN INTEGRATIVE PROCESS-ORIENTED APPROACH. Online. Comparative legilinguistics. 2017, roč. 5. ISSN 2080-5926. Dostupné z: <https://doi.org/10.14746/cl.2011.5.01>. [cit. 2025-08-20].
 8. PRIETO RAMOS, Fernando. Legal and institutional translator competence: developments and training implications. Online. The interpreter and translator trainer. 2024, roč. 18, č. 2. ISSN 1750-228X. Dostupné z: <https://doi.org/10.1080/1750399X.2024.2351780>. [cit. 2025-08-25].
 9. PROFIROIU, Constantin Marius; NEGOIȚĂ, Ciprian Ionuț a COSTEA, Adrian Vladimir. Digitalization of public administration in EU member states in times of crisis: the contributions of the national recovery and resilience plans. Online. International review of administrative sciences. 2024, roč. 90, č. 2, s. 336-352. ISSN 0020-8523. Dostupné z: <https://doi.org/10.1177/00208523231177554>. [cit. 2025-08-10].
 10. REIMAN, Cindi. Soft skills. Hoboken, New Jersey: John Wiley & Sons, 2023. ISBN 9781119906551.
 11. TOKOVSKA, Miroslava; FERREIRA, Vanessa Nolasco; VALLUŠOVA, Anna a SEBERÍNI, Andrea. E-Government—The Inclusive Way for the Future of Digital Citizenship. Online. Societies (Basel, Switzerland). 2023, roč. 13, č. 6, s. 141. ISSN 2075-4698. Dostupné z: <https://doi.org/10.3390/soc13060141>. [cit. 2025-08-01].

12. WREDE, Oľga. Právny preklad a jeho translačné modely – teória a prax. Nitra: Univerzita Konštantína Filozofa v Nitre, 2021. ISBN 978-80-558-1691-3.

Internetové zdroje

1. SLOVENSKO.SK. eID karta. Online. Dostupné z: https://www.slovensko.sk/sk/eid/eid-karta/?utm_source=chatgpt.com. [cit. 2025-08-21].
2. LEXIKA. Elektronický úradný preklad – príručka pre prekladateľov. Online. Dostupné z: <https://www.lexika.sk/blog/elektronicky-uradny-preklad-prirucka-pre-prekladatelov/>. [cit. 2025-08-25].
3. MINISTERSTVO SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY. Rozvoj elektronických služieb súdnictva (RESS). Online. Dostupné z: <https://www.justice.gov.sk/agenda-ministerstva/nase-projekty/europske-strukturalne-a-investicne-fondy/rozvoj-elektronickych-sluzieb-sudnictva-ress/>. [cit. 2025-08-26].

Právne predpisy

1. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
2. Vyhláška č. 228/2018 Z. z. Ministerstva spravodlivosti Slovenskej republiky, ktorou sa vykonáva zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
3. Vyhláška č. 491/2004 Z. z. Ministerstva spravodlivosti Slovenskej republiky o odmenách, náhradách výdavkov a náhradách za stratu času pre znalcov, tlmočníkov a prekladateľov.
4. Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.
5. Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

Kontaktné údaje

Mgr. Bc. Sandra Banková
sandra.bankova@flaw.uniba.sk
Ústav cudzojazyčnej právnej komunikácie, PraF UK
Mgr. Sylvia Mičíková, PhD.
sylvia.micikova@flaw.uniba.sk
Ústav cudzojazyčnej právnej komunikácie, PraF UK

DIGITÁLNE TECHNOLOGIE VO VÝUČBE PRÁVNEHO PREKLADU: VÝZVY A PRÍLEŽITOSTI

DIGITAL TECHNOLOGIES IN TEACHING LEGAL TRANSLATION: CHALLENGES AND OPPORTUNITIES

Sylvia Mičíková, Sandra Banková¹

Abstrakt: Preklad právnych textov predstavuje špecifickú oblasť prekladateľskej praxe, ktorá si vyžaduje nielen jazykovú presnosť, ale aj porozumenie právneho kontextu a interkultúrnym odlišnostiam, ako aj terminologickú konzistenciu. Digitalizácia a rozvoj umelej inteligencie zásadne transformujú prekladateľské postupy a kladú nové nároky na vzdelávanie. Cieľom príspevku je predstaviť návrh integrácie digitálnych nástrojov, menovite strojového prekladu, generatívnych jazykových modelov, CAT nástrojov, terminologických databáz a AI nástrojov na podporu písania a kontrolu textu do prekladového seminára pre študentov práva. Navrhované vzdelávacie aktivity majú za cieľ systematicky rozvíjať odborný, digitálny a etický rozmer prekladateľských kompetencií, s dôrazom na post-editing, kritické zhodnotenie automatizovaných výstupov a zodpovedné rozhodovanie v kontexte právnej záväznosti textu. Implementácia týchto nástrojov podporuje efektívnosť, autonómne a personalizované učenie a zároveň posilňuje pripravenosť študentov na profesionálne úlohy v prostredí hybridného prekladu. Predložený model výučby ilustruje vzťahy medzi rozvíjanými kompetenciami. Výsledkom prieniku týchto kompetencií je integrovaný projekt prekladu, v ktorom sa práca s digitálnymi nástrojmi, terminologický rešerš a etické posúdenie spoja do jednotného celku.

Kľúčové slová: právny preklad, vzdelávacie aktivity, digitálne technológie, etické využitie AI, ESP

Abstract: Legal translation constitutes a specialized field of translation practice that demands not only linguistic accuracy but also a thorough understanding of the legal context, intercultural differences, and terminological consistency. Digitalization and the advancement of artificial intelligence are fundamentally reshaping translation processes and creating new challenges for translator education. This paper proposes a framework for integrating digital tools,

¹ Právnická fakulta Univerzity Komenského v Bratislave

particularly machine translation, generative language models, CAT tools, terminological databases, and AI-assisted writing and text-checking tools, into a translation seminar for law students. The designed educational activities aim to systematically develop professional, digital, and ethical dimensions of translation competence, emphasizing post-editing, critical evaluation of automated outputs, and responsible decision-making in the context of legally binding texts. Implementing these tools enhances efficiency, fosters autonomous and personalized learning, and prepares students for professional practice in hybrid translation environments. The proposed teaching model illustrates the interplay between the competences being developed. Their intersection culminates in an integrated translation project, in which the use of digital tools, terminological research, and ethical evaluation converge into a coherent unit.

Keywords: legal translation, educational activities, digital technologies, ethical use of AI, ESP

Úvod

Preklad právnych textov predstavuje jednu z najnáročnejších oblastí prekladu, nielen z hľadiska jazykovej presnosti, ale aj právneho dopadu a právnych dôsledkov², kultúrneho prenosu a terminologickej konzistencie. Prekladový seminár pre študentov práva reflektuje potrebu pripraviť študentov na prácu v prostredí, kde sa právne texty pohybujú nielen medzi rôznymi jazykmi, ale aj právnymi systémami a kultúrami.

Digitalizácia a rozvoj umelej inteligencie zásadným spôsobom menia oblasť prekladateľskej praxe aj vzdelávania. Cieľom tohto príspevku je predstaviť návrh integrácie digitálnych nástrojov do prekladového seminára a navrhnúť konkrétne vzdelávacie aktivity rozvíjajúce kompetencie špecifické pre preklad právnych textov. Pre právny preklad to prináša nielen príležitosti (napr. vyššiu efektivitu, podporu terminologickej konzistentnosti), ale aj riziká v podobe nesprávnej interpretácie a naskoľuje aj etické otázky.

Výučba prekladového seminára na PraF UK

Seminár anglického odborného prekladu vyučovaný na PraF UK má od AR 2019/2020 status povinne voliteľného predmetu študijného programu právo v bakalárskom

² Keďže lingvistické rozhodnutia/rozhodovania [pri preklade právneho textu] prinášajú právne dôsledky. ŠARČEVIĆ, Susan: *New Approach to Legal Translation*, Kluwer Law International, 2008, ISBN 90 411 0401 01, str. 3

štúdiu v dennej forme³. V porovnaní s obdobím pred AR 2019/20 sa po jeho zaradení do kategórie PVP počet študentov zvýšil troj- až šesťnásobne⁴. Jeho zaradenie medzi predmety nevyhnutné pre získanie bakalárskeho titulu, ktorý „musia“ úspešne absolvovať všetci študenti bez ohľadu na ich záujem o translatologické vzdelávanie, ako aj heterogénnosť seminárnych skupín, si vyžiadalo prípravu osobitného študijného materiálu⁵ a uplatnenie špecifických pedagogických postupov a hodnotenia. Príprava študentov pred samotným prekladom pozostávala z osvojenia špecifickej právnej terminológie (napr. z oblasti pracovného práva), krátkych prekladov na vetnej úrovni, naštudovanie a precvičenie si určitého gramatického javu typického pre Legalese (napr. passive voice vs active voice) a prácu s vzorovými prekladmi. Každá téma sa preberala najskôr v smere z angličtiny do slovenčiny a zakončila sa prekladom zo slovenčiny do angličtiny. Hodnotenie pozostávalo z Moodle testu (40 bodov resp. 30 bodov v AR 2024/25) a záverečného 60 bodového resp. 70 bodového písomného testu, v ktorom sa okrem prekladu testovali špecifické gramatické javy, ustálené spojenia a ďalšie jazykové aspekty. Rápidny rozvoj digitálnych technológií, jednoduchá dostupnosť nástrojov umelej inteligencie a strojového prekladu po roku 2022 sa prejavili aj v prístupe študentov pri výučbe prekladového semináru. Anketové hodnotenia predmetov a vyučujúcich študentami čoraz intenzívnejšie poukazujú na potrebu zapojenia digitálnych technológií do procesu výučby prekladu právnych textov.

Komentáre študentov ilustrujú praktickú potrebu začleniť digitálne nástroje do prekladového seminára:

„...Práve umelá inteligencia mohla byť kľúčom tejto hodiny a či už zaujímavými novými zadaniami mohla ozvláštniť anglický od.preklad. Viem si predstaviť zadanie, kde by sme kontrolovali umelú inteligenciu, takisto zadania kde by sme sa snažili umelú inteligenciu promptami usmerňovať...; koniec koncov umelá inteligencia je čoraz viac prítomná...; Zameral by som výučbu na prácu so slovníkom a prekladačmi - aby študent vedel pracovať lepšie a zručnejšie s nástrojmi dnešnej doby. Lebo preklad cez rôzne internetové platformy nie je stále dokonalý a je na nás, aby sme to doladili do krásy, a práve to doladenie a pochopenie celku je to, na čo by som zameral výučbu. Lebo dnes každý pracuje s IT...; Na seminári nie je možné používať ani slovník ani počítač a hoci v praxi to pri preklade právnici bežne používajú, a je potrebné vedieť pracovať s modernými prekladačmi ako DeepL...; odporúčam skôr zmeniť spôsob výučby tohto predmetu, prikloniť sa k modernejšiemu spôsobu, využívať efektívnejšie umelú

³ V externej forme sa prvý krát predmet vyučoval v AR 2020/21.

⁴ Pre porovnanie podľa údajov z AIS-u: počet študentov SAOP v ZS 2018/19 58, po zaradení predmetu medzi PVP v ZS 2019/20 195, v AR 2024/25 356.

⁵ Jednotlivé lekcie vypracovali Mgr. Petra Uličná, PhD. a JUDr. Lucia Smolková, PhD. Odkaz na súbory <https://www.flaw.uniba.sk/pracoviska/ustavy/ustav-cudzojazycnej-pravnej-komunikacie/dokumenty/> [cit. 24.9.2025]

inteligenciu, aby sme sa vyhli tomu že napokon budeme všetko robiť len s ňou".⁶ Našou ambíciou je pripraviť taký návrh modelu výučby právneho prekladu, ktorý kombinuje odbornú presnosť, digitálnu kompetenciu a etickú reflexiu.

Teoreticko-metodologické východiská

Výučba prekladateľských zručností v právnom kontexte si vyžaduje teoretické východisko, ktoré reflektuje nielen tradičné lingvistické a interkultúrne aspekty prekladu, ale aj aktuálne technologické a etické výzvy. Ako vhodný teoretický základ sme si zvolili rámec prekladateľskej kompetencie EMT (European Master's in Translation), vypracovaný Európskou komisiou (2017⁷, aktualizovaný 2022⁸). Tento rámec definuje kľúčové oblasti prekladateľskej spôsobilosti, medzi ktoré patria: jazyková a kultúrna kompetencia, prekladateľská kompetencia, technologická kompetencia, personálna a interpersonálna kompetencia a kompetencia v poskytovaní služieb.

V kontexte prekladového seminára na Právnickej fakulte Univerzity Komenského je našou snahou rozšíriť rámec EMT o dve nadstavbové zložky, digitálnu a etickú kompetenciu.

Digitálna kompetencia presahuje technologickú kompetenciu rámca EMT. Nezahŕňa len ovládanie digitálnych nástrojov, ale aj kritické a reflexívne používanie AI-podporovaných technológií, schopnosť posúdiť spoľahlivosť digitálnych zdrojov a vedomie limitov automatizovaných riešení. Táto kompetencia je preto prierezová, keďže ovplyvňuje aj ďalšie dimenzie prekladateľskej činnosti, napríklad rozhodovanie pri voľbe právneho termínu či hodnotenie adekvátnosti výstupu strojového prekladu. Etická kompetencia nadväzuje na diskusie o profesijnej zodpovednosti a transparentnosti prekladateľov v digitálnom prostredí. V rámci výučby prekladového seminára nadobúda osobitný význam pri vedení študentov práva k rešpektovaniu autorských práv, dôvernosti dokumentov, ochrany údajov a etických princípov práce s generatívnymi systémami AI.

Didaktickým východiskom pre výučbu prekladateľských zručností študentov práva je učenie založené na úlohách (task-based learning, TLB), ktoré vychádza z konštruktivistického chápania učenia ako aktívneho procesu tvorby poznania. V súlade s týmto prístupom sa študenti učia prostredníctvom riešenia autentických zadání, ktoré odrážajú reálne situácie prekladateľskej praxe, napríklad preklad

⁶ Výber z odpovedí študentov anketového hodnotenia predmetu Seminár anglického odborného prekladu LS 2024/25 v AIS-e na otázku *K hodnotenému semináru by som chcel/a uviesť (pozitíva, negatíva, návrhy na zlepšenie)*. Komentáre uvádzame bez jazykových úprav.

⁷https://commission.europa.eu/system/files/2018-02/emt_competence_fw_k_2017_en_web.pdf

⁸https://commission.europa.eu/document/download/b482a2c0-42df-4291-8bf8-923922ddc6e1_en?filename=emt_competence_fw_k_2022_en.pdf

právnych zmlúv, súdnych rozhodnutí alebo stanovísk. Takéto úlohy podporujú rozvoj jazykovej, prekladateľskej a právnej kompetencie, pričom zároveň integrujú digitálnu a etickú dimenziu rámca EMT. V kontexte právnického vzdelávania umožňuje TBL prepojenie teoretických znalostí z oblasti práva so strategickým a reflexívnym uplatňovaním prekladových postupov.

Prehľad digitálnych technológií aplikovaných (nielen) v preklade právnych textov

Strojový preklad (Machine translation MT)

Medzi najrozšírenejšie nástroje MT patria Google Translate, DeepL a Bing Translator, využívajúce neurónové siete na generovanie prekladov v reálnom čase.

Prístupy⁹ k strojovému prekladu možno rozdeliť do dvoch skupín: prístupy založené na pravidlách (Rule based machine translation, RBMT) a prístupy založené na korpuse (Corpus based machine translation, CBMT). Historicky dominovali prístupy RBMT strojovému prekladu až do 90. rokov 20. storočia. Tento prístup je založený na lingvistických informáciách o zdrojovom a cieľovom jazyku, ktoré sa získavajú z jednojazyčných, dvojazyčných alebo viacjazyčných slovníkov a príručiek obsahujúcich základné sémantické, morfológické a syntaktické zákonitosti jazyka. Po spracovaní vstupnej vety systém RBMT generuje výstupné vety na základe analýzy zdrojového aj cieľového jazyka. S rozvojom technológií však RBMT ustúpilo efektívnejším metódam, najmä neurónovým strojovým prekladom.

S dostupnosťou dvojazyčných korpusov sa stali dominantnými metódy založené na korpusoch, medzi ktoré patrí strojový preklad založený na príkladoch (example-based machine translation, EBMT), štatistický strojový preklad (statistical machine translation, SMT) a neurónový strojový preklad (neural machine translation NMT).¹⁰ Po roku 2000 došlo k výraznému nástupu SMT, čo predstavovalo paradigmatický posun od RBMT k MT trénovanému na rozsiahlych korpusoch. Tieto korpusy často obsahujú milióny viet v jednom jazyku zosúladených s ekvivalentnými vetami v inom jazyku. Hoci SMT prispel k výraznému zlepšeniu kvality prekladu, jeho využitie log-lineárnych modelov na integráciu viacerých ručne navrhnutých komponentov¹¹, ako

⁹ T.j. kritériá, podľa ktorých je systém strojového prekladu navrhnutý

¹⁰ WANG, Haifeng – WU, Hua – HE, Zhongjun – HUANG, Liang – CHURCH, Kenneth Ward: Progress in Machine Translation. In: *Engineering*, 18, 2022, 143–153. ISSN 2095-8099. Dostupné online: <https://doi.org/10.1016/j.eng.2021.03.023> s. 143,144.

¹¹ Log-lineárny model je štatistický nástroj, ktorý umožňuje kombinovať rôzne zdroje informácií – napríklad pravidlá, jazykové vlastnosti alebo výstupy z iných systémov – do jedného celkového hodnotenia. Každý komponent prispieva svojím „bodovým skóre“ a model ich spočíta tak, aby výsledok čo najlepšie zodpovedal realite. Tento prístup sa často používa v oblasti spracovania textu, kde je potrebné zohľadniť viacero aspektov naraz.

je prekladový model, jazykový model a model preusporiadania, môže viesť k vážnym problémom s preusporiadaním pri vzdialených jazykových pároch.¹²

Vďaka výraznému pokroku v technológii hlbokého učenia založenom na neurónových sieťach bolo možné aplikovať túto technológiu na strojový preklad. Základnou myšlienkou NMT je zmapovať zdrojový jazyk do hustého sémantického zobrazenia a potom vygenerovať preklad pomocou mechanizmu pozornosti (attention mechanism)¹³. Typický model NMT pozostáva z dvoch hlavných komponentov: zo siete kodérov, ktorá premieta zdrojovú vetu do vektora s reálnymi hodnotami, a siete dekodérov, ktorá z tohto vektora vytvára preklad. Tento proces je analogický s ľudským prekladom, keďže model NMT najprv „prečíta“ celú zdrojovú vetu a následne, na základe jej komplexného pochopenia, generuje cieľovú vetu slovo za slovom.¹⁴

Generatívne AI nástroje

Generatívne jazykové modely ChatGPT, Gemini či Copilot predstavujú novú generáciu prekladových systémov založených na veľkých jazykových modeloch (Large Language Model, LLM). Jednou z kľúčových aplikácií veľkých jazykových modelov je automatizovaný preklad, ktorý nadobúda zásadný význam aj v právnej praxi. Právne texty sa vyznačujú vysokou mierou formalizmu, terminologickou presnosťou a väzbou na národné i nadnárodné právne systémy. Správne a konzistentné preklady legislatívnych ustanovení, judikatúry či zmluvných klauzúl sú preto nevyhnutné nielen pre cezhraničné obchodné transakcie, ale aj pre implementáciu práva Európskej únie či medzinárodných záväzkov do vnútroštátneho právneho poriadku.

Tradičné systémy strojového prekladu, ako sú Google Translate alebo DeepL, sú optimalizované pre bežné jazykové páry a často poskytujú uspokojivé výsledky v neutrálnych textoch.¹⁵ V právnom prostredí narážajú na limity: chyba im dostatočná terminologická konzistentnosť a schopnosť zachytiť špecifické väzby medzi právnymi inštitútmi.¹⁶ Významný posun v tejto oblasti priniesli LLM založené na

¹² WANG, Haifeng – WU, Hua – HE, Zhongjun – HUANG, Liang – CHURCH, Kenneth Ward: Progress in Machine Translation. In: *Engineering*, 18, 2022, 143–153. ISSN 2095-8099. Dostupné online: <https://doi.org/10.1016/j.eng.2021.03.023> . s.144 [cit.8.10.2025]

¹³ Ibid s. 144

¹⁴ Ibid s. 144

¹⁵ PALANICHAMY, Naveen – TROJOVSKÝ, Pavel: Overview and challenges of machine translation for contextually appropriate translations. In: *iScience*, roč.27, č.10, 110878, 2024. ISSN 2589-0042. Dostupné online: <https://doi.org/10.1016/j.isci.2024.110878> s.10 [cit. 8.10.2025]

¹⁶ Ibid s.17

transformerovej architektúre¹⁷, ktoré umožňujú preklad v režime zero-shot alebo few-shot t. j. bez špecifického tréningu na daný jazykový pár alebo len na základe niekoľkých príkladov. Tento prístup zvyšuje potenciál využitia LLM aj v menej rozšírených jazykoch alebo v textoch s vysokou mierou špecializácie, akými sú právne dokumenty.

Najnovšie empirické porovnania naznačujú, že LLM, napríklad GPT-4, dosahujú kvalitatívne parametre prekladu porovnateľné so špecializovanými systémami a v niektorých prípadoch ich dokonca prekonávajú¹⁸. V oblasti právnych textov to môže znamenať nielen verný preklad ustanovení, ale aj zachovanie právne záväzného významu. Súčasne však aplikácia LLM v právnom preklade prináša aj riziká. Modely môžu generovať tzv. halucinácie, t. j. obsah, ktorý sa v pôvodnom texte nevyskytuje, čo je v právnej oblasti obzvlášť problematické. Terminologická nekonzistentnosť môže viesť k odlišnému výkladu právnych noriem alebo zmluvných klauzúl. Z pohľadu aplikačnej praxe nemožno opomenúť ani otázku ochrany dôverných údajov, keďže právne dokumenty často obsahujú citlivé informácie, ktorých spracúvanie prostredníctvom cloudových služieb môže byť v rozpore s povinnosťami advokátov alebo pravidlami compliance.

Praktické aplikácie LLM sa v právnom prostredí sústreďujú predovšetkým na podporu pracovných prekladov legislatívnych návrhov, medzinárodných zmlúv či rozhodnutí súdov. Aj napriek ich výraznému potenciálu nemožno LLM chápať ako náhradu profesionálneho právneho prekladu, ale skôr ako nástroj významne zvyšujúci jeho efektivitu a dostupnosť.

V tomto kontexte zohráva dôležitú úlohu post-editing (PE), ktorý je nevyhnutným krokom pri spracovaní právnych textov. Post-editing strojového prekladu predstavuje odborný zásah do automaticky generovaného prekladu s cieľom dosiahnuť požadovanú kvalitatívnu úroveň textu. Výskum v oblasti post-editingu strojovo preložených textov potvrdzuje, že sa stáva nevyhnutnou súčasťou pracovného postupu prekladateľov. Napr. Koponen zdôrazňuje posun post-editingu z pomerne okrajovej pozície do centrálnejšej pozície v troch oblastiach: ako prax v

¹⁷ VASWANI, A. – SHAZEER, N. – PARMAR, N. – USZKOREIT, J. – JONES, L. – GOMEZ, A. N. – KAISER, L. – POLOSUKHIN, I.: Attention Is All You Need. In: Advances in Neural Information Processing Systems, 2017. Dostupné online <https://doi.org/10.48550/arXiv.1706.03762> s. 2 [cit. 8.10. 2025]

¹⁸ JIAO, Wenxiang – WANG, Wenxuan – HUANG, Jen-tse – WAN G, Xing – SHI, Shuming: Is ChatGPT A Good Translator? Yes With GPT-4 As The Engine. 2023. Dostupné online <https://doi.org/10.48550/arXiv.2301.08745> s. 9 [cit. 8.10.2025]

prekladateľskom priemysle, ako predmet výskumu translatológie, aj ako téma pre vzdelávanie prekladateľov.¹⁹

V právnom kontexte post-editing zahŕňa najmä korekciu terminologických nepresností, syntaktických chýb a štylistických odchýlok, ktoré by mohli ovplyvniť právnu záväznosť alebo interpretáciu dokumentu. Rozlišujeme tzv. light post-editing, ktorý zabezpečí porozumenie textu a full post-editing, ktorý vyžaduje komplexnú revíziu s prihliadnutím na jazykové, štylistické a právne normy cieľového jazyka.

Praktická seminárna úloha spočíva v tom, že študenti upravujú výstupy z nástrojov DeepL alebo Google Translate v oboch režimoch a následne sa porovnávajú kvantitatívne aj kvalitatívne výsledky.

Vzhľadom na to, že právny preklad je často právne záväzný dokument, nemôže byť text generovaný umelou inteligenciou prijatý bez ľudskej revízie. Túto požiadavku reflektuje aj medzinárodný štandard ISO 18587:2017, ktorý stanovuje rámec a požiadavky na post-editing strojovo preložených textov vrátane špecifických nárokov na kvalitu a profesionálnu zodpovednosť za obsah.²⁰

CAT (Computer assisted translation) nástroje

CAT nástroje ako SDL Trados, MemoQ a Memsource predstavujú štandard v profesionálnej prekladateľskej praxi. Ich kľúčovou funkciou je využívanie prekladových pamätí (Translation Memories – TM) a terminologických databáz, ktoré zabezpečujú konzistentnosť a efektivitu. Prekladová pamäť je program, ktorý uchováva paralelné texty zarovnané po segmentoch. Segment spravidla zodpovedá vete, avšak môže predstavovať aj kratšiu jazykovú jednotku, napr. frázu. Paralelný text pozostáva z originálu a jeho prekladu, ktoré sú spárované a ukladané do databázy. Pri následných prekladateľských projektoch môže systém vyhľadávať a ponúkať tieto uložené segmenty, čím sa zvyšuje jednotnosť a rýchlosť prekladu. Okrem prekladových pamätí (ktorých môže mať prekladateľ viacero) poskytujú CAT nástroje aj možnosť vytvárania a správy terminologických databáz. Tieto databázy umožňujú systematickú evidenciu odborných pojmov a zabezpečujú ich konzistentné používanie v rámci textov i projektov.

¹⁹ KOPONEN, Maarit: Is Machine Translation Post-editing Worth the Effort? A Survey of Research into Post-editing and Effort. In: The Journal of Specialized Translation, 25, 2019. 131-148. ISSN 1740-357X s. 12.

²⁰ ISO (2017) ISO 18587 Translation Services – Post-editing of Machine Translation Output – Requirements, Geneva: International Standards Office.

Terminologické databázy a korpusy

Medzi kľúčové terminologické a textové zdroje, ktoré sú relevantné pre preklad právnych textov, patrí predovšetkým oficiálna terminologická databáza Európskej únie IATE (InterActive Terminology for Europe)²¹ ktorá obsahuje štandardizované výrazy vo všetkých úradných jazykoch. Dopĺňa ju databáza právnych dokumentov EÚ EUR-Lex²², ktorá sprístupňuje paralelné texty a legislatívne akty v multilingválnej podobe a národné právne databázy (napr. Slov-lex²³), ktoré poskytujú terminologické a kontextové informácie pre národné právne systémy. Z moderných nástrojov možno spomenúť platformu Juremy,²⁴ ktorá umožňuje simultánne vyhľadávanie v IATE a EUR-Lex a ponúka bilingválne výsledky priamo v kontexte, čím výrazne prispieva k efektívnosti prekladateľskej praxe.

Vzdelávacie aktivity sa realizujú sa formou zostavenia zoznamu kľúčových pojmov s ekvivalentmi overenými v databázach IATE, EUR-Lex a UNTERM, doplnených o kontextové poznámky. Následne sa precvičuje korpusové vyhľadávanie prostredníctvom nástrojov typu Sketch Engine či Linguae, ktoré umožňujú identifikovať typické kolokácie a ustálené právne spojenia.²⁵

Nástroje na podporu písania a kontrolu textu pomocou umelej inteligencie (AI-assisted writing and checking tools)

Tieto nástroje predstavujú samostatnú kategóriu medzi klasickými prekladateľskými nástrojmi. Neslúžia primárne na preklad celých textov, ale na podporu používateľa v procesoch jazykovej kontroly, parafrázovania a výberu adekvátnych kolokácií. V rámci klasifikácie digitálnych nástrojov ich možno zaradiť medzi hybridné riešenia, stojace na rozhraní medzi systémami strojového prekladu a korpusovými nástrojmi. Patrí sem napr. Grammarly a Writefull, pričom ich spoločným cieľom je podpora používateľa pri tvorbe a revízii textu, avšak s odlišným zameraním a rozsahom využitia.

Writefull²⁶ vyvinutý špecificky pre akademické písanie a predstavuje pokročilý nástroj založený na umelej inteligencii, trénovaný na rozsiahlych korpusoch vedeckých článkov. Medzi kľúčové funkcie Writefull patrí *Sentence Palette*, ktorá

²¹ <https://iate.europa.eu/home>

²² <https://eur-lex.europa.eu/homepage.html>

²³ <https://www.slov-lex.sk/>

²⁴ <https://www.juremy.com/about/>

²⁵ BJEL, Lucia: Corpora in Institutional Legal Translation: Small Steps and the Big Picture. In: Institutional Translation for International Governance: Enhancing Quality in Multilingual Legal Communication, 2018, 25–36. Dostupné online: https://www.researchgate.net/publication/341883578_Corpora_in_Institutional_Legal_Translation_Small_Steps_and_the_Big_Picture. s. 6 [cit. 8.10.2025]

²⁶ <https://www.writefull.com/>

ponúka návrhy vhodných akademických formulácií v závislosti od kontextu a *Paraphraser* umožňujúci prepis textu do rôznych jazykových štýlov. Funkcia *Title Generator* automaticky navrhuje názvy článkov na základe ich abstraktu, zatiaľ čo *Abstract Generator* zas umožňuje generovanie abstraktov z odborných textov.

Nástroj *Writefull Revise* navyše poskytuje spätnú väzbu priamo v texte prostredníctvom funkcie „Track Changes“, čo umožňuje používateľom kriticky zhodnocovať odporúčané úpravy.

Grammarly²⁷ je v súčasnosti najrozšírenejší jazykový asistent, dostupný ako samostatná aplikácia aj ako rozšírenie do internetových prehliadačov. Jeho primárnym cieľom je zlepšovanie kvality textov vo všeobecnej a pracovnej komunikácii. Poskytuje kontrolu gramatiky, pravopisu a interpunkcie, doplnenú o návrhy na zvýšenie čitateľnosti, štylistickej plynulosti a celkovej jazykovej kvality textu.

Benefity využívania digitálnych technológií vo výučbe právneho prekladu

Efektivita a dostupnosť

Výskumy realizované v európskom kontexte ukazujú, že nástroje založené na umelej inteligencii, ako sú ChatGPT, DeepL či Gemini, dokážu výrazne zvýšiť efektivitu výučby. Študentom poskytujú prístup k rozsiahlym jazykovým databázam, právnym korpusom a automatizovaným návrhom prekladu. Tieto technológie uľahčujú rýchle vytváranie pracovných verzií textov, ktoré následne podliehajú post-editácii a detailnej analýze. Takýto postup podporuje schopnosť študentov kriticky hodnotiť jazykové výstupy a rozvíjať zručnosti potrebné pre profesionálnu prekladateľskú prax.

Clément-Wilz et al. upozorňujú, že hoci AI technológie zefektívňujú prekladateľské procesy, ich využitie si vyžaduje diferencovaný prístup podľa typu právneho dokumentu. Autori navrhujú vytvorenie taxonómie právnych textov, ktorá by umožnila cielenejšie zapojenie AI do výučby a výskumu právneho prekladu²⁸. Zároveň poukazujú na potrebu pedagogickej reflexie technologických zmien a vývoja nových vzdelávacích rámcov.²⁹

Podobné prístupy prinášajú aj európske projekty LT-LiDER³⁰ a MultiTraiNMT³¹, ktoré sa zameriavajú na integráciu digitálnych nástrojov do výučby prekladu. Tieto

²⁷ <https://www.grammarly.com/>

²⁸ CLÉMENT-WILZ, Laure – DE LAFORCADE, Agata – CENNAMO, Ilaria: Translation in the European Union: Navigating Technical and Legal Issues in the Light of Artificial Intelligence — Conclusions. In: International Journal of Language & Law, 14, 2025. 240-255. DOI: 10.14762/jll.2025.240. s. 251

²⁹ Ibid s. 252

³⁰ [EU-funded research projects on translation | Knowledge Centre on Translation and Interpretation](#)

³¹ www.multitrainmt.eu/index.php/en/

iniciatívy podporované Európskou úniou vytvárajú otvorené vzdelávacie zdroje a platformy, ktoré umožňujú profesionálom aj študentom samostatne pracovať s neuronovým strojovým prekladom, rozvíjať digitálne kompetencie a reflektovať jazykové rozhodnutia v právnom kontexte.

Giampieri³² upozorňuje, že automatizované preklady sa na prvý pohľad môžu javiť ako správne, avšak pri dôkladnejšej analýze je zrejma nevyhnutnosť ľudskej intervencie. Potreba dôkladnej post-editácie, pri ktorej sa zohľadnia dôveryhodné zdroje, ako sú právne slovníky, legislatívne dokumenty a judikatúra sa preto javí ako nevyhnutná.

Aplikovanie generatívnych AI nástrojov na prekladovom seminári umožní študentom rýchlo vytvoriť návrh prekladu, ktorý následne podrobí jazykovej a terminologickej analýze. Tento proces podporuje rozvoj kritického myslenia, jazykovej presnosti a schopnosti reflektovať právne významy.

Podpora personalizovaného učenia

Využitie umelej inteligencie vo vzdelávaní predstavuje výrazný posun smerom k personalizovanému a autonómnemu učeniu. Van der Vorst a Jellic³³ konštatujú, že AI nástroje umožňujú študentom pracovať vlastným tempom, pričom systémy na báze strojového učenia dokážu prispôbiť obsah výučby individuálnym potrebám študenta. Tým sa naplňa potenciál tzv. „one-to-one“ výučby, ktorá bola doteraz z praktických dôvodov nedosiahnuteľná. Prieto Ramos vo svojom výskume zdôrazňuje potrebu aktualizácie kompetenčných modelov právneho prekladu tak, aby reflektovali technologické zmeny v profesijnej praxi. V rámci inštrumentálnej kompetencie sa pritom kladie dôraz na efektívne využívanie spoľahlivých zdrojov a softvéru informačných technológií, vrátane systémov strojového prekladu³⁴.

³² GIAMPIERI, Patrizia: The use of AI in the translation of legal documents: A critical analysis. In: trans-kom, roč. 17, č. 2, 2024. 343–358. ISSN 1867-4844. Dostupné online: https://www.trans-kom.eu/bd17nro2/trans-kom_17_02_05_Giampieri_AI.20241128.pdf s. 354 [cit. 8.10.2025]

³³ VAN DER VORST, Tommy – JELICIC, Nick: Artificial Intelligence in Education: Can AI bring the full potential of personalized learning to education? In: 30th European Conference of the International Telecommunications Society (ITS): "Towards a Connected and Automated Society", Helsinki, Finland, 16.–19. 6., 2019. Calgary: International Telecommunications Society (ITS). Dostupné online: <https://hdl.handle.net/10419/205222> s.15 [cit. 8.10.2025]

³⁴ PRIETO RAMOS, Fernando: Revisiting translator competence in the age of artificial intelligence: the case of legal and institutional translation. In: The Interpreter and Translator Trainer, roč. 18, č. 2, 2024, 148–173. ISSN 1757-0417. DOI: 10.1080/1750399X.2024.2344942. s. 155. [cit. 8.10.2025]

Riziká a výzvy využívania digitálnych technológií vo výučbe právneho prekladu

Kontextové nepresnosti a terminologické chyby

Prieto Ramos vo svojej štúdii prezentoval výsledky rozsiahleho prieskumu medzi inštitucionálnymi prekladateľmi z EÚ, OSN, WTO a ďalších medzinárodných organizácií, ktorý bol zameraný na charakteristiky post-editingu a na vplyv využívania NMT na prekladové procesy, výsledné produkty a prekladateľské kompetencie³⁵. Prieskum konštatuje zmenu pracovných postupov prekladateľov. Dôraz sa kladie na potrebu disponovať solídnymi prekladateľskými zručnosťami s cieľom zabezpečiť kvalitu v čoraz hybridnejšej a dynamickejšej kombinácii prekladateľských činností v prostredí rozšíreného (augmented) prekladu. Na základe uvádzaného prieskumu väčšina prekladateľov vnímala využívanie NMT ako prevažne prínosné, hoci zároveň identifikovala zvýšené riziko zníženia kvality prekladu a potenciálne negatívne dôsledky pre cieľový jazyk. Podľa ich názoru strojový preklad nedokáže zabezpečiť terminologickú konzistentnosť ani reflektovať špecifický „inštitucionálny jazyk“ jednotlivých organizácií. Zároveň obsahuje nepredvídateľné chyby, ktoré revíziu textu výrazne časovo predlžujú. Skúsenejšie skupiny prekladateľov navyše hodnotili vplyv NMT na kvalitu prekladu kritickejšie než menej skúsení kolegovia. Na druhej strane sa však väčšina respondentov zhodla, že strojový preklad zvyšuje produktivitu prekladového procesu, šetrí čas a umožňuje sústrediť sa na riešenie náročnejších prekladateľských problémov a na zlepšovanie celkovej kvality prekladu.³⁶

Etické aspekty využívania umelej inteligencie vo výučbe právneho prekladu

Integrácia generatívnej umelej inteligencie (GenAI) do výučby právneho prekladu prináša nielen technologické výhody, ale aj komplexné etické výzvy. Tieto výzvy sa týkajú akademickej integrity, rovnosti prístupu, transparentnosti hodnotenia, ako aj profesionálnej zodpovednosti budúcich právnych prekladateľov.

Sarah Eaton poukazuje na to, že nástup umelej inteligencie mení samotné chápanie akademickej integrity a prináša fenomén postplagiátorstva, v ktorom sa prelínajú ľudský a strojovo generovaný text.³⁷ Tento posun vytvára nové etické dilemy vo

³⁵ PRIETO RAMOS, F.: Embracing New Translation Technologies at International Organizations: Translators' Perceptions of Machine Translation and its Impact on Institutional Translation. In: *International Journal of Language & Law*, roč. 14, č. 1, 202. S., 1-29. ISSN: 2194-7414. DOI: 10.14762/jll.2025.001 s.4 [cit.8.10.2025]

³⁶ Ibid, s.25

³⁷ EATON, Sarah Elaine: Postplagiarism: transdisciplinary ethics and integrity in the age of artificial intelligence and neurotechnology. In: *International Journal of Educational Integrity*, roč. 19:23, 2023. S. 1-10. ISSN 1833-2595. Dostupné online: <https://doi.org/10.1007/s40979-023-00144-1> s.2 [cit.8.10.2025]

vzdelávaní, pretože tradičné chápanie plagiátu a originality prestáva byť postačujúce. Ak tieto úvahy prenesieme do kontextu výučby právneho prekladu, stáva sa kľúčovou otázkou, ako odlíšiť legitímne využitie AI ako podporného nástroja od neetického nahrádzania vlastnej analytickej a terminologickej práce študenta. Transparentné pravidlá používania AI tak nadobúdajú zásadný význam nielen pre zachovanie akademickej integrity, ale aj pre formovanie profesionálnej zodpovednosti budúcich právnych prekladateľov.

Eaton ďalej zdôrazňuje, že hoci v hybridnej forme tvorby textu (hybrid human-AI writing), môže byť proces tvorby prekladu do istej miery ovplyvnený umelou inteligenciou, konečnú zodpovednosť za výsledný preklad nesie vždy autor.³⁸ Toto je kľúčový etický imperatív: aj keď študent využíva generatívnu AI na vygenerovanie návrhu prekladu alebo terminologických možností, je zodpovedný za presnosť, spoľahlivosť, jazykovú aj právnu adekvátnosť prekladu.

Podobne aj Pym a Hao prezentujú koncept rozšíreného prekladu (augmented translation)³⁹, kde sa prekladateľský proces rozširuje o asistenciu technológií, avšak zodpovednosť za výsledok nesie prekladateľ. Pre výučbu právneho prekladu to znamená, že AI môže fungovať ako cenný podporný nástroj, napríklad pri navrhovaní terminologických variantov, ale konečný výsledok musia študenti kriticky zvážiť, overiť a prijať zaň plnú zodpovednosť.

V právnom kontexte má tento prístup zásadne vyššiu váhu: nesprávne AI-generované preklady môžu viesť k vážnym právnym konzekvenciám, ovplyvniť platnosť dokumentu alebo presnosť právnych úkonov. V neposlednom rade budúci právní prekladatelia musia byť pripravení na etické dilemy, ktoré vznikajú pri používaní AI v profesionálnej praxi. Týka sa to nielen zodpovednosti za chyby v preklade generovanom AI, ale aj ochrany dôverných údajov a rešpektovania autorských práv.

Návrh rámca vzdelávacích aktivít pre študentov prekladového seminára

Prehľad digitálnych nástrojov načrtnutých v predchádzajúcej časti predstavuje technologické východisko, ktoré je v súčasnosti dostupné pre oblasť právneho prekladu. Aby však tieto nástroje nestratili svoj pedagogický potenciál a nestali sa len technickými pomôckami, je potrebné ich integrovať do didaktického rámca, ktorý cielene rozvíja odborný, digitálny a etický rozmer prekladateľských kompetencií. V nasledujúcej tabuľke predstavíme návrh modelu seminárnych aktivít, ktorý

³⁸ Ibid s.5

³⁹ PYM, Antony – HAO, Yu: How to Augment Language Skills: Generative AI and Machine Translation in Language Learning and Translator Training. Londýn a New York: Routledge, 2025. 218 s. ISBN 978-1-032-61495-3. . Dostupné online: DOI: 10.4324/9781032648033. s.XI [cit.8.10.2025]

demonštruje, ako možno jednotlivé kategórie digitálnych technológií uplatniť pri výučbe právneho prekladu a aké špecifické zručnosti si študenti osvojujú.

Digitálna technológia	Seminárna aktivita	Rozvíjaná kompetencia
Strojový preklad (Google translate, DeepL)	Post-editing (light vs full)	Kritické zhodnotenie, terminologická presnosť, zodpovednosť za preklad
Generatívne AI nástroje (ChatGPT, Copilot, Gemini)	Tvorba promptov a porovnanie výsledkov prekladu; diskusia o halucinovaní a dôvere	Digitálna gramotnosť, práca s generatívnou AI;
CAT nástroje (Trados, Memos,..) <i>(Realizované iba v prípade zaobstarania potrebných licencií)</i>	Tvorba a využitie prekladovej pamäte a terminologickej databázy	Konzistentnosť terminologickej databázy
Terminologické databázy a korpusy (IATE, EUR-Lex, Slov-Lex, Linguee, Sketch Engine)	Terminologický rešerš pre konkrétny právny inštitút; porovnanie ekvivalentov rôznych databázach; tvorba kolokácií	Práca s korpusmi, terminologická presnosť; právna komparatistika;
Nástroje na podporu písania a kontrolu textu pomocou umelej inteligencie (Writefull, Grammarly)	Revízia vlastného prekladu pomocou AI nástrojov; hodnotenie navrhnutých zmien	Jazyková kultivovanosť; kritická reflexia

Tabuľka č. 1
Digitálne nástroje, aktivity a kompetencie

Navrhovaný model výučby právneho prekladu demonštruje, že digitálne technológie možno integrovať do seminárnej výučby systematicky a s jasným cieľom rozvoja špecifických kompetencií.

Strojový preklad, reprezentovaný nástrojmi ako Google Translate alebo DeepL, sa uplatňuje najmä v kombinácii s post-editingom. Úlohou študentov je vykonať buď minimálnu úpravu, alebo komplexnú revíziu preloženého textu. Tento postup rozvíja schopnosť kriticky hodnotiť kvalitu prekladu, precízne pracovať s terminológiou a uvedomovať si zodpovednosť za obsah právne záväzných dokumentov.

Veľké jazykové modely, ako napríklad ChatGPT, Gemini či Copilot, predstavujú ďalšiu oblasť využiteľnú vo výučbe. Prostredníctvom tvorby a modifikácie promptov študenti testujú limity týchto systémov a porovnávajú kvalitu výstupov. Dôraz sa pritom kladie na diskusiu o potenciálnych rizikách, akými sú tzv. halucinácie alebo otázky dôveryhodnosti údajov. Týmto spôsobom sa rozvíja nielen digitálna gramotnosť, ale aj etická reflexia práce s generatívnou umelou inteligenciou.

CAT nástroje (napr. Trados, MemoQ, Memsource) umožňujú študentom vytvárať a spravovať prekladové pamäte a terminologické databázy, čím si osvojujú postupy zabezpečujúce konzistentnosť terminológie a zvyšujú efektívnosť prekladového procesu.

Terminologické databázy a právne korpusy, ako IATE, EUR-Lex, Juremy či Slov-lex zohrávajú kľúčovú úlohu v upevňovaní terminologickej presnosti. V rámci rešeršných cvičení študenti vyhľadávajú a porovnávajú ekvivalenty konkrétnych právnych inštitútov vo viacerých zdrojoch, čo zároveň rozvíja schopnosť práce s paralelnými textami a osvojenie si prvkov právnej komparatistiky.

AI nástroje na podporu písania a jazykovej revízie (Grammarly, Writefull) poskytujú priestor na rozvoj kritickej reflexie vo fáze editácie prekladu. Študenti aplikujú tieto nástroje na vlastné preklady a posudzujú navrhované zmeny z hľadiska ich vhodnosti v právnom kontexte. Týmto spôsobom si rozvíjajú jazykovú kultivovanosť a schopnosť odlíšiť všeobecný jazykový register od striktne právneho štýlu.

Model výučby právneho prekladu

Pre lepšie znázornenie návrhu koncepcie výučby právneho prekladu sme s pomocou AI nástroja chatGPT vytvorili nasledovný Vennov diagram:

Model výučby právneho prekladu

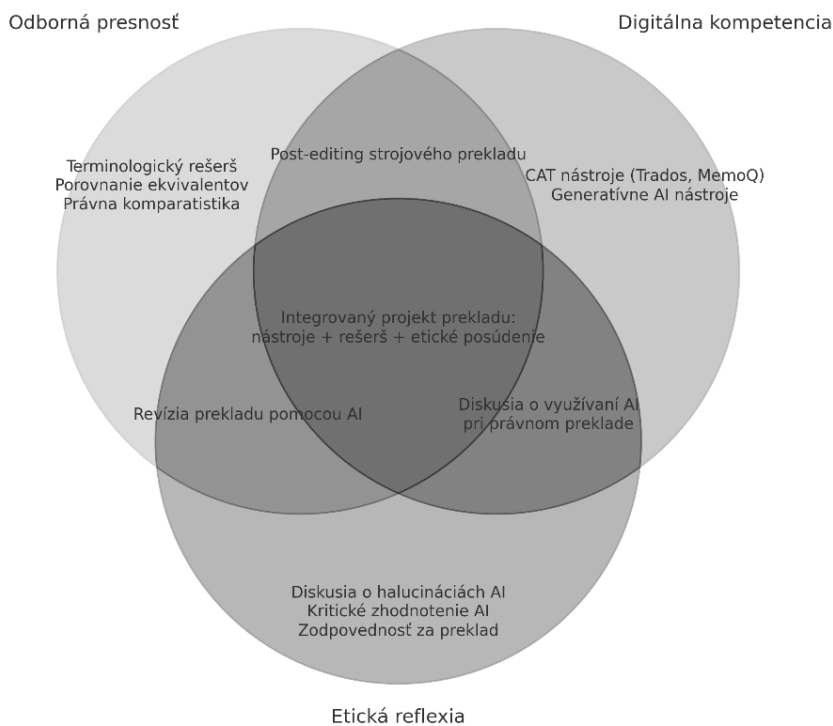


Schéma č. 1

Model výučby právneho prekladu

Uvedená schéma ilustruje vzťahy medzi jednotlivými kompetenciami. Prienik odbornej presnosti a digitálnej kompetencie sa prejavuje najmä v post-editingu strojového prekladu. Študenti sa učia, ako spojiť technické možnosti prekladového nástroja s odbornou kontrolou právnej terminológie a významu.

Prienik odbornej presnosti a etickej reflexie je zrejmý pri revízii prekladu pomocou AI. Hoci nástroj ponúkne návrh riešenia, študenti musia kriticky posúdiť jeho správnosť a zároveň uvažovať o hraniciach zodpovednosti, ktoré sa s takýmto postupom spájajú.

Spojenie digitálnej kompetencie a etickej reflexie sa realizuje v diskusii o využívaní AI pri právnom preklade. Ide o priestor, kde študenti skúmajú možnosti a limity umelej inteligencie a zamýšľajú sa nad jej etickými a praktickými dôsledkami.

Napokon sa všetky tri kompetencie sa pretínajú v integrovanom projekte prekladu, kde je potrebné zlúčiť prácu s digitálnymi nástrojmi, terminologický rešerš a etické posúdenie do jednotného celku. Tento prienik predstavuje vrchol celého modelu, pretože vyžaduje uplatnenie všetkých zručností v komplexnej úlohe.

Záver

Využitie digitálnych technológií vo výučbe prekladového seminára pre študentov práva predstavuje významný pedagogický a technologický posun. Ako ukazuje analýza dostupných nástrojov, technológií a vzdelávacích prístupov, integrácia AI a strojového prekladu do výučby rozširuje tradičné metódy o nové formy učenia, ktoré podporujú efektivitu, reflexiu a profesijnú pripravenosť študentov.

Digitálne nástroje poskytujú študentom možnosť pracovať s autentickými právnymi textami, analyzovať výstupy automatizovaných systémov a rozvíjať kritické myslenie. Zároveň však ich využívanie prináša výzvy, najmä v oblasti etiky a terminologickej presnosti.

Odporúčania pre integráciu digitálnych technológií do výučby prekladového semináru sú nasledovné: a) systematické začlenenie digitálnych nástrojov do výučby právneho prekladu, vrátane ich kritickej analýzy; b) rozvoj digitálnej a translatologickej gramotnosti študentov prostredníctvom praktických aktivít, c) zabezpečenie etickej reflexie pri práci s AI nástrojmi, najmä v kontexte právnej zodpovednosti a akademickej integrity.

Integrácia technológií do výučby právneho prekladu by nemala byť cieľom sama o sebe, ale nástrojom na podporu kvalitného, zodpovedného a kritického vzdelávania budúcich odborníkov v oblasti prekladu právnych textov.

Prirodzením pokračovaním nášho výskumu je nastavenie vhodných foriem hodnotenia študentov v prostredí, kde sa preklad čoraz viac opiera o digitálne a AI nástroje. Tradičné hodnotenie výsledného prekladu plánujeme rozšíriť o procesne orientované hodnotenie, ktoré zohľadňuje spôsob práce študenta, konkrétne jeho schopnosť používať digitálne zdroje, kriticky reflektovať návrhy strojového alebo generatívneho prekladu a dodržiavať etické zásady. Našou ambíciou bude preskúmať možnosti tvorby rubriík, dotazníkov alebo hodnotiacich protokolov pre právny preklad, ktoré by spájali odbornú, digitálnu a etickú dimenziu prekladovej kompetencie.

Zoznam použitej literatúry

1. BJEL, Lucia: Corpora in Institutional Legal Translation: Small Steps and the Big Picture. In: Institutional Translation for International Governance: Enhancing Quality in Multilingual Legal Communication, 2018. S. 25–36. Dostupné online: https://www.researchgate.net/publication/341883578_Corpora_in_Institutional_Legal_Translation_Small_Steps_and_the_Big_Picture
2. CLÉMENT-WILZ, Laure – DE LAFORCADE, Agata – CENNAMO, Ilaria: Translation in the European Union: Navigating Technical and Legal Issues in the Light of Artificial Intelligence — Conclusions. In: International Journal of Language & Law, 14, 2025. S. 240-255. DOI: 10.14762/jll.2025.240

3. EATON, Sarah Elaine: Postplagiarism: transdisciplinary ethics and integrity in the age of artificial intelligence and neurotechnology. In: *International Journal of Educational Integrity*, roč. 19, č. 23, 2023. S. 1-10. ISSN 1833-2595. Dostupné online: <https://doi.org/10.1007/s40979-023-00144-1>
4. ISO (2017) ISO 18587 Translation Services – Post-editing of Machine Translation Output – Requirements, Geneva: International Standards Office
5. GIAMPIERI, Patrizia: The use of AI in the translation of legal documents: A critical analysis. In: *trans-kom*, roč. 17, č. 2, 2024. S. 343–358. ISSN 1867-4844. Dostupné online: https://www.trans-kom.eu/bd17nro2/trans-kom_17_02_05_Giampieri_AI.2024.1128.pdf
6. JIAO, Wenxiang – WANG, Wenxuan – HUANG, Jen-tse – WANG, Xing – SHI, Shuming: Is ChatGPT A Good Translator? Yes With GPT-4 As The Engine. 2023. In: arXiv:2301.08745
7. KOPONEN, Maarit: Is Machine Translation Post-editing Worth the Effort? A Survey of Research into Post-editing and Effort. In: *The Journal of Specialized Translation*, 25, 2019. S.131-148. ISSN 1740-357X
8. PALANICHAMY, Naveen – TROJOVSKÝ, Pavel: Overview and challenges of machine translation for contextually appropriate translations. In: *iScience*, roč. 27, č. 10, 110878, 2024. ISSN 2589-0042. Dostupné online: <https://doi.org/10.1016/j.isci.2024.110878>
9. PRIETO RAMOS, Fernando: Embracing New Translation Technologies at International Organizations: Translators' Perceptions of Machine Translation and its Impact on Institutional Translation. In: *International Journal of Language & Law*, roč. 14, č. 1, 2025. S. 1–29. ISSN: 2194-7414. DOI: 10.14762/jll.2025.001
10. PRIETO RAMOS, Fernando: Revisiting translator competence in the age of artificial intelligence: the case of legal and institutional translation. In: *The Interpreter and Translator Trainer*, roč. 18, č. 2, 2024. S. 148–173. ISSN 1757-0417. DOI: 10.1080/1750399X.2024.2344942
11. PYM, Antony – HAO, Yu: *How to Augment Language Skills: Generative AI and Machine Translation in Language Learning and Translator Training*. Londýn a New York: Routledge, 2025. 218 s. ISBN 978-1-032-61495-3. DOI: 10.4324/9781032648033
12. ŠARČEVIĆ, Susan: *New Approach to Legal Translation*, Kluwer Law International, 2008. 308 s. ISBN 90 411 0401 01
13. VAN DER VORST, Tommy – JELICIC, Nick: Artificial Intelligence in Education: Can AI bring the full potential of personalized learning to education? In: 30th European Conference of the International Telecommunications Society (ITS):

"Towards a Connected and Automated Society", Helsinki, Finland, 16.–19. 6. 2019. Calgary: International Telecommunications Society (ITS). Dostupné online: <https://hdl.handle.net/10419/205222>

14. VASWANI, A. – SHAZEER, N. – PARMAR, N. – USZKOREIT, J. – JONES, L. – GOMEZ, A. N. – KAISER, L. – POLOSUKHIN, I.: Attention Is All You Need. In: Advances in Neural Information Processing Systems, 2017. Dostupné online <https://doi.org/10.48550/arXiv.1706.03762>
15. WANG, Haifeng – WU, Hua – HE, Zhongjun – HUANG, Liang – CHURCH, Kenneth Ward: Progress in Machine Translation. In: Engineering, 18, 2022. S. 143–153. ISSN 2095-8099. Dostupné online: <https://doi.org/10.1016/j.eng.2021.03.023>

Internetové zdroje:

1. <https://iate.europa.eu/home>
2. <https://eur-lex.europa.eu/homepage.html>
3. <https://www.slov-lex.sk/>
4. <https://www.juremy.com/about/>
5. <https://www.writefull.com>
6. <https://www.grammarly.com>
7. <https://knowledge-centre-translation-interpretation.ec.europa.eu/en/EU-funded-research-projects-on-translation>
8. www.multitrainmt.eu/index.php/en/
9. https://commission.europa.eu/system/files/2018-02/emt_competence_fw_k_2017_en_web.pdf
10. https://commission.europa.eu/document/download/b482a2c0-42df-4291-8bf8-923922ddc6e1_en?filename=emt_competence_fw_k_2022_en.pdf

Kontaktné údaje

Mgr. Sylvia Mičíková, PhD.

sylvia.micikova@flaw.uniba.sk

Ústav cudzojazyčnej právnej komunikácie, PraF UK

Mgr. Bc. Sandra Banková

sandra.bankova@flaw.uniba.sk

Ústav cudzojazyčnej právnej komunikácie, PraF UK

UMELÁ INTELIGENCIA VO VÝUČBE ANGLICKEJ PRÁVNEJ TERMINOLÓGIE: PRÍNOSY A LIMITY

ARTIFICIAL INTELLIGENCE IN TEACHING ENGLISH LEGAL TERMINOLOGY: BENEFITS AND LIMITATIONS

Jarmila Brtková¹

Abstrakt: Umelá inteligencia je fenoménom dnešnej doby, ktorý výrazne zasahuje do všetkých oblastí pracovného aj osobného života a čoraz významnejšie ovplyvňuje aj vzdelávací proces a akademickú sféru. Napriek určitým pochybnostiam, obavám a množstvu nezodpovedaných otázok je očividné, že jej vplyv na vzdelávanie bude zásadný a dlhodobý. Ako inovatívny nástroj otvára nové perspektívy aj vo vysokoškolskom vzdelávaní, keďže umožňuje individualizovať výučbu, vytvárať študijné materiály prispôbené individuálnym potrebám študentov, poskytovať systematickú spätnú väzbu a zároveň efektívnejšie a presnejšie hodnotiť ich práce. Cieľom príspevku je poskytnúť komplexný pohľad na možnosti a prínosy, ktoré ponúka generatívna AI vo výučbe anglickej právnej terminológie v rámci angličtiny pre špecifické účely (ESP), a zároveň poukázať na jej limity a riziká z pohľadu učiteľov ESP. Výsledky prieskumu realizovaného medzi učiteľmi ESP odhaľujú potenciál umelej inteligencie podporiť proces osvojovania si anglickej právnej terminológie, zvýšiť motiváciu a autonómiu študentov, ale aj problémy spojené s presnosťou, kontextualizáciou a odbornosťou generovaných výstupov. Zároveň upozorňujú na nedostatok odborných školení pre učiteľov, etické otázky a obavy zo straty kritického myslenia a nadmerného spoliehania sa študentov na AI.

Kľúčové slová: ESP, generatívna AI, vnímanie učiteľov, anglická právna terminológia, vysokoškolské vzdelávanie

Abstract: Artificial intelligence is a contemporary phenomenon that significantly affects all areas of professional and personal life and is increasingly influencing the educational process and the academic sphere. Despite certain doubts, concerns, and many unanswered questions, it is evident that its impact on education will be both fundamental and long-term. As an innovative tool, it also opens new perspectives in higher education, as it enables the

¹ Univerzita Komenského v Bratislave, Právnická fakulta, Ústav cudzojazyčnej právnej komunikácie

individualization of teaching, the development of study materials tailored to students' needs, the provision of systematic feedback, and more efficient and accurate assessment of student work. The aim of this paper is to provide a comprehensive overview of the opportunities and benefits that generative AI offers in teaching English legal terminology within English for Specific Purposes (ESP), while also highlighting its limitations and risks from the perspective of ESP teachers. The results of the survey conducted among ESP teachers reveal the potential of artificial intelligence to support the acquisition of English legal terminology, enhance students' motivation and autonomy, but also the challenges related to the accuracy, contextualization, and professional quality of generated outputs. At the same time, they draw attention to the lack of specialized teacher training, ethical issues, and concerns about the loss of critical thinking and students' overreliance on AI.

Keywords: ESP, generative AI, teachers' perceptions, English legal terminology, higher education

Úvod

Umelá inteligencia sa v posledných rokoch stala neodmysliteľnou súčasťou nášho života a jednou z kľúčových tém akademickej a odbornej diskusie. Jej dynamický rozvoj zasahuje do viacerých oblastí spoločenského života vrátane vzdelávania, kde otvára nové možnosti, ale zároveň prináša aj početné výzvy. Špecifickú pozornosť je potrebné venovať využitiu generatívnej AI v oblasti výučby anglickej právnej terminológie, ktorá je súčasťou Angličtiny pre špecifické účely (English for Specific Purposes - ESP).² Právnická angličtina (v odbornej literatúre pod názvom English for Legal Purposes - ELP) si totiž vyžaduje nielen vysokú úroveň jazykových zručností, ale aj porozumenie právnomu kontextu, v ktorom sa terminológia používa.

Výučba právnickej angličtiny sa začala systematickejšie rozvíjať od druhej polovice 20. storočia v súvislosti s rastúcou internacionalizáciou práva a globalizáciou právnej praxe. ESP sa etablovalo ako samostatný prúd jazykového vzdelávania zameraného na potreby konkrétnych profesií, medzi ktorými právnici predstavujú jednu z najnáročnejších skupín. Efektívna výučba právnickej angličtiny si vyžaduje hlbokú integráciu jazyka a právneho obsahu s dôrazom na autentické texty, praktické cvičenia a komunikačné zručnosti viazané na danú profesiu, ktoré pripravujú študentov na požiadavky právnickej praxe.³ Ako upozorňujú viacerí autori, práve v

² Podrobnejšie k tejto téme pozri: HUTCHINSON, Tom - WATERS, Alan: English for Specific Purposes. A learning-centred approach. Cambridge: Cambridge University Press, 2010.

³ GIBBONS, John: Forensic Linguistics: An Introduction to Language in the Justice System. Oxford, UK: Wiley Blackwell, 2003, p. 8.

oblasti právnickej angličtiny sa odborné a jazykové vzdelávanie prelínajú výraznejšie než v iných disciplínach, keďže jazyk je pre právnikov primárnym nástrojom výkonu povolania.⁴

Učitelia ESP si preto kladú otázku, ako môže AI podporiť proces osvojovania si právnej terminológie a do akej miery môže byť jej integrácia do výučby prínosná. Generatívne nástroje ako napr. ChatGPT alebo Gemini dokážu študentom sprostredkovať okamžitý prístup k rozsiahlym jazykovým zdrojom, zvýšiť ich motiváciu a posilniť autonómiu pri práci s odborným textom. Umelá inteligencia však nemôže nahradiť úlohu učiteľov pri poskytovaní emocionálnej podpory, kritického vedenia a ľudskej interakcie.⁵ Zároveň sa objavujú zásadné problémy spojené s presnosťou a odbornosťou generovaných výstupov, rizikom nadmerného spoliehania sa na digitálne technológie či otázkami etickej povahy. Táto situácia je ešte komplikovanejšia vzhľadom na to, že väčšina učiteľov ESP nedisponuje systematickým odborným školením v oblasti umelej inteligencie a jej pedagogického využitia. Chýbajúce vzdelávanie môže viesť k neistote v praxi, k nedostatočnej kontrole kvality generovaných výstupov či k neschopnosti efektívne usmerniť študentov pri práci s AI nástrojmi.

Cieľom tohto článku je analyzovať prínosy a limity umelej inteligencie vo výučbe anglickej právnej terminológie z perspektívy učiteľov ESP a poukázať na to, akým spôsobom môže AI dopĺňať, no nie nahrádzať, tradičné didaktické prístupy.

K problematike umelej inteligencie

Umelá inteligencia je fenomén, ktorý zásadne mení takmer všetky oblasti nášho života vrátane vysokoškolského vzdelávania. S príchodom veľkých jazykových modelov, ako sú ChatGPT⁶ či Gemini, sa objavujú rôzne názorové prúdy: jedni hovoria **s obavou o revolúcii umelej inteligencie, ktorá v histórii nemá obdobu**, iní ju prirovnávajú k nástupu počítačov či internetu, ktoré spočiatku vyvolávali obavy, no dnes sú bežnou súčasťou života. Vzhľadom na šírku a dynamiku tejto problematiky

⁴ CHOVANCOVÁ, Barbora: Training Legal Skills in the ESP Classroom: Mediation Activities and Student Self-Reflection. In: *Hermes – Journal of Language and Communication in Business*, 64, (2024), s. 138.

⁵ ZHANG, Zhijuan: The role of artificial intelligence tools on Chinese EFL learners' self-regulation, resilience and autonomy. In: *European Journal of Education*, 60 (2), (2025), s. 12.

⁶ ChatGPT (Chat Generative Pre-trained Transformer), vyvinutý spoločnosťou OpenAI, je veľký jazykový model (LLM) založený na architektúre transformátora. Mechanizmus pozornosti mu umožňuje analyzovať kontext vstupov a generovať koherentné textové výstupy. V krátkom čase sa etabloval ako jeden z najpoužívanějších digitálnych nástrojov. Podrobnejšie k tejto téme pozri: XU, Wendi – WANG, Xianpeng – GUO, Qingxin – SONG, Xiangman – ZHAO, Ren – ZHAO, Guodong – HE, Dakuo – XU, Te – ZHANG, Ming – YANG, Yang: Decomposition is all you need: single-objective to multi-objective optimization towards artificial general intelligence. *Mathematics*, 11(20), (2023), 4390.

nie je jednoduché sa v nej zorientovať, preto je potrebné najskôr objasniť samotný pojem umelej inteligencie.

AI patrí medzi emergentné technológie⁷ a zahŕňa nielen jazykové chatboty, ale aj autonómne autá, bezpilotné lietadlá či systémy rozpoznávania obrazu. Termín „*artificial intelligence*“ použili prvýkrát John McCarthy a Marvin Minsky na konferencii v Dartmouth College v roku 1956, čím položili základný kameň jej vývoja.⁸ Odvtedy **sa rozvíjala nielen samotná technológia, ale aj diskusia o tom, čo vlastne pojem umelá inteligencia znamená.**

Dodnes však neexistuje jednotná, univerzálna definícia – jej vymedzenie sa líši podľa toho, či sa zdôrazňuje technický, filozofický alebo právny aspekt. Russell a Norvig ju opisujú ako „*vedeckú disciplínu, ktorá sa zaoberá tvorbou systémov schopných vykazovať inteligentné správanie podobné človeku.*“⁹ Podľa Spana je AI odlišná od ľudskej inteligencie, keďže ide o oblasť informatiky usilujúcu sa reprodukovať činnosti ľudského mozgu, ako je vnímanie sveta prostredníctvom zmyslov, porozumenie a reakcia na reč, schopnosť učiť sa, plánovať a riešiť problémy.¹⁰

Rozmanitosť pohľadov na AI a jej rýchly rozvoj však vyvolali potrebu jasných pravidiel. Z právneho hľadiska preto predstavuje zásadný krok prijatie Nariadenia o umelej inteligencii (AI Act)¹¹, ktoré je prvým komplexným právnym rámcom na reguláciu umelej inteligencie v Európskej únii. Jeho cieľom je zabezpečiť, aby boli systémy AI bezpečné, transparentné a v súlade so základnými právami a etickými princípmi, pričom dôležitý dôraz sa kladie aj na ich zodpovedné využívanie vo vzdelávacom procese.

⁷ Slovo „emergentný“ pochádza z latinského „*emergens*“, čo je príčastie od slovesa „*emergere*“, teda „*vynoriť sa*“ alebo „*objaviť sa*“. (PRAŽÁK, Jozef M. – NOVOTNÝ, František – SEDLÁČEK, Jozef: Latinsko-český slovník. Praha: Státní pedagogické nakladatelství, 1955. s. 468) Emergentné technológie sú rýchlo sa rozvíjajúce technológie, ktoré majú potenciál výrazne zmeniť spoločnosť, priemysel alebo spôsob života.

⁸ SPANO, Martin: Umelá inteligencia v orechovej škrupinke: Stručný úvod do umelej inteligencie, strojového učenia, neurónových sietí, hlbokého učenia a robotov. 1. vyd. Bratislava: Žive.sk, 2019. s. 12.

⁹ RUSSELL, Stuart - NORVIG Peter: Artificial Intelligence – A Modern Approach. New Jersey: Pearson Education, Inc., 2010. s. 1.

¹⁰ SPANO, Martin: Umelá inteligencia v orechovej škrupinke: Stručný úvod do umelej inteligencie, strojového učenia, neurónových sietí, hlbokého učenia a robotov. 1. vyd. Bratislava: Žive.sk, 2019. s. 15.

¹¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)

Prehľad literatúry: AI vo výučbe ESP

Problematike využívania umelej inteligencie vo výučbe ESP sa v posledných rokoch venovalo viacero autorov. Merino-Campos (2025)¹² zdôrazňuje, že nástroje umelej inteligencie umožňujú individualizovať obsah a tempo výučby, čo je obzvlášť dôležité pri odbornom jazyku, kde sa úroveň študentov výrazne líši. Na personalizáciu a okamžitú spätnú väzbu nadväzujú aj Marzuki (2023)¹³ či Pham a Cao (2025)¹⁴, ktorí ukázali, že ChatGPT zvyšuje motiváciu a angažovanosť študentov v kurzoch ESP a zároveň odbremeňuje učiteľov od rutinných úloh.

Osobitná pozornosť sa venuje právnickej angličtine, kde viacerí autori potvrdzujú efektívnosť AI pri precvičovaní odborného písania a terminológie. Shestakova (2023)¹⁵, Bretan (2024)¹⁶ a Xatamova a Ashurov (2024)¹⁷ zdôrazňujú, že nástroje umelej inteligencie dokážu poskytnúť modelové texty a cvičenia šité na mieru právnickému diskurzu. Podobne Boeru (2024)¹⁸, Georgieva (2025)¹⁹ či El-Farahaty (2025)²⁰ ukázali, že AI je prínosná aj v iných profesijných oblastiach, keďže dokáže identifikovať konkrétne jazykové chyby a generovať doplnkové materiály. Savitri et al. (2025)²¹ poukázali na to, že AI chatboti podporujú interaktivitu a samostatné precvičovanie ESP.

¹² MERINO-CAMPOS, Carlos: The Impact of Artificial Intelligence on Personalized Learning in Higher Education: A Systematic Review. In: Trends in Higher Education, 4 (2), (2025), 17, s. 1.

¹³ MARZUKI – WIDIATI, Utami – RUSDIN, Diyenti – DARWIN & INDRAWATI, Inda: The impact of AI writing tools on the content and organization of students' writing: EFL teachers' perspective. In: Cogent Education, 10 (2), (2023), 2236469. s. 12.

¹⁴ PHAM, Manh Tri – CAO, Thi Xuan Tu: The Practice of ChatGPT in English Teaching and Learning in Vietnam: A Systematic Review. In: International Journal of TESOL & Education, 5 (1), (2025), s. 52.

¹⁵ SHESTAKOVA, Elizaveta: Using Generative AI in ESP Classes to Teach Formal Style. In: SSRN Electronic Journal, (2023).s. 2.

¹⁶ BRETAN, Bianca Doris: Teaching and Learning Legal English with AI: A Case Study on Student Engagement in an ESAP Course. In: Studia Universitatis Babeş-Bolyai – Philologia, 69 (4), (2024), s. 166-167.

¹⁷ XATAMOVA, Nodiraxon – ASHUROV, Jahongir: The Future of Legal English Learning: Integrating AI into ESP Education. In: SPAST Reports, 1 (7), (2024), s. 6.

¹⁸ BOERU, Mariana: Exploring the Use of AI Tools in Teaching English for Specific Purposes (ESP). In: Scientific Bulletin of Naval Academy, 27 (1), (2024), s. 92.

¹⁹ GEORGIEVA, Valentina: Embracing the Inevitable: Tips for EFL and ESP Learning with AI. In: E-Learning Innovations Journal, 3(1), (2025). s. 101.

²⁰ EL-FARAHATY, Hala: Integrating Corpora and AI Tools in the Teaching, Learning, and Assessing of Arabic/English Legal Translation. In: International Journal for the Semiotics of Law, 38 (6), (2025), s. 2050.

²¹ SAVITRI, Wiwiet Eva – NUGROHO, Him'mawan Adi – MUNIR, Ahmad – PUSPARINI, Ririn – KURNIASIH, Esti – ARINDA, Desi: Perspectives of pre-service English teachers on AI chatbots in ESP worksheet development. In: JOLLT Journal of Languages and Language Teaching, 13 (1), (2025), s. 430-431.

K viacerým pozitívnym aspektom patrí aj psychologická podpora študentov. Crompton a kol. (2024)²² zistili, že AI znižuje úzkosť pri používaní cudzieho jazyka a umožňuje študentom bezpečne experimentovať s odborným vyjadrovaním. Asrifan (2025)²³ a Silitonga a kol. (2025)²⁴ zase zdôrazňujú, že AI podporuje spoluprácu a rozširovanie slovnej zásoby, čo je v ESP kľúčové. Kovačević (2023)²⁵ uvádza, že ChatGPT môže podporovať rozvoj digitálnych zručností a kreativity učiteľov. Zároveň však viacerí autori upozorňujú na limity využívania AI v ESP. Selwyn (2024)²⁶ upozorňuje, že generatívna AI produkuje len štatistické simulácie bez ľudskej tvorivosti. Pham a Luong (2025)²⁷ varujú, že nadmerné spoliehanie sa na technológie môže viesť k oslabeniu kritického myslenia a k plagiátorstvu. Etické otázky spojené s ochranou dát a akademickou integritou analyzujú Zeide (2019)²⁸, Babu a kol. (2024).²⁹ Podľa štúdie Memarian a Doleck (2023)³⁰ sa medzi ďalšie problémy radí aj nedostatok vyšších kognitívnych schopností, obmedzená transparentnosť fungovania modelov a neistá kvalita dát, čo môže viesť k nespoľahlivým alebo príliš všeobecným odpovediam.

²² CROMPTON, Helen; EDMETT, Adam; ICHAPORIA, Neenaz; BURKE, Diane: AI and English Language Teaching: Affordances and Challenges. In: *British Journal of Educational Technology*, 55 (6), (2024), 2521–2522.

²³ ASRIFAN, Andi – CARDOSO, Luís Miguel Oliveira de Barros – VARGHEESE, K. J.: Fostering collaborative learning in ESP: AI-driven approaches integrating learning styles and multiple intelligences. In: *Englisia: Journal of Language, Education, and Humanities*, 12 (2), (2025), s. 291.

²⁴ SILITONGA, Lusía – WIYAKA, Wiyaka – PRASTIKAWATI, Entika Fani: Boosting students' ESP vocabulary by utilizing AI chatbot. In: *ETERNAL (English Teaching Journal)*, 15 (2), (2024), s. 279.

²⁵ KOVAČEVIĆ, Darko: Use of ChatGPT in ESP Teaching Process. In: 22nd International Symposium INFOTEH-JAHORINA, (2023), s. 4.

²⁶ SELWYN, Neil: On the Limits of Artificial Intelligence (AI) in Education. In: *Nordisk tidsskrift for pedagogikk og kritikk*, 10, (2024), s. 6.

²⁷ PHAM, Thi Thuy Dung – LUONG, Minh Hieu: Students' Challenges in Employing AI Tools in Legal Writing. In: *International Journal of TESOL & Education*, 5 (2), (2025), s. 82.

²⁸ ZEIDE, Elana: Artificial Intelligence in Higher Education: Applications, Promise and Perils, and Ethical Questions. In: *EDUCAUSE Review*, 54 (3), (2019), s. 7.

²⁹ BABU, Md. Asaduzzaman – YUSUF, Kazi Md. – ENI, Lima Nasrin – JAMAN, Shekh Md. Sahiduj – SHARMIN, Mst. Rasna: ChatGPT and Generation 'Z': A study on the usage rates of ChatGPT. In: *Social Sciences & Humanities Open*, 10, (2024), s. 2.

³⁰ MEMARIAN, Bahar – DOLECK, Tenzin: ChatGPT in education: Methods, potentials, and limitations. In: *Computers in Human Behavior: Artificial Humans*, 1, (2023), s. 6.

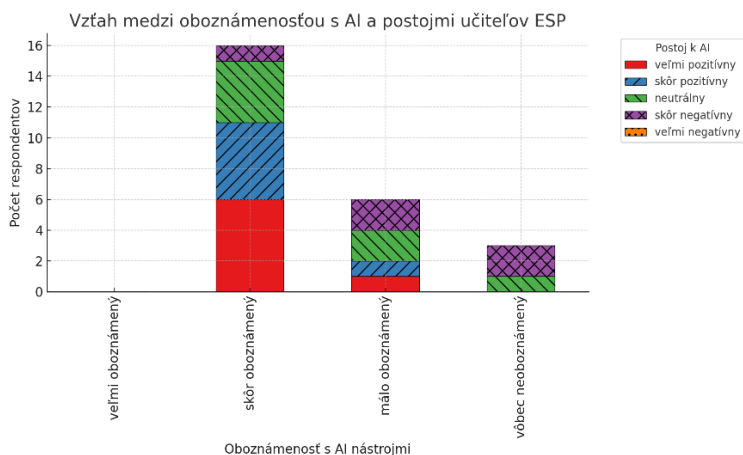
Výsledky prieskumu: prínosy a limity AI

Cieľom nasledujúcej časti je analyzovať vybrané výsledky prieskumu,³¹ ktorý bol uskutočnený v júni 2025 medzi učiteľmi ESP. Do prieskumu sa zapojilo 27 respondentov z dvanástich fakúlt slovenských univerzít, ktorí vyplnili dotazník s 15 otázkami. Ten obsahoval uzavreté (Likertova škála, výber odpovedí) aj otvorené otázky a zameriaval sa na postoje učiteľov k využívaniu umelej inteligencie vo výučbe ESP, znalosť a používanie AI nástrojov, vnímané prínosy a obavy, skúsenosti so školeniami a očakávania do budúcnosti. Keďže prieskum mapoval viacero oblastí, v tomto článku sú spracované len výsledky týkajúce sa vnímaných prínosov a limitov využívania umelej inteligencie vo výučbe ESP.

Prieskum ukázal, že z celkového počtu 27 učiteľov ESP už 20 (74 %) využilo umelú inteligenciu vo výučbe, zatiaľ čo 7 (26 %) ju zatiaľ nepoužilo, čo naznačuje aktívny, hoci nie vždy fundovaný prístup k technológiám. Pokiaľ ide o postoje, väčšina respondentov hodnotí AI pozitívne: „veľmi pozitívny“ postoj uviedlo 33,3 % a „skôr pozitívny“ 22,2 %, pričom neutrálny postoj zaujalo 25,9 % a „skôr negatívny“ 18,5 %; možnosť „veľmi negatívny“ ne zvolil nikto. Výsledky naznačujú prevažne pozitívne hodnotenie, pričom neistota u časti učiteľov podčiarkuje potrebu ďalšej podpory a systematického vzdelávania. Z hľadiska oboznámenosti s AI nástrojmi sa 59,3 % respondentov označilo za „skôr oboznámených“ (väčšinou samoukovia, ktorí využívajú aj rozšírené platené verzie nástrojov, ako je ChatGPT), 22,2 % za „málo oboznámených“, 11,1 % za „vôbec neoboznámených“ a 7,4 % zvolilo neutrálnu možnosť; možnosť „veľmi oboznámený“ neuviedol nikto.

Keď sme sa bližšie pozreli na vzťah medzi oboznámenosťou a postojmi, ukázalo sa, že respondenti s „veľmi pozitívnym“ alebo „skôr pozitívnym“ prístupom sú väčšinou zároveň „skôr oboznámení“ alebo „veľmi oboznámení“ s AI nástrojmi. Naopak, neutrálny alebo negatívny postoj sa častejšie viaže na nižšiu úroveň oboznámenosti. Ako znázorňuje graf č. 1, táto tendencia poukazuje na možnú pozitívnu koreláciu medzi znalosťou AI nástrojov a ich akceptáciou – čím lepšie sú učitelia oboznámení s týmito technológiami, tým pozitívnejšie ich hodnotia a sú otvorenejší ich používaniu v praxi.

³¹ Ďalšie detailné výsledky prieskumu uvádzame v článku: PROCHÁZKOVÁ, Lenka – BRTKOVÁ, Jarmila – KEČKA, Roman: When AI meets ESP: Exploring AI in English for specific purposes in higher education from the teachers' perspective. In: Aplikované jazyky v univerzitnom kontexte (12), (2025), s. 177-187.



Graf č. 1

Postoje k AI podľa oboznámenosti s nástrojmi

Čo sa týka prínosov umelej inteligencie vo výučbe ESP, prieskum potvrdil, že učitelia vnímajú AI predovšetkým ako nástroj, ktorý šetrí čas a znižuje pracovnú záťaž najmä pri príprave materiálov. Až 85,2 % respondentov súhlasilo, že AI uľahčuje tvorbu materiálov prispôbených potrebám študentov, čím sú učitelia odbremenení od potreby zostavovať rôznorodé cvičenia či modelové dokumenty. Toto zistenie je v súlade aj s výskumom, ktorý uskutočnila spoločnosť Anthropic vo Veľkej Británii medzi vysokoškolskými pedagógmi, kde 34 % učiteľov uviedlo, že sa im vďaka AI znížila pracovná záťaž, a 49 % dokonca potvrdilo, že pociťujú menší stres.³²

Podľa nášho prieskumu sa najčastejšie AI využíva na tvorbu ESP materiálov (17 učiteľov, 63 %), na prípravu plánov hodín (14, 51,9 %) a na precvičovanie odbornej terminológie (11, 40,7 %). V menšej miere sa používa na opravu a zlepšovanie jazykových výstupov (10, 37 %), administratívu (3, 11,1 %) či hodnotenie úloh (2, 7,4 %). Niektorí učitelia uviedli aj iné formy využitia, napríklad preklad odborných textov, tvorbu testových otázok do systému Moodle alebo vyhľadávanie vhodných vzdelávacích videí.

AI sa ukazuje ako významná podpora v oblasti plánovania a diferenciacie výučby. Podľa 77,8 % respondentov dokáže efektívne naplánovať hodiny ESP prispôbené konkrétnym odborom a potrebám študentov. Okrem tvorby osnov a kurzov na mieru dokáže rýchlo generovať personalizované úlohy podľa jazykovej úrovne študenta, čím posilňuje individualizáciu a samostatné učenie. Tento prínos potvrdilo aj 66,7 % učiteľov, ktorí uviedli, že AI podporuje autonómiu študentov. Učitelia zároveň oceňovali možnosť tvoriť nové interaktívne materiály s pomocou AI, ako napríklad

³² ANTHROPIC: Anthropic Education Report: How Educators Use Claude. In: Anthropic [online]. 27. 8. 2025. Dostupné na: <https://www.anthropic.com/news/anthropic-education-report-how-educators-use-claude>.

simulácie, rolové hry či vizuálne pomôcky, ktoré zvyšujú atraktivitu výučby. AI zároveň mení dynamiku vzťahu medzi študentom a učiteľom, posúva učiteľa od tradičnej roly poskytovateľa poznatkov k facilitátorovi učenia, pričom dôraz sa kladie na vedenie procesu učenia a rozvoj kritického myslenia.

Ďalšou prínosnou oblasťou je spätná väzba a hodnotenie. AI dokáže rýchlo opravovať cvičenia z gramatiky a slovnej zásoby, pripravovať rubriky pre odborné prezentácie či písomné úlohy, čo umožňuje učiteľovi viac sa sústrediť na obsah, štýl a odbornú presnosť. V administratíve môže šetriť čas pri písaní grantov, vedení záznamov či sumarizovaní údajov a zároveň podporuje odborný rozvoj učiteľov, keďže pomáha pri rýchlom vyhľadávaní literatúry a brainstormingu.

Učitelia zároveň oceňujú dostupnosť a „nekonečnú trpezlivosť“ AI nástrojov. Funkcia *Guided Learning* (Gemini) umožňuje viesť študentov krok za krokom, kladť im otázky a poskytovať vizuálne vysvetlenia. To prináša nové možnosti pre flexibilné a inkluzívne vzdelávanie, dostupné bez časových či priestorových obmedzení. Celkovo 77,8 % učiteľov sa zhodlo, že AI môže účinne podporovať výučbu ESP, pričom len 3,7 % s týmto tvrdením nesúhlasilo.

V prieskume sme sa okrem prínosov zamerali aj na možné riziká a obavy učiteľov z používania AI vo výučbe ESP. Z odpovedí vyplynulo viacero oblastí, ktoré pedagógovia vnímajú ako problematické a ktoré si vyžadujú zvýšenú pozornosť pri implementácii AI do vzdelávacieho procesu.

Jednou z najčastejšie uvádzaných obáv je riziko nadmerného spoliehania sa študentov na AI, čo môže viesť k duševnej lenivosti, k oslabovaniu kritického myslenia, kreativity a schopnosti samostatne produkovať jazykové výstupy. Ako upozorňuje Gerlich (2023) vo svojom výskume, časté využívanie chatbotov môže spôsobovať pokles kognitívnych schopností a znižovať schopnosť kriticky vyhodnocovať informácie. Ako riešenie navrhuje systematickú osvetu, tréning zručností a podporu študentov v orientácii na samotný proces učenia, nielen na výsledok.³³

Medzi ďalšie obavy učiteľov ESP patria etické otázky a riziko podvádzania. Učitelia upozorňujú, že je čoraz ťažšie rozlíšiť, či text vypracoval samotný študent alebo ho generovala AI, a práve z tohto dôvodu tradičné eseje postupne strácajú svoj význam. Existujúce detektory AI sú často nepresné a môžu predstavovať riziko porušenia súkromia, preto sa pedagógovia spoliehajú skôr na identifikáciu znakov typických pre AI, ako sú mechanický až neosobný tón, prehnane dokonalá gramatika, zabudnuté prompty, falošné citácie či nesúlad s bežnou úrovňou študenta.

Ďalšou často spomínanou obavou je nedostatočná digitálna pripravenosť samotných pedagógov, keďže mnohí z nich nemajú odborné školenia a môžu zaostávať za

³³ GERLICH, Michael: *AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking*. In: *Societies*, 15 (1), (2025), 6.

študentmi v digitálnych zručnostiach. Tento problém ešte viac prehľbuje digitálna nerovnosť, keďže nie každý má prístup k pokročilým alebo plateným verziám AI nástrojov. Situáciu zároveň zhoršuje slabá reakcia univerzít na rýchly rozvoj AI, ktorá sa prejavuje v nedostatočnej metodologickej podpore.

Učitelia sa obávajú aj postupnej straty tradičných akademických zručností, akými sú samostatný výskum, originálne písanie či analytické schopnosti, keďže AI môže viesť k tzv. kognitívnemu odľahčeniu. V odborných kontextoch je navyše potrebné počítať s rizikom chýb, nepravdivých alebo zavádzajúcich výstupov či dokonca ideologickej manipulácie prostredníctvom AI. Nemenej dôležité sú aj otázky ochrany súkromia a dodržiavania pravidiel GDPR, keďže existuje riziko úniku citlivých údajov.

Napokon, viacerí učitelia upozorňujú na riziko straty osobného kontaktu medzi učiteľom a študentom, ktorý je neoddeliteľnou súčasťou akademického prostredia. Tieto zistenia sú v súlade s Johnom (2025), ktorý rovnako konštatuje, že nadmerné využívanie AI môže oslabovať prirodzenú interakciu medzi učiteľom a študentom.³⁴ Hoci traja respondenti (11,1 %) neuviedli žiadne obavy, väčšina zdôraznila potrebu jasných smerníc a systematických školení, ktoré by pomohli minimalizovať negatívne dôsledky využívania AI vo vzdelávaní.

AI ako podpora výučby anglickej právnej terminológie

Umelá inteligencia predstavuje efektívny nástroj aj pri výučbe anglickej právnej terminológie, keďže dokáže generovať zoznamy pojmov podľa jednotlivých právnych odvetví, ponúknuť definície a autentické príklady ich použitia v zmluvách, súdnych rozhodnutiach či právnych stanoviskách, ako aj rozlišovať medzi synonymami, ktoré bývajú pre študentov mätúce (napr. *breach* vs. *violation*). Zároveň vie vysvetľovať archaické a cudzie výrazy (*hereinafter*, *obiter dictum*) či bežné slová so špecifickým právnym významom (*consideration*, *action*).

Okrem pasívneho osvojovania právnej terminológie umožňuje AI tvoriť interaktívne cvičenia, kartičky alebo prípadové štúdie, vďaka čomu študenti získavajú nielen slovnú zásobu, ale aj schopnosť terminológiu prakticky aplikovať. AI dokáže generovať alebo adaptovať autentické právne dokumenty – zmluvy, žaloby, rozhodnutia či právne stanoviská - ktoré študenti môžu analyzovať a cvične prekladať. Takto sa pripravujú na reálne situácie, v ktorých je presnosť terminológie rozhodujúca. Jednou z najsilnejších stránok AI je možnosť interakcie 24/7. Chatboty dokážu simulovať právne dialógy - napríklad rozhovor medzi advokátom a klientom alebo rokovanie medzi dvoma stranami sporu. Študenti si v takýchto simuláciách precvičia používanie právnej terminológie v reálnom kontexte a zároveň získajú

³⁴ JOHN, Aby: Exploring the Impact of Artificial Intelligence on Language Acquisition, Linguistic Development, and Language Use: A Case Study from India. In: *Forum for Linguistic Studies*, 7 (3), (2025), s. 1114.

okamžitú spätnú väzbu. Výučba anglickej právnej terminológie sa tak stáva dynamickejšou a cielenejšou, čo prispieva k lepšej pripravenosti študentov na právnu prax.

Záver

Výsledky uskutočneného prieskumu potvrdzujú, že umelá inteligencia predstavuje v kontexte ESP významný inovačný nástroj, ale nikdy nemôže nahradiť učiteľa. Jej prínosy najmä v oblasti personalizácie, okamžitej spätnej väzby, motivácie študentov a zníženia pracovnej záťaže sú nespochybniteľné, ale súčasne sa objavujú riziká spojené s kvalitou odbornej jazykovej prípravy, etickými otázkami a nadmerným spoliehaním sa na umelú inteligenciu. Učitelia zároveň deklarujú potrebu jasného usmernenia zo strany univerzít a systematických školení, ktoré by mali prebiehať v spolupráci s IT odborníkmi. Len tak možno zabezpečiť, že AI bude využívaná v súlade s pedagogickými cieľmi a etickými zásadami. Prieskum bol však limitovaný veľkosťou vzorky, a preto nemožno jeho výsledky zovšeobecňovať. Napriek tomu môže poslúžiť ako východisko pre ďalší výskum v oblasti implementácie AI do ESP výučby. Vo všeobecnosti možno konštatovať, že umelá inteligencia je dobrým sluhom, ale zlým pánom. Jej zavádzanie do vzdelávania si vyžaduje opatrnosť, flexibilitu a neustálu reflexiu, aby sa inovácie stali skutočnou podporou učiteľov a študentov, nie hrozbou pre kvalitu a integritu akademického prostredia.

Zoznam použitej literatúry

1. ANTHROPIC: Anthropic Education Report: How Educators Use Claude. In: Anthropic [online]. 27. 8. 2025. Dostupné na: <https://www.anthropic.com/news/anthropic-education-report-how-educators-use-claude>.
2. ASRIFAN, Andi – CARDOSO, Luís Miguel Oliveira de Barros – VARGHEESE, K. J.: Fostering collaborative learning in ESP: AI-driven approaches integrating learning styles and multiple intelligences. In: *Englisia: Journal of Language, Education, and Humanities*, 12 (2), (2025), s. 275–298. Dostupné online na <https://doi.org/10.22373/ej.v12i2.29330>.
3. BABU, Md. Asaduzzaman – YUSUF, Kazi Md. – ENI, Lima Nasrin – JAMAN, Shekh Md. Sahiduj – SHARMIN, Mst. Rasna: ChatGPT and Generation 'Z': A study on the usage rates of ChatGPT. In: *Social Sciences & Humanities Open*, 10, (2024), 101163. Dostupné online na <https://doi.org/10.1016/j.ssaho.2024.101163>.
4. BOERU, Mariana: Exploring the Use of AI Tools in Teaching English for Specific Purposes (ESP). In: *Scientific Bulletin of Naval Academy*, 27 (1), (2024), s. 91–96. Dostupné online na <https://doi.org/10.21279/1454-864X-24-l1-013>.

5. BRETAN, Bianca Doris: Teaching and Learning Legal English with AI: A Case Study on Student Engagement in an ESAP Course. In: *Studia Universitatis Babeş-Bolyai – Philologia*, 69 (4), (2024), s. 153–168. Dostupné online na <https://doi.org/10.24193/subbphilolo.2024.4.07>.
6. CROMPTON, Helen; EDMETT, Adam; ICHAPORIA, Neenaz; BURKE, Diane: AI and English Language Teaching: Affordances and Challenges. In: *British Journal of Educational Technology*, 55 (6), (2024), 2503–2529. Dostupné online na <https://doi.org/10.1111/bjet.13460>.
7. EDMETT, Adam – ICHAPORIA, Neenaz – CROMPTON, Helen – CRICHTON, Ron: *Artificial intelligence and English language teaching: Preparing for the future (Second edition)*. In: *British Council Report*, (2024). Dostupné online na <https://doi.org/10.57884/78EA-3C69>.
8. EL-FARAHATY, Hala: Integrating Corpora and AI Tools in the Teaching, Learning, and Assessing of Arabic/English Legal Translation. In: *International Journal for the Semiotics of Law*, 38 (6), (2025), s. 2031–2060. Dostupné online na <https://doi.org/10.1007/s11196-025-10281-0>.
9. GEORGIEVA, Valentina: Embracing the Inevitable: Tips for EFL and ESP Learning with AI. In: *E-Learning Innovations Journal*, 3(1), (2025), s. 89–115. Dostupné online na <https://doi.org/10.57125/ELIJ.2025.03.25.05>.
10. GERLICH, Michael: *AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking*. In: *Societies*, 15 (1), (2025), 6. Dostupné online na <https://doi.org/10.3390/soc15010006>.
11. GIBBONS, John: *Forensic Linguistics: An Introduction to Language in the Justice System*. Oxford, UK: Wiley Blackwell, 2003. 352 s. ISBN 0-631-21246-9.
12. HUTCHINSON, Tom - WATERS, Alan: *English for Specific Purposes. A learning-centred approach*. Cambridge: Cambridge University Press, 2010. 183 s. ISBN 9780511733031.
13. CHOVANCOVÁ, Barbora: Training Legal Skills in the ESP Classroom: Mediation Activities and Student Self-Reflection. In: *Hermes – Journal of Language and Communication in Business*, 64, (2024), s. 137–148.
14. JOHN, Aby: Exploring the Impact of Artificial Intelligence on Language Acquisition, Linguistic Development, and Language Use: A Case Study from India. In: *Forum for Linguistic Studies*, 7 (3), (2025), s. 1104–1117. Dostupné online na <https://doi.org/10.30564/fls.v7i3.8671>.
15. KOVAČEVIĆ, Darko: Use of ChatGPT in ESP Teaching Process. In: 22nd International Symposium INFOTEH-JAHORINA, (2023), s. 1–5. Dostupné online na <https://doi.org/10.1109/INFOTEH57020.2023.10094133>.
16. MARZUKI – WIDIATI, Utami – RUSDIN, Diyenti – DARWIN & INDRAWATI, Inda: The impact of AI writing tools on the content and organization of students'

- writing: EFL teachers' perspective. In: *Cogent Education*, 10 (2), (2023), 2236469. Dostupné online na <https://doi.org/10.1080/2331186X.2023.2236469>.
17. MEMARIAN, Bahar – DOLECK, Tenzin: ChatGPT in education: Methods, potentials, and limitations. In: *Computers in Human Behavior: Artificial Humans*, 1, (2023), 100022. Dostupné online na <https://doi.org/10.1016/j.chbah.2023.100022>.
 18. MERINO-CAMPOS, Carlos: The Impact of Artificial Intelligence on Personalized Learning in Higher Education: A Systematic Review. In: *Trends in Higher Education*, 4 (2), (2025), 17. Dostupné online na <https://doi.org/10.3390/higheredu4020017>.
 19. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)
 20. PHAM, Manh Tri – CAO, Thi Xuan Tu: The Practice of ChatGPT in English Teaching and Learning in Vietnam: A Systematic Review. In: *International Journal of TESOL & Education*, 5 (1), (2025), s. 50–70.
 21. PHAM, Thi Thuy Dung – LUONG, Minh Hieu: Students' Challenges in Employing AI Tools in Legal Writing. In: *International Journal of TESOL & Education*, 5 (2), (2025), s. 75–86. Dostupné online na <https://doi.org/10.54855/ijte.25524>.
 22. PRAŽÁK, Jozef M. – NOVOTNÝ, František – SEDLÁČEK, Jozef: *Latinsko-český slovník*. Praha: Státní pedagogické nakladatelství, 1955. 743 s.
 23. PROCHÁZKOVÁ, Lenka – BRTKOVÁ, Jarmila – KEČKA, Roman: When AI meets ESP: Exploring AI in English for specific purposes in higher education from the teachers' perspective. In: *Aplikované jazyky v univerzitnom kontexte* (12), (2025), s. 177-187. (online)
 24. RUSSELL, Stuart - NORVIG Peter: *Artificial Intelligence – A Modern Approach*. New Jersey: Pearson Education, Inc., 2010. 1132 s. ISBN-13: 978-0-13-604259-4.
 25. SAVITRI, Wiwiet Eva – NUGROHO, Him'mawan Adi – MUNIR, Ahmad – PUSPARINI, Ririn – KURNIASIH, Esti – ARINDA, Desi: Perspectives of pre-service English teachers on AI chatbots in ESP worksheet development. In: *JOLLT Journal of Languages and Language Teaching*, 13 (1), (2025), s. 425–435. Dostupné online na <https://doi.org/10.33394/joltt.v13i1.12964>.
 26. SELWYN, Neil: On the Limits of Artificial Intelligence (AI) in Education. In: *Nordisk tidsskrift for pedagogikk og kritikk*, 10, (2024), s. 3–14. Dostupné online na <https://doi.org/10.23865/ntpk.v10.6062>.
 27. SHESTAKOVA, Elizaveta: Using Generative AI in ESP Classes to Teach Formal Style. In: *SSRN Electronic Journal*, (2023). Dostupné online na <https://doi.org/10.2139/ssrn.4469507>.

28. SILITONGA, Lusia – WIYAKA, Wiyaka – PRASTIKAWATI, Entika Fani: Boosting students' ESP vocabulary by utilizing AI chatbot. In: *ETERNAL (English Teaching Journal)*, 15 (2), (2024), s. 275–283. Dostupné online na <https://doi.org/10.26877/eternal.v15i2.605>.
29. SPANO, Martin: Umelá inteligencia v orechovej škrupinke: Stručný úvod do umelej inteligencie, strojového učenia, neurónových sietí, hlbokého učenia a robotov. 1. vyd. Bratislava: Žive.sk, 2019. 44 s. ISBN 978-80-570-0680-0.
30. XATAMOVA, Nodiraxon – ASHUROV, Jahongir: The Future of Legal English Learning: Integrating AI into ESP Education. In: *SPAST Reports*, 1 (7), (2024), s. 1–6. Dostupné online na <https://www.spast.org/ojspath>.
31. XU, Wendi – WANG, Xianpeng – GUO, Qingxin – SONG, Xiangman – ZHAO, Ren – ZHAO, Guodong – HE, Dakuo – XU, Te – ZHANG, Ming – YANG, Yang: Decomposition is all you need: single-objective to multi-objective optimization towards artificial general intelligence. *Mathematics*, 11(20), (2023), 4390. Dostupné online na <https://doi.org/10.3390/math11204390>.
32. **ZEIDE, Elana**: Artificial Intelligence in Higher Education: Applications, Promise and Perils, and Ethical Questions. In: *EDUCAUSE Review*, 54 (3), (2019), s. 34–38. Dostupné online na <https://ssrn.com/abstract=4320049>.
33. ZHANG, Zhijuan: The role of artificial intelligence tools on Chinese EFL learners' self-regulation, resilience and autonomy. In: *European Journal of Education*, 60 (2), (2025), e70127. Dostupné online na <https://doi.org/10.1111/ejed.70127>.

Kontaktné údaje

PaedDr. Jarmila Brtková, PhD.

jarmila.brtkova@flaw.uniba.sk

Univerzita Komenského v Bratislave

Právnická fakulta

Ústav cudzojazyčnej právnej komunikácie

K PROBLEMATIKE KOLOKAČNÉHO POTENCIÁLU VYBRANÝCH INŠTITÚTOV DEDIČSKÉHO PRÁVA V SLOVENSKÝCH A ANGLICKÝCH JUDIKÁTOCH Z OBLASTI DEDIČSKÉHO PRÁVA ¹

ON THE ISSUES OF COLLOCABILITY OF THE SELECTED TERMINOLOGICAL UNITS OF SUCCESSION LAW IN SLOVAK AND ENGLISH JUDICIAL DECISIONS IN THE FIELD OF SUCCESSION LAW

Andrea Demovičová²

Abstrakt: Cieľom predloženého príspevku je predostrieť komparatívnu a kontrastívnu (obojsmernú) analýzu kolokácií v dvoch jazykoch (slovenský jazyk a anglický jazyk) na príklade sporov o dedičské právo v kontexte aktuálnej domácej (slovenskej) aplikačnej praxe, ako aj v angloamerickom právnom systéme. Pri analýze odbornej právnej terminológie v oblasti dedičského práva sa zameriame na výskyt kolokácii vo vzťahu k vybraným ťažiskovým terminologickým jednotkám. Na lexikálnej rovine budeme venovať pozornosť kolokačnému správaniu týchto ťažiskových terminologických jednotiek a ich schopnosti sa spájať s konkrétnymi substantívami, adjektívami a slovesami. Ďalším cieľom príspevku je sledovať aké slovnodruhovú kombinácie vytvárajú. Na základe korpusového výskumu anglických a slovenských judikátov v dedičskoprávných veciach bude príspevok analyzovať ekvivalenčné vzťahy vyexcerpovaných kolokačných spojení, to jest či pre danú kolokáciu v slovenskom jazyku existuje priamy ekvivalent v anglickom jazyku alebo dochádza skôr k nejednoznačnému prelínaniu viacerých ekvivalentov. Predmetom skúmania bude aj uplatňovanie štylistických princípov opakovania a variácie pri tvorbe právnych textov. Následne sa bude venovať pozornosť makroštruktúre právneho textu.

Kľúčové slová: dedičské právo, právny text, kolokácie, kolokačné spojenie, spätelnosť, korpusová lingvistika

¹ Publikačný výstup je úlohou plnenou v rámci projektu s názvom *Kontrastívny výskum kolokácií v slovenských a nemeckých dedičskoprávných textoch*, ktorý bol schválený Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-23-0192 s dobou riešenia v rokoch 2024 až 2028.

² Ekonomická univerzita v Bratislave, Fakulta aplikovaných jazykov, Katedra anglického jazyka

Abstract: The aim of this paper is to present a comparative and contrastive (two-way) analysis of collocations in two languages (Slovak and English) using the example of succession law disputes in the context of current domestic (Slovak) legal practice, as well as in the Anglo-American legal systems. In analysing specialized legal terminology in the field of succession law, we will focus on the occurrence of collocations in relation to selected key terminological units. At the lexical level, we will focus on the collocation behaviour of these key terminological units and their ability to combine with specific nouns, adjectives, and verbs. Another objective of the paper is to observe what word type combinations they form. Based on the corpus research of English and Slovak case law in succession matters, the paper will analyse the equivalence relationships of the collocation combinations extracted, i.e., whether there is a direct equivalent in English for a given collocation in Slovak, or whether there is rather an ambiguous overlap of several equivalents. The study will also examine the application of stylistic principles of repetition and variation in the creation of legal texts. Subsequently, attention will be paid to the macrostructure of legal texts.

Keywords: succession law, legal text, collocations, collocation structure, word co-occurrence, corpus linguistics

Úvod

V úvode príspevku sa pokúsme o vymedzenie základných kategórií jazykového prejavu. Hneď na začiatku je však potrebné uviesť, že neexistuje jedna jediná klasifikácia, podľa ktorej by sa jednoznačne dalo určiť jediné a absolútne miesto konkrétneho textu v systéme druhov, typov a tried textov a textových žánrov. Vytvoriť jednotný systém a nájsť jednotnú ekvivalenciu medzi slovenskými a cudzojazyčnými odbornými názvami, ktoré sa používajú pri textovej typológii, nie je jednoduché a ani konečné.³

Vzťah medzi textom a štýlom sa v jazykovede chápe nasledovne: text je konkrétny jazykový celok, súvislý prejav, ktorý má obsah (čo sa píše) a formu (ako je to vyjadrené); štýl je spôsob, akým je text utvorený. Zahŕňa výber jazykových prostriedkov, ich usporiadanie a celkový charakter prejavu. Text neexistuje bez štýlu, ako neexistuje štýl bez textu. Štýl je vždy viazaný na konkrétny prejav. Textu a jeho štýlu sa v jednotlivých etapách vývoja štylistiky venovala pozornosť (ako to bolo uvedené vyššie) ako produktu, ako procesu a v najnovších prístupoch ako rečovému aktu, ktorý sa realizuje v komunikačnej situácii, využívajúc rozličné komunikačné

³ VAJIČKOVÁ, Mária: K typológii textov dedičského práva. In: *Philologia*, Roč. 35, č. 1 (2025). Bratislava: Univerzita Komenského v Bratislave, s. 8

kanály (písomná komunikácia a ústna komunikácia). Na komunikácii participujú komunikační partneri (komunikanti: autor textu a adresát textu) a výsledkom ich komunikácie je text, označovaný aj ako komunikát.⁴ Štýl ma teda na jednej strane funkciu odlišovaciu, na druhej strane funkciu zaraďovaciu: určuje do akej komunikačnej oblasti možno komunikát zaradiť.

Konkrétne príklady textov (rozsudok, zápisnica, zákon, predvolanie, osvedčenie o dedičskom konaní) by sme mohli označiť ako druh textu alebo žáner (útvár) a jednotlivé kategórie tak, ako ich uvádza Abrahámová ako žánrové skupiny (skupiny útvarov), keďže sa zhodujú z funkčného hľadiska a podobnosti môžeme skonštatovať aj z lingvistického a štylistického hľadiska.

Ako uvádza M. Vajičková, aj v odbornej slovakistickej literatúre sa pracuje s pojmom žáner, odvolávajúc sa na Slančovú (Slančová et al. 2022a), ktorá považuje žáner za „zovšeobecnený abstraktný koncept, ktorý sa vytvoril induktívnou generalizáciou, abstrakciou, zovšeobecnením textov, vyznačujúcich sa podobnými tematickými, funkčnými, kompozičnými, jazykovými a formálnymi znakmi. Žáner je abstrakciou, konceptom, zovšeobecneným pojmom. Je to invariant, ktorý v sebe obsahuje súhrn všetkých znakov daného typu textov; tvorí isté pozadie, na ktoré projektujeme všetky konkrétne texty. Má funkciu systematizačnú, priraduje konkrétny tvorený, resp. percipovaný text k iným podobným textom.“⁵

V súvislosti s používaním jazykových prostriedkov v právnej komunikácii, i s ohľadom na predmet štylistiky si Abrahámová kladie nasledovnú otázku: existuje vôbec právnický štýl, t.j. vyberajú právnici jazykové a mimojazykové prostriedky pre svoj prejav cieľavedome a usporadúvajú ich do vyšších jazykových celkov osobitným spôsobom a s určitým zámerom? Odpoveď na túto otázku je kladná.⁶

Pri ďalšej analýze odborného textu budeme vychádzať z premisy, že právny text predstavuje základný a ťažiskový prvok právnej komunikácie. Ak tvrdíme, že štýl konkrétneho právneho textu, napríklad rozsudku, je zvláštny, uvedomujeme si jeho špecifiká na pozadí ostatných textov, ktorými sa od nich líši. Pri členení právnych textov uvádza Abrahámová nasledujúcu klasifikáciu, ktorá platí v práve:

1. Legislatívne texty (zákony, nariadenia, vyhlášky, vykonávacie predpisy),
2. Notárske písomnosti (zmluvy, testamenty, osvedčenia o dedičskom konaní, overovacie listiny, nostrifikačné záznamy, splnomocnenia),
3. Forenzné komunikáty (žaloby, obžaloby, obhajoby, rozsudok, uznesenie, opatrenie, svedecká výpoveď, znalecký posudok, odvolanie, dovolanie),

⁴ VAJIČKOVÁ, Mária: K typológii textov dedičského práva. In: *Philologia*, Roč. 35, č. 1 (2025). Bratislava: Univerzita Komenského v Bratislave, s. 12

⁵ VAJIČKOVÁ, Mária: K typológii textov dedičského práva. In: *Philologia*, Roč. 35, č. 1 (2025). Bratislava: Univerzita Komenského v Bratislave, s. 10

⁶ ABRAHÁMOVÁ, Eva: *Základy právnej komunikácie*. Šamorín: Heuréka. 2012.s. 34

4. Administratívno-právne písomnosti (zápisnica, predvolanie, upomienka, žiadosť, povolenie, výpis z registra trestných činov, z obchodného registra, z katastra nehnuteľností) a

5. Odborné a vedecké texty (monografie, štúdie, články, rigorózne a dizertačné práce, učebnice a učebné texty, komentáre k zákonom).⁷

Právny text je svojim charakterom odborný text. Charakteristika odborných textov a určenie druhov textov úzko súvisí s ich makroštruktúrou. Práve makroštruktúrou sa odborné texty odlišujú od iných textov, ale aj navzájom medzi sebou.⁸ Snaha odborného jazyka dosiahnuť čo najvyšší stupeň jasnosti a zrozumiteľnosti sa odráža v tendencii zosúladiť makroštruktúrnú formu a funkciu textu. Táto tendencia vedie k bohatému členeniu a stavbe textu, charakteristickej pre určitý druh textov. Rôzne formy členenia, ako napr. kapitoly, odseky, nadpisy a pod., sledujú tému odborného textu a dodržiavajú záväznú stavbu odborného textu.⁹

Cieľom predloženého príspevku je skúmať kolokačné správanie vybraných terminologických jednotiek z oblasti dedičského práva, ako aj výskyt štylistických princípov variácie a opakovania, ktoré sa uplatňujú v právnom texte. Podstatou výskumu je predostrieť komparatívnu a kontrastívnu analýzu kolokačných spojení, ktoré sa vyskytujú v súdnych rozhodnutiach z oblasti dedičského práva v slovenskej a v anglickej jazykovej mutácii. Za hlavnú metódu sme si zvolili metódu komparácie súdnych rozhodnutí pochádzajúcich z dvoch odlišných právnych systémov. Ďalšou použitou metódou je kontrastívna analýza vyexcerpovaných kolokačných spojení prostredníctvom ktorej identifikujeme, či pre danú kolokáciu v slovenskom jazyku existuje rovnocenný ekvivalent v anglickom jazyku. Za účelom zatriedenia skúmaných kolokačných spojení sme v metodológii výskumu zadefinovali najčastejšie typy kolokačných spojení, do ktorých vybrané terminologické jednotky vstupujú, a následne uvádzame ich príklady v tabuľkách.

Lexikálna rovina právneho jazyka

Právny jazyk má osobitné postavenie v rámci odborných jazykov na základe skutočnosti, že právny jazyk nie je medzinárodným, univerzálnym odborným jazykom ako ostatné odborné jazyky, keďže je viazaný na právny systém konkrétneho štátu.

⁷ ABRAHÁMOVÁ, Eva: Základy právnej komunikácie. Šamorín: Heuréka. 2012.s. 38

⁸ Pomerne ustálenú makroštruktúru právnych textov je možné identifikovať aj v súkromnoprávných dokumentoch. Bola špecifická aj pre staršie závetý z polovice 19. storočia, ktorých formulár bol na makroúrovni relatívne stabilný a jeho jednotlivé časti boli lineárne radené. GERGEL, Peter: Formulár trnavských meštianskych závetov prvej polovice 19. storočia zo štylistického hľadiska. In: Slovenská reč, Roč. 82, č. 2 (2017), s. 137

⁹ ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Belianum. Vydavateľstvo UMB v Banskej Bystrici. 2016, s. 34

Právny jazyk chápeme ako jeden z mnohých odborných jazykov, ktorý je reprezentovaný preferovanými jazykovými prostriedkami v jednotlivých jazykových rovinách. Osobitosťou právneho jazyka je jeho vzťah k bežnému jazyku. Na rozdiel od ostatných odborných jazykov ide o jednostranný vzťah. To znamená, že právny jazyk vo veľkej miere používa bežný jazyk, avšak jazykové prostriedky právneho jazyka na rozdiel od ostatných odborných jazykov len málo prenikajú do bežného jazyka. Rozdiel medzi právnym jazykom a inými odbornými jazykmi je aj v používaní cudzích slov. Právny jazyk takmer nepoužíva cudzie slová a pokiaľ je to možné, vyhýba sa im. Používanie cudzích slov, konkrétne slov latinského pôvodu, je viazané na určité druhy právnych textov, napr. učebnice, vedecké state, právne stanoviská či rozhodnutia.¹⁰

Z funkčného hľadiska je právny jazyk prostriedkom komunikácie v rámci právnej komunikačnej sféry. Z obsahového hľadiska je právny jazyk znakový systém, v ktorom za jednotlivé znaky považujeme právne termíny, slovné spojenia alebo celé vety. Realizuje sa formou písomného prejavu, v ktorom sa prenáša právna informácia.¹¹

Slovník právneho jazyka (právna lexika) pozostáva: a) z výrazov výlučne právnych, t.j. termínov, b) zo slovných spojení, ktoré sa využívajú k popisu právnych skutočností a c) z výrazov, ktoré sú súčasťou všeobecného základu spisovného jazyka. V slovenskej právnej terminológii prevažujú dvoj až viacslovné termíny nad jednoslovnými, ktoré sú často najstaršími základnými právnymi výrazmi (napríklad termín právo).¹²

História slovenskej právnej terminológie siaha hlboko do minulosti a mali na ňu vplyv kontaktné jazyky (maďarčina, nemčina a latinčina). Odborná lexika sa etablovala postupne a napr. pre odbornú právnu terminológiu v závetoch bola v prvej polovici 19. storočia typická pomerne bohatá synonymia.¹³

Pri otázke výskytu slovných spojení v právnej lexike, niektorí ich chápu ako terminologické jednotky, iní ich zaraďujú k neterminologickým súčastiam právneho jazyka. Veľmi časté sú verbálno-substantívne spojenia, kedy ide o pevnú väzbu slovesa k určitému podstatnému menu. Z čisto lingvistického hľadiska vznikli ako výsledok implikácie, kedy sám termín implikuje použitie určitého slovesa zo všeobecnej slovnej zásoby, slovesá pomáhajú termín včleniť do syntaktickej

¹⁰ ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Belianum. Vydavateľstvo UMB v Banskej Bystrici. 2016, s. 16

¹¹ ABRAHÁMOVÁ, Eva – ŠKVARENINOVÁ, Oľga: Kapitoly so štylistiky a rétoriky pre právnikov. Bratislava: vydavateľské oddelenie PF UK v Bratislave. 2006. s. 75

¹² ABRAHÁMOVÁ, Eva – ŠKVARENINOVÁ, Oľga: Kapitoly so štylistiky a rétoriky pre právnikov. Bratislava: vydavateľské oddelenie PF UK v Bratislave. 2006. s. 77

¹³ GERGEL, Peter: Slovenská právna terminológia v trnavských meštianskych závetoch prvej polovice 19. storočia. In: Slovenská reč, Roč. 82, č. 3 (2017), s. 254

konštrukcie.¹⁴ Napríklad termín v dedičskom práve „majetok“ implikuje použitie sloviess zanechať, odkázať, nadobudnúť (nie však získať). Typickými pojmovými slovami sú substantíva. Substantívne (menné) vyjadrenie poskytuje veľké možnosti využitia v právnej lexike: substantívum možno doľava i doprava rozvíjať atribútom. Bližšie sa určujú zhodným atribútom (závetný dedič, dedičský podiel) alebo nezhodným atribútom (dedič zo zákona, uznesenie o dedičstve).¹⁵

Variácia a opakovanie

Popri vlastnostiach právneho jazyka, ktoré charakterizujú textovú rovinu a podieľajú sa na tvorbe právnych textov, je potrebné poukázať aj na štylistické princípy tvorby právnych textov, t.j. na variáciu a opakovanie. Napriek tomu, že princíp variácie má pri tvorbe odborných textov obmedzené uplatnenie a realizuje sa predovšetkým v morfológicko-syntaktickej rovine, uplatňuje sa pri tvorbe právnych textov aj mimo nej. Vzhľadom na skutočnosť, že používanie synonym v odborných a právnych textoch nie je nijakou zvláštnosťou, môžeme aj v právnych textoch pozorovať uplatňovanie štýlotvorného princípu variácie.¹⁶ V morfológicko-syntaktickej rovine súvisí princíp variácie s používaním generického maskulína na pomenovanie osôb mužského aj ženského pohlavia. V súčasnosti možno v textoch justičných orgánov z oblasti dedičského práva pozorovať tendenciu používať v mužskom rode ťažiskové termíny aj pre označenie žien (príklady zo spisu: zákonný dedič, určiť dediča).

Opakovanie ako štylistický princíp tvorby textov je pre právne texty charakteristické a vyplýva z požiadavky presnosti a jednoznačnosti právneho jazyka. Princíp opakovania predstavuje dokonca jeden zo základných princípov tvorby právnych textov justičných orgánov. Texty justičných orgánov majú definovaný obsah a stanovenú, resp. zaužívanú štruktúru. Obsahujú označenie strán konania, ich zákonných zástupcov, splnomocnené osoby, označenie justičných orgánov, ich zástupcov, skutkovú podstatu, výrok, zákonné ustanovenia, dôvody rozhodnutia, atď. Mnohé z uvedených označení sa v tom istom texte opakujú viackrát. Za opakovanie možno pokladať uvádzanie konkrétnych paragrafov príslušných zákonov a poriadkov, prípadne použitie časti príslušných ustanovení v uzneseniach, v odôvodnení rozhodnutí a pod.¹⁷

¹⁴ ABRAHÁMOVÁ, Eva – ŠKVARENINOVÁ, Oľga: Kapitoly so štylistiky a rétoriky pre právnikov. Bratislava: vydavateľské oddelenie PF UK v Bratislave. 2006. s. 79

¹⁵ ABRAHÁMOVÁ, Eva – ŠKVARENINOVÁ, Oľga: Kapitoly so štylistiky a rétoriky pre právnikov. Bratislava: vydavateľské oddelenie PF UK v Bratislave. 2006. s. 78

¹⁶ ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Belianum. Vydavateľstvo UMB v Banskej Bystrici. 2016, s. 41

¹⁷ ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Belianum. Vydavateľstvo UMB v Banskej Bystrici. 2016, s. 41-42

V predkladanom príspevku ide o korpusovú analýzu kolokácií v právnych textoch, výskumný korpus však tvoria výhradne súdne rozhodnutia z oblasti dedičského práva vynesené Najvyšším súdom SR. Z hľadiska makroštruktúry má text sledovaných súdnych rozhodnutí nasledovnú pevnú formu členenia: úvodná časť, odôvodnenie a poučenie, pričom táto výstavba textu je nemenná. Vychádzajúc z obsahu rozhodnutí princíp opakovania je markantný najmä v časti poučenie, kedy sa v každom judikáte uvádza veta rovnakého znenia: „Proti tomuto uzneseniu nie je prípustný opravný prostriedok.“

Teoretické východiská pojmu kolokácia

Právny jazyk a lexika právneho jazyka sa svojimi zvláštnosťami odlišuje od ostatných odborných jazykov. Hoci je terminológia podstatnou súčasťou právnych textov, v poslednom období stúpa aj záujem o štúdium ostatných typických črt právnych textov, ako sú napr. ustálené slovné spojenia a kolokácie, ktoré súvisia do veľkej miery s konvenciami v právnom jazyku.

Slovenskí lingvisti sa venujú otázke spätelnosti a ustálenosti istých spojení slov v slovenskom jazyku skôr pod pojmom ustálené slovné spojenie. Až v poslednom desaťročí sa objavujú pojmy kolokácia a kolokabilita. Diskrepancie v interpretácii pojmu kolokácia majú svoje korene vo vágnosti tohto pojmu, kdeže v odbornej literatúre absentuje jeho jednotná, všeobecne akceptovateľná definícia. Z kvalitatívneho hľadiska sa kolokácie vymedzujú vágnymi pojmami ako typické, uzuálne, preferované slovné kombinácie, čo tiež neposkytuje pevný lingvistický fundament na ich delimitáciu.¹⁸ M. Stubbs definuje kolokáciu ako častý spoluvýskyt lexikálnych jednotiek, pričom kolokácie sú isté typy syntagmatických vzťahov medzi týmito lexikálnymi jednotkami.¹⁹ M. Vajičková uvádza, že pojem kolokácia sa používa pre viac alebo menej ustálené spojenie, ktoré sa skladá z bázy/ kolokanta, ktorý je nositeľom hlavného významu, je sémanticky autonómny a v podstate sa používa v pôvodnom význame. Kolokátor je sémanticky závislý od bázy/kolokantu, v spojení nadobúda špecifický význam (niekedy prenesený a vtedy sa spojenie blíži k frazémam, pričom hranica je vágna). K báze *majetok* máme kolokátory *odkázať, zanechať, nadobudnúť* a pod.²⁰

V poslednom čase sa s pojmom kolokácia pracuje intenzívnejšie aj na Slovensku v súvislosti s korpusovo orientovaným výskumom slovnej zásoby slovenčiny. D.

¹⁸ ĎURČO, Peter: Princípy zostavovania glosára kolokácií pre kolokačnú didaktiku. In: *Philologia*, Roč. 30, č. 2 (2020). Bratislava: Univerzita Komenského v Bratislave, s. 24

¹⁹ STUBBS, Michael: *Words and phrases: Corpus studies of lexical semantics*. Oxford: Blackwell Publishing. 2001, s. 29

²⁰ VAJIČKOVÁ, Mária: Ako ovplyvňuje typologická príslušnosť tvorbu kolokácií v cudzom jazyku. In: *Philologia*, Roč. 29, č. 1-2 (2019). Bratislava: Univerzita Komenského v Bratislave, s. 20-21

Majchráková (2005) používa pomenovanie kolokácia v diplomovej práci pri analýze dvojíc a trojíc slov nachádzajúcich sa tesne vedľa seba (tzv. bigramy a trigramy), ktoré boli vo vyváženom podkorpuse o veľkosti 12 miliónov textových jednotiek (tokenov) extrahované vďaka príslušnému softvéru a zoradené podľa frekvencie. Pomenovanie kolokácia používa aj P. Ďurčo (2007) v súvislosti s koncipovaním Nemecko-slovenského slovníka kolokácií. Autor pracuje na báze korpusového materiálu a na identifikáciu relevantných slovných spojení používa frekvenčné aj štatistické kritériá.²¹ Aj z uvedeného vyplýva, že korpusová lingvistika pracuje so širším poňatím pojmu kolokácie v porovnaní s lexikológiou, prípadne frazeológiou. Lexikológia a frazeológia vymedzuje ustálené slovné spojenia ako tie, ktoré majú binárnu (dvojčlennú štruktúru). Korpusová lingvistika zahŕňa širšie kontinuum analyzovaného slova a za kolokáciu považuje aj spojenia, ktoré majú trinárnu (trojčlennú) až viacčlennú štruktúru.²²

Spojenie kolokácia by však mohlo byť definované aj z hľadiska širokého spektra lexikalizovaných spojení, pričom môže označovať terminologické i neterminologické slovné spojenia. Kolokácie je možné pojmovo vymedziť napr. voči frazeologizovaným spojeniam. Tieto však majú s kolokáciami spoločnú istú stabilitu a je v nich (frazeologizovaných spojeniach) „jeden alebo viac prvkov pevne daných a ostatné prvky sú variabilné.“ Stabilitu je možné dať do paralelného vzťahu k štylistickému princípu opakovania, na druhej strane variabilita znamená obmenu lexikálnych jednotiek, na základe ktorej sa dajú rekonštruovať paradigmatické vzťahy.²³

Delimitácia kolokácií naráža na dva problémy. Z kvantitatívneho hľadiska je kolokačný potenciál slova otvorený, je ťažké presne stanoviť limity kolokability a lexikálnej distribúcie jednotlivých slov. Frekvencia nie vždy poukazuje na typickosť slovného spojenia, pričom frekvencia kolokátov má graduálnu povahu a možno si ju predstaviť ako istú radiálnu štruktúru s kvantitatívnym centrom a perifériou v rámci pevných, typických, uzuálnych spojení, ale aj voľných slovných spojení. Medzi frekvenciou výskytu a lexikalizovanosťou nefunguje priama úmera.²⁴

²¹ JAROŠOVÁ, Alexandra: Problém vymedzenia kolokácií. In: Jazykovedný časopis, Roč.58, číslo 2 (2007). Bratislava: Slovak Academic Press, s. 82

²² GERGEL, Peter: Kolokácie v preklade právnych textov. In: Philologia, Roč. 30, č. 2 (2020). Bratislava: Univerzita Komenského v Bratislave, s.91

²³ ĎURČO, Peter: Frazeologizované konštrukcie na príklade nemeckého a slovenského jazyka. In: Slovenská reč, Roč. 90, č. 1 (2025), s. 32.

²⁴ ĎURČO, Peter: Princípy zostavovania glosára kolokácií pre kolokačnú didaktiku. In: Philologia, Roč. 30, č. 2 (2020). Bratislava: Univerzita Komenského v Bratislave, s.24.

Výsledky analýzy a interpretácia výskumu kolokačného správania vybraných ťažiskových jednotiek

Cieľom predloženého príspevku je predostrieť komparatívnu a kontrastívnu (obojsmernú) analýzu kolokácií v dvoch jazykoch (slovenský jazyk a anglický jazyk) v právnych textoch. Výskumný korpus však tvorí výhradne jeden konkrétny typ právneho textu, a to súdne rozhodnutia z oblasti dedičského práva. Kolokačné správanie vybraných terminologických jednotiek porovnávame na judikátoch pochádzajúcich z dvoch odlišných právnych systémov. Porovnávame ich v kontexte aktuálnej domácej (slovenskej) aplikačnej praxe, ako aj v kontexte právnej úpravy Spojeného kráľovstva Veľkej Británie a Severného Írska, ktorá je súčasťou anglo-amerického právneho systému.

Za účelom komparatívnej a kontrastívnej analýzy sme si zvolili 5 ťažiskových terminologických jednotiek z oblasti dedičského práva, a to: *závet*, *dedič*, *dedičstvo*, *dedičský*, *majetok*. Predmetom analýzy bolo vymedziť ich kolokačný potenciál. Z lexikálneho pohľadu sme skúmali aké ustálené konštrukčné typy a variantné modely tieto terminologické jednotky vytvárajú v analyzovanom type právneho textu. Za účelom zatriedenia skúmaných kolokácií v metodológii výskumu sme zadefinovali tri typy kolokačných spojení: verbálno-substantívne, adjetívno-substantívne a čisto substantívne spojenia, do ktorých vybrané terminologické jednotky vstupujú. V príspevku analyzujeme či pre danú kolokáciu v slovenskom jazyku existuje aj priamy ekvivalent v anglickom jazyku, s ktorým by bol významovo totožný.

Za účelom výskumu sme realizovali zber dát. Vyexcerpovali sme 10 rozhodnutí Najvyššieho súdu Slovenskej republiky, zamerali sme sa výlučne na rozhodnutia v konaniach o dedičstve. Analyzované rozhodnutia sa stali základom k vytvoreniu prvého zdrojového korpusu v slovenskom jazyku. Excerpcia judikátov sa realizovala pomocou kľúčového slova „DEDIČ“. Následne bol ešte urobený výber na základe merita veci, z obsahového hľadiska išlo o neplatnosť závetu, určenie platnosti závetu a prejednanie dedičstva. Časové rozpätie súdnych rozhodnutí zahŕňalo roky 2018 – 2024. V takto vymedzenom korpuse judikátov sme vyselektovali tematicky relevantné slovné spojenia, t.j. identifikovali sme celkom 70 odlišných kolokačných spojení, s ktorými sa viaže päť zvolených terminologických jednotiek.

Druhý zdrojový korpus v anglickom jazyku vytvorilo 30 súdnych rozhodnutí, ktoré vyniesol súd patriaci do sústavy vyšších súdov v Spojenom kráľovstve Veľkej Británie a Severného Írska. Názov tohto súdu je *His Majesty's High Court of Justice in England* (divízia *Chancery Division*). Excerpcia judikátov sa realizovala pomocou kľúčového slova „HEIR“ a „TESTATOR“. Všetky rozhodnutia, ktoré sme podrobili analýze kolokačného potenciálu vo vzťahu k vybraným terminologickým jednotkám, sú verejne dostupné na webovej stránke <https://www.bailii.org/databases.html>.

Nachádzajú sa tu databázy, ktoré obsahujú britské a írské sudcovské právo, súdne rozhodnutia vydané súdmi na všetkých stupňoch súdnej sústavy v Spojenom kráľovstve Veľkej Británie a Severného Írska. Časové rozpätie rozhodnutí zahŕňalo roky 2000 – 2024. V takto vymedzenom korpuse judikátov sme identifikovali celkom 66 odlišných kolokačných spojení, s ktorými sa viaže 5 zvolených terminologických jednotiek. Nižšie číslo kolokačných spojení, ktoré sme vyexcerpovali z anglického zdrojového korpusu vo vzťahu k slovenskému korpusu (výskyt 70), je možné zdôvodniť tým, že buď v anglo-americkej právnej úprave označovaný inštitút absentuje alebo pre neho neexistuje terminologicky rovnocenný (alebo aspoň príbuzný) ekvivalent v anglickom jazyku.

V nasledujúcej tabuľke ponúkame exemplifikáciu kolokačného potenciálu termínu „ZÁVET“. Uvádzame prehľad vyexcerpovaných kolokácií, ktoré sa viažu s termínom „ZÁVET“ v troch kolokačných typoch a ich ekvivalentné náprotivky v anglickom jazyku.

Verbálno-substantívny kolokačný typ		Adjektívno-substantívny kolokačný typ	
slovenský jazyk	anglický jazyk = priamy ekvivalent	slovenský jazyk	anglický jazyk = priamy ekvivalent
napísať závet spísať závet vyhotoviť závet zriadiť závet podpísať závet zmeniť závet predložiť závet zanechať závet zrušiť závet napadnúť závet	make a will make a will draw up a will make a will sign a will change a will handing over of the will leave a will revoke a will contest a will	holografný závet vlastnoručný závet alografný závet sporný závet platný závet neplatný závet skorší závet neskorší závet	holographic will handwritten will ----- contested will valid will invalid will former will/old will later will/new will
Substantívno-substantívny kolokačný typ			
slovenský jazyk	anglický jazyk = priamy ekvivalent		
neplatnosť závetu	invalidity of a will		
dedenie bez závetu	intestate succession		
dedenie zo závetu	testate succession		
obsah závetu	content of a will		
svedok závetu	witness to a will		

Tabuľka č. 1

Príkladová analýza kolokačných spojení s komponentom závet

Z uvedenej príkladovej analýzy vyplýva frekvenčne vyšší počet slovies (v počte 10) ako aj ich heterogenita v pomere k podstatným menám (v počte 5), s ktorými sa spája jedna terminologická jednotka, v tomto prípade substantívum „ZÁVET“. Dôvodom bohatého kolokačného potenciálu skúmaného substantíva so slovesami je snaha zákonodarcu zachytiť a explicitne vyjadriť prostredníctvom činnostných slovies čo najväčšie množstvo jednostranných právnych úkonov, ktorými fyzická osoba (poručiteľ) rozhoduje o svojom majetku pre prípad smrti. Rovnako pozorujeme vyššiu kombinovateľnosť skúmaného substantíva s adjektívami (v počte 8) v pomere k podstatným menám (v počte 5), čo preukazuje aj jeho schopnosť vstupovať do adjektívno-substantívnych kolokačných spojení. Na lexikálnej úrovni, pri tvorbe odborného právneho textu, adjektívno- substantívne kolokačné spojenia odrážajú snahy zákonodarcu vyjadriť formálne alebo materiálne náležitosti pre platnosť závetu.

Ekvivalenčné vzťahy kolokácií však nie sú jednoduché a priamočiare. Požiadavku absolútnej ekvivalencie medzi kolokačnými spojeniami vo východiskovom texte (slovenský judikát) a cieľovom texte (anglický judikát) nie je možné vždy jednoznačne naplniť vzhľadom na odlišné konštruovanie pojmovej reality v oboch skúmaných právnych poriadkoch. Pre právny jazyk sú typické jazykové konvencie, ktoré sa však vzhľadom na diskrepancie v odlišných právnych poriadkoch nie vždy dajú dodržať. Vidíme to na príklade kolokačného spojenia „alogafný závet“, ktorý v anglickom jazyku nemá svoj náprotivok, pretože označovaný inštitút v anglo-amerikej právnej úprave chýba. V ostatných uvedených príkladoch pozorujeme monoekvivalenciu, kedy monosémantickej kolokácii zodpovedá v druhom jazyku jeden priamy ekvivalent.

V predkladanej tabuľke pozorujeme variantnosť a synonymickosť v kolokačných spojeniach, ktorá sa realizuje v textovej rovine judikátov. Paralelné používanie konštrukcií *napísať závet* - *spísať závet* - *vyhotoviť závet* - *zriadiť závet* alebo *holografný závet*- *vlastnoručný závet* označujú rovnakú pojmovú realitu a možno ich pokladať za variácie. Rovnako anglické adjektívno- substantívne kolokačné spojenia *former will* - *old will* alebo *later will* - *new will* možno pokladať za variantné a významovo totožné.

V nasledujúcej tabuľke si predstavíme prehľad vyexcerpovaných kolokačných spojení, ktoré sa viažu s termínom „DEDIČSKÝ“ a ich ekvivalentné náprotivky v anglickom jazyku.

Adjektívno-substantívny kolokačný typ	Variantnosť kolokačných typov
slovenský jazyk	anglický jazyk = priamy ekvivalent

dedičské právo	right to inherit
dedičský titul	right to inherit
dedičský súd	probate court
dedičská skupina	line in succession
dedičský podiel	portion of the estate /share in a will
dedičské konanie	probate (process)
dedičská vec	inheritance
dedičské rozhodnutie/uznesenie	law of succession judgment

Tabuľka č. 2

Príkladová analýza kolokačných spojení s komponentom *dedičský*

Z uvedenej príkladovej analýzy vyplýva, že ekvivalenčné vzťahy medzi kolokačnými spojeniami v oboch sledovaných právnych úpravách môžu byť komplikovanejšie. Komparáciou výkladu právnych úprav (slovenskej a anglo-americkej) sme sa dostali ku vzťahu semiekvivalencie, kde dochádza k prelínaniu sa viacerých potenciálnych ekvivalentov. To znamená, že napr. kolokácia s komponentom *dedičský* môže mať v inom jazyku potenciálne viaceré ekvivalenty: *dedičský podiel* verzus jeho anglické náprotivky *a portion of the estate - share in a will*.

Okrem priamej, jednoznačnej substitúcie kolokácií nachádzajúcich sa v slovenských a anglických judikátoch, pozorujeme pri analýze právneho textu v oboch jazykových mutáciách aj možnosti využitia sémanticky a odborne blízkej kolokácie, ktorá by ešte spĺňala kritérium akceptability. Tento jav je možné pozorovať na príklade slovenskej kolokácie *dedičská vec*, pre ktorú sme vyexcerpovali v anglickom korpuse terminologicky príbuzný ekvivalent *inheritance*.

Zaujímavé je pozorovať slovnodruhovú kombináciu uvedených kolokácií. V zdrojom korpuse v slovenskom jazyku patria všetky kolokácie s komponentom *dedičský* k adjektívno-substantívnomu kolokačnému typu a tvoria dvojčlenné štruktúry. V anglickej mutácii zdrojového korpusu nemožno jednoznačne určiť typ kolokačného spojenia, tak ako sme ho zadefinovali v metodológii výskumu. V praxi dochádza k arbitrárnym modelom z hľadiska kombinácie slovných druhov (napríklad: *dedičský titul – right to inherit*). Z hľadiska počtu komponentov, ktoré tvoria kolokačné spojenie, môže dôjsť k vytvoreniu viacslovných celkov (napríklad *dedičské rozhodnutie - law of succession judgment*), avšak ojedinele aj k situácii, kedy v inom jazyku nebude naplnená požiadavka na vznik kolokačného spojenia, keďže terminologicky najpresnejšiemu ekvivalentu adjektívno-substantívnej kolokácie *dedičská vec* zodpovedá v anglickom judikáte iba jedno slovo *inheritance*.

Záver

Predkladaný príspevok je pokusom o lingvistickú analýzu kolokačného správania vybraných kolokácií, ktorých výber podlieha výlučne kritériám v rámci odboru, v

tomto prípade v rámci dedičského práva. Štúdia je štruktúrovaná nasledujúcim spôsobom: v úvodnej časti sa venujeme charakteristike právneho jazyka vo všeobecnosti, berieme do úvahy právne texty v širšom význame, t. j. bez konkretizácie oblasti práva a druhu textov, s cieľom priblížiť vlastnosti a zvláštnosti právneho jazyka všeobecne. V časti teoretické východiská definujeme pojem kolokácia a predstavíme miesto kolokácií v kontexte právnej lexiky. Kolokácie ako špecifický typ ustálených slovných spojení sú na rozdiel od frazeologizmov sémanticky priezračné spojenia, kombinácie ich komponentov sú však v každom jazyku arbitrárne a nepredpovedateľné, takže si ich treba osvojovať ako dvojslovné až viacslovné celky. V časti výsledky analýzy a interpretácia výskumu poukážeme na charakter ekvivalenčných vzťahov medzi slovnými spojeniami v slovenskom jazyku a anglickom jazyku a detailnejšie opíšeme dané slovné spojenia z hľadiska ich zaradenia k príslušnému kolokačnému typu. Výskum a vytváranie mikrokorpusov (kam zaraďujeme aj súdne rozhodnutia vymedzené na základe odborných a obsahových kritérií) prispieva podľa nášho názoru významnou mierou k poznaniu kolokačného správania vybraných ťažiskových inštitútov z oblasti dedičského práva v odborne špecifickom type textu.

Zoznam použitej literatúry

1. ABRAHÁMOVÁ, Eva – ŠKVARENINOVÁ, Oľga: Kapitoly so štylistiky a rétoriky pre právnikov. Bratislava: vydavateľské oddelenie PF UK v Bratislave. 2006. 124 s. ISBN 80-7160-219-1.
2. ABRAHÁMOVÁ, Eva: Základy právnej komunikácie. Šamorín: Heuréka. 2012. 127 s. ISBN 978-80-89122-81-3.
3. ĎURČO, Peter: Frazeologizované konštrukcie na príklade nemeckého a slovenského jazyka. In: Slovenská reč, Roč. 90, č. 1 (2025), s. 32 – 50. ISSN 0037-6981
4. ĎURČO, Peter: Princípy zostavovania glosára kolokácií pre kolokačnú didaktiku. In: Philologia, Roč. 30, č. 2 (2020). Bratislava: Univerzita Komenského v Bratislave, s.23-36. ISSN 1339-2026.
5. ĎURICOVÁ, Alena: Preklad právnych textov. Teória, prax, konvencie, normy. Banská Bystrica: Belianum. Vydavateľstvo UMB v Banskej Bystrici. 2016, 148 s. ISBN 978-80-1170-6.
6. GERGEL, Peter: Formulár trnavských meštianskych závetov prvej polovice 19. storočia zo štylistického hľadiska. In: Slovenská reč, Roč. 82, č. 2 (2017), s. 129 – 138.
7. GERGEL, Peter: Kolokácie v preklade právnych textov. In: Philologia, Roč. 30, č. 2 (2020). Bratislava: Univerzita Komenského v Bratislave, s.89-102. ISSN 1339-2026.

8. GERGEL, Peter: Slovenská právna terminológia v trnavských meštianskych závetoch prvej polovice 19. storočia. In: Slovenská reč, Roč. 82, č. 3 (2017), s. 249 – 255.
9. JAROŠOVÁ, Alexandra: Problém vymedzenia kolokácií. In: Jazykovedný časopis, Roč. 58, číslo 2 (2007). Bratislava: Slovak Academic Press, s. 81-102. ISSN 0021-5597.
10. STUBBS, Michael: Words and phrases: Corpus studies of lexical semantics. Oxford: Blackwell Publishing. 2001, 287 s. ISBN 978-0631208334.
11. VAJIČKOVÁ, Mária: K typológii textov dedičského práva. In: Philologia, Roč. 35, č. 1 (2025). Bratislava: Univerzita Komenského v Bratislave, s. 7-23. ISSN 1339-2026.
12. VAJIČKOVÁ, Mária: Ako ovplyvňuje typologická príslušnosť tvorbu kolokácií v cudzom jazyku. In: Philologia, Roč. 29, č. 1-2 (2019). Bratislava: Univerzita Komenského v Bratislave, s. 17-34. ISSN 1339-2026.

Kontaktné údaje

Mgr. Andrea Demovičová, PhD.

andrea.demovicova@euba.sk

Ekonomická univerzita v Bratislave, Fakulta aplikovaných jazykov, Katedra anglického jazyka

NÁSLEDNÉ DEDENIE PODĽA I. NÁVRHU UHORSKÉHO VŠEOBECNÉHO OBČIANSKEHO ZÁKONNÍKA Z R. 1900 (HISTORICKÁ PRÁVNOLINGVISTICKÁ ANALÝZA)¹

SUBSEQUENT INHERITANCE UNDER THE FIRST DRAFT OF THE HUNGARIAN GENERAL CIVIL CODE OF 1900 (HISTORICAL LEGAL-LINGUISTIC ANALYSIS)

Peter Gergel²

Abstrakt: Príspevok sa zameria na inštitút podľa spomínaného návrhu (NUOZ), ktorý sa realizuje úkonmi posledného poriadku a jeho predmetom bude aj jeho lokalizácia v systematike daného návrhu. Materiálnu bázu úvodnej právnej a následnej lingvistickej analýzy tvoria §§ 1864 – 1884 NUOZ. Z právneho hľadiska sa autor bude venovať súdobej diskusii o opodstatnenosti tohto inštitútu a argumentom, ktoré hovoria za a proti jeho zachovaniu, príp. za jeho zachovanie v obmedzenej podobe. V stručnej právnej analýze sa autor bude opierať aj o príslušnú dôvodovú správu k paragrafovému zneniu návrhu. Z lingvistického hľadiska bude predmetom analýzy len (nemecký) text NUOZ. V tejto časti štúdie bude dôležité definovanie pojmu štýléma a klasifikácia štýlém na základe príslušnej odbornej (germanistickej literatúry) v oblasti štylistiky. Následne sa bude na základe vyššie uvedeného korpusu analyzovať a štatisticky vyhodnocovať vetná skladba korpusu so zameraním na identifikáciu syntaktických štýlém typických a príznakových pre tento typ odborného textu, a to najmä z funkčného hľadiska.

Kľúčové slová: následné dedenie, legislatívny text, štýléma, štylistický príznak, syntaktická štýléma

Abstract: The paper will focus on the institute according to the aforementioned draft (NUOZ), which is implemented by acts of last resort, and its subject will also be its location in the systematics of the given draft. The material basis for the introductory legal and subsequent linguistic analysis is formed by Sections

¹ Štúdia vznikla v rámci projektu APVV-23-0192 Kontrastívny výskum kolokácií v slovenských a nemeckých dediškoprávnych textoch (Contrastive Research on Collocations in Slovak and German Inheritance Law Texts), ktorý je finančne podporovaný Agentúrou na podporu výskumu a vývoja.

² Katedra nemeckého jazyka, literatúry a didaktiky, Pedagogická fakulta Univerzity Komenského v Bratislave.

1864–1884 of the NUOZ. From a legal viewpoint, the author will address the current debate on the legitimacy of this institution and the arguments for and against its preservation, or its preservation in a limited form. In the brief legal analysis, the author will also refer to the relevant explanatory memorandum to the draft wording of the sections. From a linguistic point of view, only the text of NUOZ (in German) will be analysed. In this part of the study, it will be important to define the concept of style and classify styles based on relevant specialist (German studies) literature in the field of stylistics. Subsequently, based on the above-mentioned corpus, the sentence structure of the corpus will be analysed and statistically evaluated with a focus on identifying syntactic stylistic features typical and characteristic of this type of professional text, especially from a functional point of view.

Key words: subsequent inheritance, legislative text, stylistic feature, stylistic marker, syntactic stylistic feature

Úvod

Vznik NUOZ³ treba chápať v kontexte kodifikačných snáh uhorskej civilistiky druhej polovice 19. storočia, ktorých výsledkom bolo niekoľko návrhov, z ktorých sa však vplyvom rôznych faktorov ani jeden nestal platným zákonom. Túto tému, resp. časť tohto legislatívneho dokumentu som si vybral za účelom lingvistickej analýzy z toho dôvodu, že ide o málo prebádanú tému, ktorej hlbší výskum môže iste slúžiť v mnohých ohľadoch ako inšpirácia pre ďalšie legislatívne úpravy. Ide z hľadiska právnej histórie o zaujímavý materiál, ktorý svojím rozsahom poskytuje priestor aj na lingvistické analýzy. Na základe štruktúry, premysleného spracovania a systematiky NUOZ je možné konštatovať, že j tento legislatívny návrh jednoznačne patrí medzi moderné kodifikačné úpravy konca 19. príp. začiatku 20. storočia.

Dedičské právo zakomponoval NOUZ v rozsahu a systematike jeho V. časti (§ 1794 až 2043). „Upravenú materiú rozčlenil na dve hlavné časti: 1) Prvá nosná časť (I. – V. článok) normovala základné právne skutočnosti týkajúce sa dedenia a *de iure* zodpovedala na primárnu otázku dedičskej postupnosti: Kto dedí? 2) Druhá doplnujúca časť (VI. článok) vyložila právne následky dedenia a odpovedala na otázku: Aké práva a povinnosti má osoba, ktorá dedí? VI. článok v štyroch pododdieloch upravil prijatie a odmietnutie dedičstva vo vzťahu ku všetkým trom dedičským titulom (I. oddiel); postavenie dediča vo vzťahu k veriteľom pozostalosti

³ NUOZ – Entwurf eines ungarischen allgemeinen bürgerlichen Gesetzbuches. Budapest: Grill'sche K. und K. Hofbuchhandlung, 1901.

(II. oddiel); postavenie dediča vo vzťahu k spoludedičom (III. oddiel) a postavenie dediča vo vzťahu k nepravému dedičovi (IV. Oddiel).“⁴

Čo sa týka titulov dedenia, nájdeme v NUOZ zákon, závet a dedičskú zmluvu. Podobnú úpravu nachádzame aj v mnohých iných súdobých návrhoch a legislatívnych úpravách. Povinný podiel nechápal autor NUOZ ako súčasť zákonného dedenia, ale bol začlenený ako samostatný V. článok označený za *sui generis* dedičský druh, nie delačný titul.⁵

V krátkosti je ďalej o NUOZ možné konštatovať, že jeho systematika sa v mnohom podobá na BGB⁶, príp. iné zahraničné úpravy.⁷ Aj na základe týchto faktov je daný text vhodný na porovnávanie s ostatnými legislatívnymi textami alebo návrhmi, ktoré daný inštitút takisto upravovali. V. časť NUOZ, ktorej predmetom je práve dedičské právo, pozostáva z týchto článkov: Všeobecné ustanovenia, zákonné dedenie, závetné dedenie, zmluvné dedenie, povinný podiel a právne účinky dedenia. Závetné dedenie upravené v štvrtom článku sa ďalej člení na oddiely (zriadenie závetu, obsah závetu vo všeobecnosti, určenie dediča, určenie následného dediča, odkaz, neplatnosť závetu, výkon závetu a spoločný závet). Keďže je predmetom príspevku následné dedenie, budem sa v nasledovnom výklade koncentrovať už len na tento inštitút. Materiálnou bázou príspevku je jednak paragrafové znenie príslušného oddielu a v rámci úvodnej právnej analýzy časť dôvodovej správy, ktorej predmetom je následné dedenie. Tento návrh (paragrafové znenie) bol vydaný pôvodne v maďarskom jazyku, avšak v pomerne krátkom čase bol preložený aj do nemeckého jazyka.⁸

⁴ GERGEL, Peter – ŠVECOVÁ, Adriana: Dedičské právo podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z roku 1900, s. 67.

⁵ GERGEL, Peter – ŠVECOVÁ, Adriana: Dedičské právo podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z roku 1900, s. 68.

⁶ BGB – Bürgerliches Gesetzbuch – nemecký občiansky zákonník (1896).

⁷ HAMZA Gábor: Beitrag zur Geschichte der Kodifikation des bürgerlichen Rechts in Ungarn. In: Symposium hundert Jahre BGB. Entwicklung des Privatrechts im deutschen und mitteleuropäischen Sprachraum seit dem Inkrafttreten des BGB. 13.-14. október 2000. Budapest: Eötvös Loránd Universität, Fakultät für Staats- und Rechtswissenschaften. 2006, s. 4 – 5.

⁸ Viac k historickým súvislostiam vzniku predmetného textu v publikácii GERGEL, Peter – ŠVECOVÁ, Adriana: Dedičské právo podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z roku 1900 (vo vybraných právnohistorických a lingvistických súvislostiach). Praha: Leges, 2021; preklad názvov častí oddielu do slovenského jazyka bol takisto prevzatý z uvedenej publikácie).

Inštitút následného dedenia v súdobej diskusii

V rámci spomínaného paragrafového znenia sa, ako už bolo uvedené vyššie, o následnom dedení⁹ pojednáva v §§ 1864 – 1884. V prvom rade šlo o otázku, či bol tento inštitút (a to aj na základe diachrónneho pohľadu v rámci Uhorska) opodstatnený, resp. či sa následné dedenie malo zachovať, zrušiť alebo obmedziť. Autor návrhu sa však venuje aj vymedzeniu následného dedenia (§ 1864). Zaujímavou otázkou sú aj dôvody, ktoré viedli autora k právnej konštrukcii fiktívneho následného dedenia (v origináli „construált utóörölés“, bližšie rozvedenej v §§ 1865 – 1867)¹⁰, ktorú by sme mohli dať do protikladu k reálnemu následnému dedeniu, t. j. ak je následné dedenie explicitne identifikovateľné v dispozícii závetcu. Predmetom §§ 1868 – 1871 sú podmienky následného dedenia.¹¹ Pri tomto dedičskoprávnom inštitúte je mimoriadne dôležité vymedzenie práv prvého a následného dediča¹², resp. ich vzťah §§ 1872 – 1884. Podstatnou je tu najmä otázka stupňa ochrany následného dediča voči (potencionálnemu) ohrozeniu jeho práv zo strany prvého dediča.

Otázka zachovania, obmedzenia príp. zrušenia je predmetom úvodu do komentáru k jednotlivým §§ týkajúcim sa následného dedenia.¹³ Autor v tejto časti dôvodovej správy uvádza, že následné dedenie poznalo už uhorské právo pred roka 1848. Z

⁹ „Dedičské náhradníctvo a nástupníctvo je inštitútom dedičského práva, ako úkon pre prípad smrti s ustanovením nie len dediča ale aj inej osoby, ako jeho nástupcu alebo náhradníka. Podľa toho či tou „inou“ osobou okrem závetného dediča je náhradník, teda osoba, ktorá bude dediť namiesto závetného dediča alebo či tou „inou“ osobou je nástupca, teda osoba, ktorá bude dediť po smrti závetného dediča rozlišujeme substitúciu vulgárnu alebo fideikomisárnu.“ IMRICH BREZNOŠČÁKOVÁ, Miriam: Fideikomisárna substitúcia a jej miesto v právnom poriadku Slovenskej republiky *de lege ferenda*. In: Vybrané otázky dedičského práva v úvahách *de lege ferenda*. Bratislava: Wolters Kluwer SR s. r. o., 2022, s. 9.

¹⁰ Všeobecne autor dôvodovej správy odôvodňuje túto konštrukciu prípadmi nejasných závetných dispozícií, ktoré síce neobsahujú explicitne určenie následného dediča, ale ich platnosť je naviazaná na ich prekvalifikovanie na následné dedenie. Pozri viac Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 136 – 137.

¹¹ Okrem iného sa tu uvádza, že v pochybnostiach sa považuje určenie následného dediča za určenie náhradného dediča, pre následné dedenie bola určená lehota 32 rokov od smrti poručiteľa, následné dedenie sa v pochybnostiach vzťahovalo aj na dedičský podiel, ktorý pripadol dedičovi v dôsledku odpadnutia spoludediča a v pochybnostiach sa nevzťahovalo prvý odkaz.

¹² Vzťah, resp. terminologický rozdiel medzi prvým a následným dedičom by sa dal vysvetliť tak, že následný dedič je dedičom poručiteľa, ale k dedičstvu sa dostane až po osobe, ktorá bola určená za prvého dediča. Pozri bližšie FERRARI, Susanne – HAMPTON, Christine – SCHWARZENEGGER, Peter – VACLAVEK, Anna: Die gewillkürte Erbfolge In: Erbrecht. Wien: MANZ'sche Verlags- und Universitätsbuchhandlung GmbH, 2020, s. 323.

¹³ Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 132 – 135, preklad do slovenského jazyka P. Gergel a A. Švecová.

argumentov za zachovanie následného dedenia, ktoré uvádza autor dôvodovej správy vyberám nasledovné (ťažiskové): poručiteľ sa chce postarať o zachovanie majetku, no domnieva sa, že dedič, ktorému chce zanechať dedičstvo v prvom rade, ho nebude ochotný alebo schopný udržať v celku; poručiteľ síce chce dedičovi prenechať majetok, ale nie jeho zákonným alebo závetným dedičom (napr. v prípade, ak poručiteľ zanechá majetok manželke, a pre prípad jej smrti určí za následného dediča niektorého pokrvného príbuzného).¹⁴ „Na druhej strane by sa neobmedzená realizácia následného dedenia mohla zvrhnúť, ak by sme dovolili, aby poručiteľ bezprostredne určil dedičský poriadok a zároveň prostredníctvom tohto dedenia určil stupňovité dedenie ľubovoľných budúcich generácií, čím by sme opäť umožnili večnú viazanosť majetku, ktorú po dlhých bojoch zrušilo zákonodarstvo z roku 1848.“¹⁵ Autor dôvodovej správy teda vo vzťahu k úprave tohto inštitútu v zahraničí rezumuje: „Z týchto dôvodov (zahraničné, pozn. prekl.) zákonodarstvá nedovoľujú uvedené neobmedzené určenie následného dediča, ale všade ho presne vymedzujú, ba dokonca ho niekde i zakazujú.“¹⁶ Otázka spôsobu obmedzenia, resp. časového vymedzenia následného dedenia rezonovala pochopiteľne aj v súdobých legislatívnych úpravách nemecky hovoriacich krajín. V zmysle ALR bolo fideikomisárne náhradníctvo¹⁷ prípustné len pre prvého a druhého substitúta a podľa ABGB sa mohlo fideikomisárne náhradníctvo rozšíriť aj na tretieho, príp. štvrtého dediča v prípade, že sú všetci fideikomisárni dediči rovesníkmi poručiteľa.¹⁸ Z niekoľkých nemeckých úprav spomeňme ešte nemecký občiansky zákonník. „BGB [...] umožnil určiť následného dediča bez obmedzenia i viac krát po sebe, ale toto určenie následného dediča bude neplatné, ak k nemu nedôjde v lehote do 30 rokov

¹⁴ Porovnaj Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 132.

¹⁵ Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 132 – 133.

¹⁶ Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 133.

¹⁷ Používa sa aj termín zverenecké nástupníctvo, resp. fideikomisárna substitúcia. (IMRICH BREZNOŠČÁKOVÁ, Miriam: Fideikomisárna substitúcia a jej miesto v právnom poriadku Slovenskej republiky *de lege ferenda*. In: Vybrané otázky dedičského práva v úvahách *de lege ferenda*. Bratislava: Wolters Kluwer SR s. r. o., 2022, s. 9; GANDŽALOVÁ, Daniela: Návrat k tradíciám dedenia [online]. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici – Belianum, 2023, s. 36,37 [29.10. 2025].

¹⁸ 1. časť, čl. 12, § 55 ALR – Allgemeines Landrecht für die preussischen Staaten – pruské Všeobecné zemské právo (1794) a § 611 ABGB – Allgemeines bürgerliches Gesetzbuch – rakúsky Všeobecný občiansky zákonník (1811); citované podľa Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 134.

od smrti poručiteľa (pozri bližšie odôvodnenie k § 1870 NUOZ).¹⁹ NUOZ sa teda principiálne priklonil k zachovaniu tohto inštitútu s obmedzením na 32 rokov od smrti poručiteľa.²⁰

Syntaktické štýlémy a ich charakteristika

Z globálneho štylistického hľadiska patrí analyzovaný korpus ako legislatívny text do právnej komunikačnej sféry. V tejto súvislosti sa uvádza aj termín zákonodarný štýl, na ktorý nadviazal termín legislatívny štýl.²¹ Právne texty sú špecifické svojou funkciou, s čím súvisí samozrejme aj výber jazykových prvkov, ktoré následne zohrávajú úlohu aj pri štylistickom profile daného typu textu. Jedným z princípov, ktoré sa podieľajú na utváraní právnych (legislatívnych) textov je určite aj opakovanie.²² V skúmanom korpuse teda predpokladám jeho časté využívanie. Predkladaný výskum z priestorových dôvodov zameriam výhradne na syntaktické štýlémy a štylistický princíp opakovania, ktorý by sa v nich mal aj podľa odbornej literatúry uplatňovať.

Pod pojmom štýléma rozumiem v súlade s odbornou literatúrou jazykový prvok, ktorý v štruktúrnom a situatívnom kontexte sprostredkúva štylistický význam.²³ V rámci štylistickej paradigmy rozlišuje Vajičková²⁴ tieto štýlémy: verbálne, kompozíciu a neverbálne. Verbálne štýlémy člení následne na fónické segmentálne, grafické grafemické, lexikálne, morfológické a syntaktické. Keďže sa v príspevku budem venovať výhradne vetnej skladbe predmetného textu, v nasledujúcom výklade budem analyzovať, čo tvorí syntaktické štýlémy vo všeobecnosti a vychádzajúc zo špecifik syntaxe právnych noriem budem analyzovať predmetný korpus za účelom funkčného opisu syntaktických javov. Vajičková rozumie pod syntaktickými štýlémami variačné možnosti, konkurenčné syntagmatické štruktúry, syndetické a asyndetické súvetia, radenie vetných členov, pozíciu časovaného

¹⁹ Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Oröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 135.

²⁰ Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Oröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902, s. 135.

²¹ SLANČOVÁ, Daniela – SPÁČILOVÁ, Stanislava: Štylistické výskumy v časopise Slovenská reč. In: Slovenská reč, Roč. 87, č. 3 (2022), s. 299.

²² VAJIČKOVÁ, Mária – ĐURICOVÁ, Alena – KOSTELNÍKOVÁ, Mária – TUHÁRSKA, Zuzana. Stilistische Prinzipien der Gestaltung administrativer und juristischer Texte. Nümbrecht: KIRSCH-Verlag, 2011, s. 52 – 53.

²³ BUßMANN, Hadumod. Lexikon der Sprachwissenschaft. Stuttgart: Kröner, 2008, s. 684.

²⁴ VAJIČKOVÁ, Mária. Theoretische Grundlagen stilistischer Textanalyse. Nümbrecht: KIRSCH-Verlag, 2007, s. 100 – 133.

slovesa, vetný rámec (vybočenie z rámca), dĺžku vety (krátke vety, vety strednej dĺžky, dlhé vety) a atypické syntaktické konštrukcie.²⁵

V rámci odborného (nemeckého) jazyka v oblasti syntaxe konštatuje Roelcke²⁶ dominanciu oznamovacích, účelových a vzťažných viet, viacnásobné atribúty, analytické verbonominálne spojenia a predložkové konštrukcie. Nadreprezentáciu vyššie uvedených syntaktických javov interpretuje z funkčného hľadiska tak, že producenti odborných textov k nim siahajú za účelom lepšej zrozumiteľnosti, zvýšenia anonymizácie a explicitného spôsobu vyjadrovania pomocou logického prepojenia.

Podľa Abrahámovej súvisí syntax právnej normy najmä s právnou logikou. Zo štruktúrneho hľadiska hovoríme buď o dichotomickej alebo trichotomickej štruktúre právnych noriem (hypotéza, dispozícia, sankcia). Právne normy majú formu deskriptívnych (opisných) a preskriptívnych (nariaďujúcich, normatívnych) viet. Deskriptívne vety vyskytujúce sa vo forme podmienkových viet môžu mať podobu kumulatívnych alebo alternatívnych podmienok a indikátormi sú v tomto prípade aj typické spojky. Na druhej strane slúžia preskriptívne vety na vyjadrenie príkazu, zákazu, výslovného dovolenia [...] čiže slúžia podľa právnej teórie na vyjadrenie normatívnych modalít.²⁷

Prvou výskumnou kategóriou, ktorou sa budem vo vzťahu k výskumnému korpusu zaoberať, je dĺžka viet. Výskumný korpus tvorí spolu 40 viet (§§ 1864 – 1884 nemeckej verzie NUOZ). Najdlhšia veta má 51 slov (§ 1868: „Hat der Erblasser einem solchen Abkömmlinge für den Fall des Todes desselben einen Nacherben eingesetzt, der zur Zeit der Testamentserrichtung selber noch keinen Abkömmling hat, oder von dessen Abkömmlinge der Erblasser zu dieser Zeit nicht weiss, so ist die Nacherbeinsetzung im Zweifellsfalle unwirksam, sobald der Erbe mit Hinterlassung eines Abkömmlings stirbt.“), najkratšia šesť (§ 1864: „§ 74 wird hiedurch nicht berührt.“). Ako už bolo vyššie spomenuté, dĺžka vety patrí tiež k syntaktickým štylémam. Pri klasifikácii viet na krátke, stredne dlhé a dlhé som vychádzal z členenia, ktoré uvádza Vajičková, ktorá s odvolaním sa na príslušnú odbornú literatúru za vety strednej dĺžky považuje vety, ktoré majú od 10 do 20 slov. Logicky sú potom vety krátke v rozsahu do 9 slov a dlhé nad 20 slov.²⁸ Do kategórie krátkych viet spadá spolu 6 viet (15 % viet z celého korpusu), stredne dlhých viet je 16 (t. j. 40%) a dlhých 18 (45%). Priemerný počet slov vo vete je 23,35 slova. Zaujímavé je porovnanie s priemerným počtom slov vo vete uvádzaným pre nemecký jazyk zákonov. Brandt uvádza priemernú dĺžku vety

²⁵ VAJIČKOVÁ, Mária. Theoretische Grundlagen stilistischer Textanalyse. Nümbrecht: KIRSCH-Verlag, 2007, s. 128 – 133.

²⁶ ROELCKE, Thorsten. Fachsprachen. Berlin: Erich Schmidt Verlag GmbH & Co. KG, 2010, s. 89.

²⁷ ABRAHÁMOVÁ, Eva. Základy právnej komunikácie. Šamorín: Heuréka, 2012, s. 49 – 51.

²⁸ VAJIČKOVÁ, Mária. Theoretische Grundlagen stilistischer Textanalyse. Nümbrecht: KIRSCH-Verlag, 2007, s. 131 – 132.

v zákonoch pre 1. pol. 18. stor. 89,9 slov. Neskôr došlo k jej znižovaniu až na 30,9 slov v 2. pol. 19. storočia a 26,8 slov v 1. pol. 20. storočia.²⁹ Dĺžka viet v skúmanom korpuse sa teda veľmi nevymyká priemeru. Z hľadiska kategorizácie viet na oznamovacie, opytovacie a rozkazovacie konštatujem stopercentné zastúpenie oznamovacích viet. Toto zistenie je v súlade s Roelckem,³⁰ ktorý konštatuje dominantnú úlohu oznamovacích viet v nemeckom odbornom jazyku všeobecne.

V celom korpuse mierne dominujú zložené vety (55%); ide výhradne o podradňovacie súvetia, percentuálne zastúpenie jednoduchých viet je 45 %. Čo sa týka vzťahu medzi týmito dvomi kategóriami a počtom slov, tak v súvetiach je logicky vyšší priemerný počet slov vo vete (68% súvetí pripadá na dlhé vety), na jednoduché vety pripadá 33% krátkych viet. Súvetia spadajú bez výnimky do kategórie stredne dlhých a dlhých viet a jednoduché vety až na tri výnimky (dlhé vety v rozsahu 22, 25 a 46 slov) do kategórie stredne dlhých a krátkych viet. Z hľadiska členenia súvetí na priradňovacie a podradňovacie konštatujem dominanciu podradňovacích súvetí (v pomere 91% v prospech podradňovacích súvetí), čo zrejme úzko súvisí s dominanciou podmienkových viet v rámci podradňovacích súvetí (80 %).

Z hľadiska sémantickej klasifikácie vedľajších viet³¹ teda prevládajú podmienkové vety, čo je vzhľadom na charakter skúmaného korpusu aj logické. „Podmienkové vety vypovedajú o tom, že ak sa splní podmienka, nastane následok. V dichotomickom ponímaní to znamená: ak je p, tak je q, v trichotomickom ponímaní: ak je p, tak je q, inak s (sankcia).³² V dedičskom práve je možné hovoriť skôr o dichotomickom poňatí a deskriptívnych (opisných) vetách³³, čo dokazujú aj podmienkové vety v skúmanom korpuse. (napr. § 1878: „Verweigert der Nacherbe diese Einwilligung ohne genügenden Grund, oder ist er verhindert, sie zu ertheilen und liegt Gefahr im Verzuge, so kann das Nachlassgericht die Einwilligung ertheilen.“; § 1867: „Hat der Erblasser verfügt, dass der testamentarische Erbe erst von einem gewissen Zeitpunkte oder Ereignisse angefangen Erbe sein sollte, ohne aber bis dahin einen Erben eingesetzt zu haben, so ist bis dahin der gesetzliche Erbe des Erblassers als Erbe anzusehen.“). Podmienkové vety sa v skúmanom korpuse väčšinou uvádzajú asyndeticky (10 prípadov z celkového počtu 17 podmienkových súvetí v korpuse),

²⁹ BRANDT, Wolfgang: Müssen Gesetze schwer verständlich sein? Einwände eines Linguisten gegen Schutzbehauptungen der Juristen. In: Sprache – Recht – Geschichte. Rechtshistorisches Kolloquium 5.-9. Juni 1990 Christian-Albrechts-Universität zu Kiel. (Motive – Texte – Materialien 58). Heidelberg: ECKERT, Jörn – HATTENHAUER, Hans, 1991, 339 – 361, citované podľa SEIFERT, Jan, Funktionsverbgefüge in der deutschen Gesetzessprache (18. – 20. Jahrhundert). Hildesheim – Zürich – New York: Georg Olms Verlag, 2004, s. 116.

³⁰ ROELCKE, Thorsten. Fachsprachen. Berlin: Erich Schmidt Verlag GmbH & Co. KG, 2010, s. 86.

³¹ DÜRSCHIED, Christa: Syntax. Grundlagen und Theorien. Mit einem Beitrag von Martin Businger, 5., durchgesehene Auflage. Göttingen: Vandenhoeck & Ruprecht GmbH & Co. KG, 2010, s. 61.

³² ABRAHÁMOVÁ, Eva. Základy právnej komunikácie. Šamorín: Heuréka, 2012, s. 49.

³³ ABRAHÁMOVÁ, Eva. Základy právnej komunikácie. Šamorín: Heuréka, 2012, s. 49 – 50.

príp. so spojku „wenn“ alebo „falls“. Vyskytuje sa však aj vedľajšia veta uvedená particípiom (jeden výskyt, § 1882: „Für eine Verschlechterung oder für den Verlust von Sachen hat der Erbe, vorausgesetzt, dass dies durch die ordnungsmässige Benützung herbeigeführt wurde, oder im Laufe der Zeit von selbst eingetreten ist, nicht aufzukommen.“).³⁴ Do slovenského jazyka sa uvedené podmienkové spojky, príp. asyndetické podmienkové konštrukcie prekladajú pomocou spojky „ak“.³⁵ V tejto súvislosti je potrebné podotknúť, že v slovenskom jazyku sa podmienka dá vyjadriť aj predložkovými pádmi.³⁶

V predmetnom texte sme identifikovali aj jazykové šablóny, pod ktorými Abrahámová rozumie ustálené frazeologické jednotky a bližšie ich špecifikujú ako „viacslovné, polovetné alebo vetné konštrukcie, ktoré vstupujú do jazykového prejavu právnikov ako konštrukčne hotové samostatné jednotky.“³⁷ Vzhľadom na monotematický charakter skúmaného korpusu je pochopiteľné, že dochádza k opakovaniu istých slovných spojení (jazykových šablón), ktoré tvoria kostru (podmienkových) viet, ako napr. „Hat der Erblasser..... verfügt“; „Die Nacherbfolge tritt ein/erfolgt/ erstreckt sich/..... „Der Erbe/ Nacherbe kann/ leistet....; „In Ansehung.... kann“ atď. Čiže do tejto miery sa tu prejavuje štylistický princíp opakovania. Variácia sa dostáva k slovu pri dosadzovaní do týchto „vzorcov“. Avšak podobne ako je tomu pri frazeologizovaných konštrukciách, ide len o obmedzenú kombinovateľnosť s typickými lexémami.³⁸

Záver

Následné dedenie bol v súdobej strednej Európe bežný právny inštitút, hoci niektoré právne poriadky ho z rôznych dôvodov neuznávali. Autor dôvodovej správy navrhoval tento inštitút ponechať, avšak nie v neobmedzenej forme. Aj napriek tomu ho nepovažoval za preferovaný dedičskoprávny inštitút, keďže si vyžadoval istú formu viazanosti majetku a obmedzenia pre prvého dediča pri dispozícii s ním. Z lingvistického hľadiska som v analyzovanom korpuse identifikoval také prvky na

³⁴ Ku korelátom a spôsobom uvádzania podmienových viet v nemeckom jazyku pozri HELBIG, Gerhard – BUSCHA, Joachim: Deutsche Grammatik. Ein Handbuch für den Ausländerunterricht. Leipzig, Berlin, München: Verlag Enzyklopädie Leipzig, 1998, s. 690 – 691.

³⁵ Pozri preklad paragrafového znenia NUOZ (časť následné dedenie) do slovenského jazyka v publikácii GERGEL, Peter – ŠVECOVÁ, Adriana: Dedičské právo podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z roku 1900 (vo vybraných právnohistorických a lingvistických súvislostiach). Praha: Leges, 2021, s. 158 – 161.

³⁶ IVANOVÁ, Martina: Syntaktické výskumy v časopise Slovenská reč. In: Slovenská reč, Roč. 87, č. 3 (2022), s. 137.

³⁷ ABRAHÁMOVÁ, Eva. Základy právnej komunikácie. Šamorín: Heuréka, 2012, s. 44.

³⁸ ĎURČO, Peter: Frazeologizované konštrukcie na príklade nemeckého a slovenského jazyka. In: Slovenská reč, Roč. 90, č. 1 (2025), s. 45.

syntaktickej roviny, ktoré sú zo štylistického hľadiska príznakové pre tento typ právneho textu. Patrí sem spomenuté výlučné zastúpenie oznamovacích viet, ktoré je funkčne zdôvodniteľné vo vzťahu ku komunikovanému obsahu legislatívnych textov. Nadreprezentácia podmienkových viet má z funkčného hľadiska takisto opodstatnenie, keďže slúži na formuláciu právnych noriem. Dôležitú funkciu vzhľadom na komunikovanie špecifického právneho obsahu v danom legislatívnom texte zohráva aj opakovanie spojené s dosť obmedzenými variačnými možnosťami, čo podčiarkuje strohý charakter syntaktickej a lexikálnej roviny analyzovaného korpusu. Záverom je možné konštatovať, že syntaktická skladba textu tendujúca k nadreprezentácii, príp. výlučnému zastúpeniu istých jazykových prvkov je z účelovo zdôvodniteľná a podieľa sa významne na štylistickom profile skúmaného legislatívneho textu.

Zoznam použitej literatúry

1. ABGB – Allgemeines bürgerliches Gesetzbuch – rakúsky Všeobecný občiansky zákonník (1811).
2. ABRAHÁMOVÁ, Eva. Základy právnej komunikácie. Šamorín: Heuréka, 2012. 128 s. ISBN 978-8-0891-2281-3.
3. ALR – Allgemeines Landrecht für die preussischen Staaten – pruské Všeobecné zemské právo (1794).
4. BGB – Bürgerliches Gesetzbuch – nemecký občiansky zákonník (1896).
5. BRANDT, Wolfgang: Müssen Gesetze schwer verständlich sein? Einwände eines Linguisten gegen Schutzbehauptungen der Juristen. In: Sprache – Recht – Geschichte. Rechtshistorisches Kolloquium 5.-9. Juni 1990 Christian-Albrechts-Universität zu Kiel. (Motive – Texte – Materialien 58). Heidelberg: ECKERT, Jörn – HATTENHAUER, Hans, 1991, s. 339 – 361. ISBN: 978-3-8487-3041-4.
6. BUßMANN, Hadumod. Lexikon der Sprachwissenschaft. Stuttgart: Kröner, 2008. 816 s. ISBN 978-3-520-45204-7.
7. ĎURČO, Peter: Frazologizované konštrukcie na príklade nemeckého a slovenského jazyka. In: Slovenská reč, Roč. 90, č. 1 (2025), s. 32 – 50. ISSN 0037-6981.
8. DÜRSCHIED, Christa: Syntax. Grundlagen und Theorien. Mit einem Beitrag von Martin Businger, 5., durchgesehene Auflage. Göttingen: Vandenhoeck & Ruprecht GmbH & Co. KG, 2010. 256 s. ISBN 978-3-8252-3319-8.
9. FERRARI, Susanne – HAMPTON, Christine – SCHWARZENEGGER, Peter – VACLAVEK, Anna: Die gewillkürte Erbfolge In: Erbrecht. Wien: MANZ'sche Verlags- und Universitätsbuchhandlung GmbH, 2020, s. 149 – 391. ISBN 978-3-214-05433-5.

10. GANDŽALOVÁ, Daniela: Návrat k tradíciám dedenia [online]. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici – Belianum, 2023, 137 s. [29.10. 2025]. ISBN 978-80-557-2035-7.
11. GERGEL, Peter – ŠVECOVÁ, Adriana: Dedičské právo podľa I. návrhu uhorského Všeobecného občianskeho zákonníka z roku 1900 (vo vybraných právnohistorických a lingvistických súvislostiach). Praha: Leges, 2021. 191 s. ISBN 978-80-7502-558-6.
12. HAMZA Gábor: Beitrag zur Geschichte der Kodifikation des bürgerlichen Rechts in Ungarn. In: Symposium hundert Jahre BGB. Entwicklung des Privatrechts im deutschen und mittel-osteuropäischen Sprachraum seit dem Inkrafttreten des BGB. 13.-14. október 2000. Budapest: Eötvös Loránd Universität, Fakultät für Staats- und Rechtswissenschaften. 2006, s. 1 – 12. ISBN 963-463-815- 5.
13. HELBIG, Gerhard – BUSCHA, Joachim: Deutsche Grammatik. Ein Handbuch für den Ausländerunterricht. Leipzig, Berlin, München: Verlag Enzyklopädie Leipzig, 1998. 736 s. ISBN 3-324-00118-8.
14. IMRICH BREZNOŠČÁKOVÁ, Miriam: Fideikomisárna substitúcia a jej miesto v právnom poriadku Slovenskej republiky de lege ferenda. In: Vybrané otázky dedičského práva v úvahách de lege ferenda. Bratislava: Wolters Kluwer SR s. r. o., 2022, s. 7 – 30. ISBN 978-80-571-0545-9.
15. Indokolás a magyar általános polgári törvénykönyv tervezetéhez. Otödik kötet, Öröklési jog. Budapest: Grill. Károly cs. és kir. udv. könyvkereskedése, 1902. 460 s.
16. IVANOVÁ, Martina: Syntaktické výskumy v časopise Slovenská reč. In: Slovenská reč, Roč. 87, č. 3 (2022), s. 130 – 163. ISSN 0037-6981.
17. NUOZ – Entwurf eines ungarischen allgemeinen bürgerlichen Gesetzbuches. Budapest: Grill'sche K. und K. Hofbuchhandlung, 1901.
18. ROELCKE, Thorsten. Fachsprachen. Berlin: Erich Schmidt Verlag GmbH & Co. KG, 2010. 269 s. ISBN 978-3-503-12221-9.
19. SEIFERT, Jan, Funktionsverbgefüge in der deutschen Gesetzessprache (18. – 20. Jahrhundert). Hildesheim – Zürich – New York: Georg Olms Verlag, 2004. 284 s. ISBN: 3-487-12554-4.
20. SLANČOVÁ, Daniela – SPÁČILOVÁ, Stanislava: Štylistické výskumy v časopise Slovenská reč. In: Slovenská reč, Roč. 87, č. 3 (2022), s. 283 – 306. ISSN 0037-6981.
21. VAJIČKOVÁ, Mária – ĎURICOVÁ, Alena – KOSTELNÍKOVÁ, Mária – TUHÁRSKA, Zuzana. Stilistische Prinzipien der Gestaltung administrativer und juristischer Texte. Nümbrecht: KIRSCH-Verlag, 2011. 153 s. ISBN 978-3-933586-88-9.
22. VAJIČKOVÁ, Mária. Theoretische Grundlagen stilistischer Textanalyse. Nümbrecht: KIRSCH-Verlag, 2007. 168 s. ISBN 978-80-223-2401-4.

Kontaktné údaje

PaedDr. Peter Gergel, PhD.

e-mail gergel@fedu.uniba.sk

Katedra nemeckého jazyka, literatúry a didaktiky, Pedagogická fakulta Univerzity Komenského v Bratislave.

Bratislavské právnické fórum 2024
Univerzita Komenského v Bratislave
Právnická fakulta
1. vydanie
2025

ISBN 978-80-7160-772-4
ISSN 2989-4808

The project is co-financed by the governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from the International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.



PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

ISBN: 978-80-7160-772-4