

DIGITÁLNÍ EKONOMIKA A SPOLEČNOST

Růžena Ferebauerová, Oldřich Pekárek et al.



Vysoká škola evropských a regionálních studií, z. ú.
České Budějovice

2019

Vědecká redakce VŠERS:

doc. JUDr. PhDr. Jiří Bílý, CSc.; doc. Ing. Jiří Dušek, Ph.D. (předseda); RNDr. Růžena Ferebauerová; PhDr. Jan Gregor, Ph.D.; doc. Ing. Marie Hesková, CSc.; PaedDr. Vladimír Kříž; doc. Ing. Oldřich Pekárek, CSc.; doc. Ing. Ladislav Skořepa, Ph.D.; doc. JUDr. Roman Svatoš, Ph.D.

Název:	DIGITÁLNÍ EKONOMIKA A SPOLEČNOST
Autoři:	RNDr. Růžena Ferebauerová, doc. Ing. Oldřich Pekárek, CSc. et al.
Vydavatel:	Vysoká škola evropských a regionálních studií, z. ú. Žižkova tř. 6, 370 01 České Budějovice
Recenzenti:	doc. JUDr. PhDr. Jiří Bílý, CSc. doc. Ing. Ladislav Skořepa, Ph.D.
Účel:	Monografie

Publikace neprošla jazykovou úpravou

Vzor citace:

Ferebauerová, R., Pekárek, O. et al. *Digitální ekonomika a společnost*. 1. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, 2019. 113 s. ISBN 978-80-7556-048-3.

KATALOGIZACE V KNIZE - NÁRODNÍ KNIHOVNA ČR

Ferebauerová, Růžena

Digitální ekonomika a společnost / Růžena Ferebauerová, Oldřich Pekárek et al. -- České Budějovice : Vysoká škola evropských a regionálních studií, z.ú., 2019. -- 113 stran

Částečně anglický a slovenský text, anglické resumé

Obsahuje bibliografii a rejstřík

ISBN 978-80-7556-048-3 (brožováno)

* 004 * 304 * 33 * 334.012.63/.64 * 351.78:004.7 * 342.721 * 338.45:004 *
(4) * (048.8:082)

- digitalizace -- země Evropské unie
- digitalizace -- sociální aspekty
- digitalizace -- ekonomické aspekty
- malé a střední podniky -- země Evropské unie
- kybernetická bezpečnost -- země Evropské unie
- ochrana osobních údajů -- země Evropské unie
- průmysl 4.0 -- země Evropské unie
- kolektivní monografie

33 - Ekonomie [4]

AUTORSKÝ KOLEKTIV

Barnová Silvia	kap. 2.5
Beláňová Benita	kap. 1.1
Butoracová Šindleryová Ivana	kap. 2.6
Čajková Andrea	kap. 2.6
Dorner Wolfgang	kap. 2.3
Đuriš Marcel	kap. 1.4
Falter Magdalena	kap. 2.3
Ferebauerová Růžena	úvod
Heligman Richard	kap. 1.4
Jenčo Eduard	kap. 2.1
Kotýnková Magdalena	kap. 2.7
Krásna Slávka	kap. 2.5
Matkovčíková Natália	kap. 1.2
Nováčková Daniela	kap. 1.3, 2.2
Pekárek Oldřich	úvod
Saxunová Darina	kap. 2.4
Stankovičová Iveta	kap. 2.2
Strážovská Ľubomíra	kap. 1.4
Sulíková Rozália	kap. 1.4
Wefersová Jarmila	kap. 1.3

ANOTACE

Publikace DIGITÁLNÍ EKONOMIKA A SPOLEČNOST se zabývá aktuálními otázkami a problémy spojenými s rozvojem digitalizace, které se promítají do ochrany osobních dat, důvěryhodnosti informací distribuovaných prostřednictvím internetu a Průmyslu 4.0, což má vliv nejen na rozvoj ČR, ale celé Evropské unie.

Publikace prezentuje různé pohledy autorů k probíhající digitalizaci informatického prostoru a s tím spojeným rozvojem umělé inteligence, jako základního faktoru příštího kvalitativního rozvoje lidské společnosti. Autorsky se na monografii podílelo celkem dvacet českých, slovenských a německých odborníků z různých vysokých škol a odborných pracovišť.

Monografie je rozdělena na dvě části:

- ✓ Digitalizace a její dopad na informační bezpečnost uživatelů,
- ✓ Problémy využívání možností a služeb digitálního prostředí.

Monografie čerpá z autorských účastí na vědeckých fórech a předkládá myšlenky důležitých příspěvků a závěrů.

Publikace je určena zejména vědeckým pracovníkům, empiricky orientovaným výzkumníkům a studentům, zaujmout však může svou tematikou i laickou veřejnost.

Klíčová slova:

Digitalizace, Evropská unie, kybernetická bezpečnost, malé a střední podniky, management, ochrana dat.

ANNOTATION

The publication output DIGITAL ECONOMICS AND SOCIETY deals with current issues and problems connected with the development of digitization which are reflected in personal data protection, credibility of information spread via the Internet and Industry 4.0, which affects the development not only in the Czech Republic, but also throughout the European Union.

The monograph presents various views of authors dealing with the ongoing digitization of information area and the development of artificial intelligence, which is closely connected to it. Artificial intelligence is a fundamental aspect of further quality development of human society. Overall, there are twenty Czech, Slovak and German experts from various universities and specialized workplaces, participating in this publication output.

The monograph is divided into two chapters as follows:

- ✓ Digitization and its impact on information security of users,
- ✓ Problems of use of facilities and services of digital environment.

The monograph gains the information from authors' participation at scholarly forums and presents the ideas of important contributions and conclusions.

The monograph is intended for scholars, empirically oriented researchers and students mainly, but due to its topics it can also attract non-professionals.

Key words:

Digitization, European Union, cybersecurity, SME's, management, data protection.

OBSAH

Úvod	8
1 Digitalizace a její dopad na informační bezpečnost uživatelů	10
1.1 Kybernetická bezpečnost v práci s personálními datami v malých a středních podnicích SR	10
1.2 Kybernetická bezpečnost údajov o bezpečnosti a ochrane zdravia pri práci zamestnancov v malých a stredných podnikoch.....	19
1.3 Ochrana osobných údajov v kontexte judikatúry Súdneho dvora EÚ	24
1.4 Dôveryhodnosť informácií distribuovaných prostredníctvom internetu.....	32
2 Problémy využívání možností a služeb digitálního prostředí	38
2.1 Všeobecné základy cloudovej zmluvy ako inomínátneho kontraktu pri dodávke a prevádzke informačných systémov	38
2.2 Služby poskytované digitálnymi platformami	44
2.3 Digitization and rural development - Clash or potential?	52
2.4 Výzvy riadenia blokchainových technológií v európskom priestore.....	61
2.5 Digitálny humanizmus ako aktuálna výzva pre ďalší rozvoj a smerovanie Európskej únie	73
2.6 Ekonomika 4.0 a digitálna konkurencieschopnosť	77
2.7 Stane se základní nepodmíněný příjem nástrojem přerozdělování v nadcházející éře digitalizace a robotizace?	86
Literatura	95
Rejstřík	111
Adresář	112

Úvod

Pojmy digitalizace, informační technologie, internet, počítač, mobilní telefon, kybernetický prostor, umělá inteligence, ale i kyberkriminalita jsou stále častěji předmětem odborných diskuzí a vědeckých prací. Digitalizace stále více zasahuje do všech oblastí lidské činnosti a ve svém důsledku má dopad i na soukromí občana. Pro ujednacení předmětu publikace, rozumíme pod názvem digitalizace přechod na sdělování informací výhradně v číselné formě, která umožňuje plné využití výpočetní techniky a kapacit komunikačního prostředí.

Problémy spojené s rozvojem digitalizace se promítají do ekonomiky, bezpečnosti, ekologie a sociálních vztahů jednotlivých států i regionů. Jsou proto i předmětem společných legislativních opatření Evropské unie i samotných členských zemí. Jako příklady lze uvést např. Digitální agendu pro Evropu, Digitální Česko, Digitální ekonomika a společnost, Evropa 2020, Strategie pro jednotný digitální trh atp.

Obecným cílem Digitální agendy je zajistit udržitelný hospodářský a sociální přínos jednotného digitálního trhu, založeného na rychlém a superrychlém internetu a interoperabilních aplikacích.

V České republice byly stanoveny cíle, pomocí nichž se má dosáhnout stavu, kdy: „Česká republika odstraní překážky a vytvoří předpoklady zajišťující dlouhodobou prosperitu společnosti v prostředí globální digitální revoluce.“

Stanoveny jsou tyto hlavní cíle:

- ✓ Efektivnější systém přímé i nepřímé podpory výzkumu, vývoje a inovací,
- ✓ zralost a připravenost sektorů ekonomiky na digitální transformaci,
- ✓ připravenost občanů na změny trhu práce, vzdělávání a rozvoj digitálních dovedností,
- ✓ podpora konektivity a infrastruktury digitální ekonomiky a společnosti,
- ✓ zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti,
- ✓ legislativa podporující všechny aspekty digitální ekonomiky a společnosti,
- ✓ optimální systém financování digitální ekonomiky a společnosti,
- ✓ institucionální zajištění centrální koordinace politik na podporu digitální ekonomiky a společnost.

S pojmem digitální ekonomika a společnost souvisí také pojem umělá inteligence, která je logickým důsledkem bouřlivého rozvoje kybernetiky, elektroniky a informatiky. Specializovaná umělá inteligence je dnes schopna úspěšně nahradit rutinní činnosti člověka ve výrobě, bankovníctví, administrativě, řízení obranných systémů, řízení dopravy a v dalších speciálních úlohách. Stávající pojetí výroby, administrativy, logistiky a dalších odvětví neobstojí v konkurenci s kyberneticky řízenými procesy, Uvedený trend s sebou přináší nejen větší konkurenceschopnost na trhu, ale i řadu vážných hrozeb a z nich plynoucích rizik v oblasti sociální, ekonomické, bezpečnostní, edukační a dalších. Věda musí řešit především otázky přesné identifikace těchto hrozeb a souvisejících rizik, hledat nástroje k jejich minimalizaci, ale na druhé straně podporovat užitečné trendy v ekonomice, ekologii a dalších odvětvích lidské činnosti, které rozvoj umělé

inteligence mohou významně podpořit. Vědci nemohou zůstat lhostejní k dalšímu omezování soukromí občana v důsledku možnosti úplného sledování všech jeho činností a tím jej ponížit na pouhý manipulovatelný objekt, což je jedním z možných důsledků totální digitalizace společnosti.

Je třeba se připravovat na příchod umělé inteligence. Jak ale řekl Stephen Hawking, „*Vytvoření funkční obecné umělé inteligence může být největší událostí v dějinách naší civilizace. Nebo nejhorší. Jednoduše nevíme. Nevíme proto, zda nám umělá inteligence nesmírně pomůže, nebo nás bude ignorovat, odstrčí nás či nás zničí.*“

Z prací autorů této publikace je zřejmé, že se vážně zabývají důsledky digitalizace společnosti a snaží se v jednotlivých kapitolách řešit dopady nástupu digitálních technologií, kybernetiky a informatiky, do jednotlivých oblastí jejich výzkumné a aplikační tvůrčí práce a explicitně upozorňují na vznikající problémy.

Za pomoc a podporu vzniku této monografie patří laskavé poděkování nadaci Konrad-Adenauer-Stiftung v Praze, Jihočeskému kraji, Statutárnímu městu České Budějovice, Evropskému regionu Dunaj-Vltava, Jihočeskému muzeu v Českých Budějovicích, Europe Direct České Budějovice, Eurocentru České Budějovice, HZS Jihočeského kraje a Oberbance.

1 Digitalizace a její dopad na informační bezpečnost uživatelů

1.1 Kybernetická bezpečnost' v práci s personálními datami v malých a středných podnicích SR

Riadenie malých a stredných podnikov je oblasť, ktorá sa stala predmetom ekonomického skúmania len v posledných pár rokoch. Z ohľadom na vplyv veľkých organizácií na národné hospodárstvo sa malé a stredné podniky javili ako nie príliš zaujímavý objekt skúmania a implementácie vedeckých poznatkov. Zmenu myslenia spôsobili nové trendy, vyplývajúce z presadzovania globalizácie a informatizácie. Informatizácia so sebou priniesla zároveň novú oblasť, ktorú je potrebné systematicky riadiť, a to bezpečnosť informačných systémov v podniku (Szarková, 2014). O význame, ktorý je informačnej bezpečnosti prisudzovaný, svedčí aj stále rastúci záujem spoločností o koncipovanie, presadzovanie a implementáciu bezpečnostnej politiky. Informačné systémy pozostávajú z informačných technológií, procesov a ľudí, preto neoddeliteľnou súčasťou tejto politiky musia byť aj ľudské zdroje.

V oblasti informačnej bezpečnosti predstavujú jednu z najväčších hrozieb práve zamestnanci organizácie. Tých môžeme vo všeobecnosti rozdeliť na dve skupiny. Prvú skupinu tvoria pracovníci, ktorých pracovnou náplňou je správa a bezpečnosť informačných systémov a technológií v organizácii. Druhú skupinu tvoria tzv. „pasívni používatelia“ IS/IT, a najmä táto skupina býva v súčasnosti najslabším článkom bezpečnosti informácií v organizácii. A to nielen preto, že používatelia spravidla neradi čítajú smernice, a teda nedodržiavajú ich nariadenia, ale i preto, že často radi experimentujú a dopúšťajú sa tak radu zásadných prehreškov proti bezpečnosti. Tieto dve skupiny zamestnancov musíme v personálnej politike organizácie vo vzťahu k informačnej bezpečnosti posudzovať oddelene, pretože očakávania a požiadavky na ich znalosti a zručnosti sa diametrálne líšia. Taktiež ich umiestnenie v hierarchii organizácie je rozdielne. Kým prvú skupinu vieme v štruktúre identifikovať a lokalizovať, pasívni užívatelia IS/IT sa nachádzajú od riadiacich pracovníkov až po najnižší stupeň výkonných zamestnancov.

Štruktúra výsledkov prieskumu

Predkladané výsledky sú čiastkovými výstupmi rozsiahlejšieho projektu, ktorý mapuje vývoj informačnej bezpečnosti v malých a stredných podnikoch na Slovensku. Prvé kolo tohto prieskumu prebehlo už v roku 2006, následne už v oveľa širšom rozsahu v rokoch 2008, 2012, 2015 a 2017. Respondenti odpovedali na 105 otázok, rozdelených do 15-tich tematických celkov. Jednou z oblastí bolo aj personálne zabezpečenie.

Výsledky prieskumu sú uvádzané v nasledujúcej štruktúre:

- ✓ Metodika práce a metódy skúmania,
- ✓ Charakteristika skúmanej vzorky,
- ✓ Výsledky skúmania v oblasti personálneho zabezpečenia oblasti IS/IT bezpečnosti.

- ✓ Výsledky skúmania bezpečnostnej politiky vo vzťahu k ľudským zdrojom – zamestnancom organizácie.

Metodika práce a metódy skúmania

Metódu analýzy, ktorá umožňuje rozklad celku na jeho jednotlivé časti a prvky s cieľom čo najdokonalejšie spoznať subčasti systému, sme využili pri analýze súčasného stavu riešenia danej problematiky doma a v zahraničí, a tieto získané poznatky sme pomocou syntézy spojili do nového celku. Metódou komparácie boli v teoretickej časti porovnávané názory na danú problematiku a následne metódou abstrakcie vyšpecifikovaný pojmový aparát. Metóda deskripcie je použitá pri popise princípov riadenia bezpečnostných informačných systémov.

V procese testovania sme pri overovaní hypotéz realizovali prieskum formou jednej z exploračných metód – dotazníkovej metódy. Pri aplikácii metód skúmania sú potrebné informácie získavané od skúmaných subjektov dopytovaním, t.j. kladením zámerne cielených otázok. Pomocou metód zisťovania je možné získať súčasne viac informácií o individuálnom respondentovi. Tieto informácie sa môžu týkať rozsahu a hĺbky znalostí či vedomostí respondenta, preferencií, jeho minulého, súčasného alebo zamýšľaného správania sa a charakteristík respondenta. Metódy zisťovania môžu byť použité pri skúmaní akýchkoľvek súborov, teda i podnikov rôzne veľkosti, odlišnej odvetvovej štruktúry, vlastníctva a pod. Aplikáciu metód zisťovania je možné prispôbiť cieľom deskriptívneho a aj kauzálneho výskumu. Pre správne analyzovanie a následné porovnávanie javov je nevyhnutné, aby analyzované javy nastávali v rovnakých podmienkach. Inak sa objavujú chybné závery v príčinách a dôsledkoch javov, zavinené zložitou podmienkou ekonomického života.

Preto, aby sme získali relevantné a kvantifikovateľné informácie o stave bezpečnosti informačných systémov v malých a stredných podnikoch na Slovensku, boli podniky vymedzené podľa veľkosti na základe smernice Európskej komisie č. 96/280/EC, podľa odvetvovej klasifikácie ekonomických činností SK NACE Rev.2, ďalej podľa právnej formy a vlastníctva podniku. Dotazník bol spracovávaný v elektronickej forme. Pri spracovaní boli využité databázový program MS Access a tabuľkový procesor MS Excel. Pri vyhodnocovaní dotazníka boli použité matematicko-štatistické metódy. Výsledky boli transformované do formy tabuliek a grafov.

Porovnávaním javov v čase a priestore sme na základe dotazníkového prieskumu identifikovali spoločné a rozdielne stránky správania sa jednotlivých typov podnikov. Metóda indukcie nám umožnila skúmaním všetkých dostupných javov a ich častí zovšeobecniť získané poznatky.

Charakteristika skúmanej vzorky

Prieskum bol realizovaný na vzorke náhodne vybraných malých a stredných podnikoch v Slovenskej republike. Dotazník bol vytvorený podľa vzoru prieskumu stavu informačnej bezpečnosti v podnikovej sfére v SR, ktorý vykonal Národný bezpečnostný úrad SR, v spolupráci s časopisom DSM – data security management a spoločnosťou Ernst & Young v rokoch 2006 a 2008a Príručky na vykonávanie auditu informačných systémov. Prieskum formou momentkového pozorovania a náhodného výberu má v porovnaní s cieľným oslovením vopred vybranej skupiny

podnikov isté nedostatky, no objektivnosť výsledkov zvyšuje veľký počet podnikov a ich značná odvetvová rozmanitosť. V roku 2008 sa prieskumu zúčastnilo 247 podnikov, 2012 – 129 podnikov, 2015 – 209 podnikov a v roku 2017 – 219 podnikov. Podľa právnej formy mali najväčšie zastúpenie spoločnosti s ručením obmedzeným. Podľa štruktúry vlastníkov prevládali podniky s výlučne domácim vlastníkom, resp. prevažujúcim domácim vlastníkom.

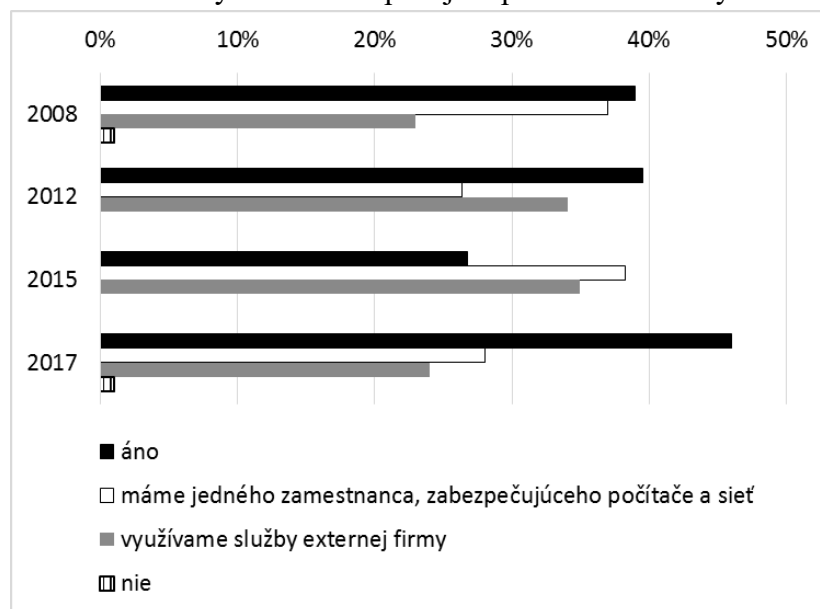
Personálne zabezpečenie v oblasti informačnej bezpečnosti

Kvalitné personálne zabezpečenie je jednou zo základných a nevyhnutných podmienok uplatňovania bezpečnostnej politiky IS v podniku, preto je nutné na tento faktor klásť obzvlášť dôraz. Konkrétne na definíciu, vytvorenie a personálne obsadenie rolí, ktoré v spoločnosti zabezpečujú kontinuálny rozvoj informačnej bezpečnosti v súlade s novými legislatívnymi prvkami, organizačnými zmenami resp. rozvojom spoločnosti, zmenami IS a v súlade so samotnou bezpečnostnou dokumentáciou (Matkovčíková, 2017).

Kľúčové role, ktoré v praxi predstavujú primárnu zložku každého systému riadenia informačnej bezpečnosti musia rešpektovať existujúce prvky riadenia v spoločnosti (napr. líniové resp. procesné riadenie, odborná spôsobilosť atď.). Vytvorenie týchto rolí nemusí nutne vyžadovať vytvorenie a obsadenie nového pracovného miesta, často krátko sa priraduje nová rola existujúcim pracovníkom. Je však dôležité, aby príslušné role zabezpečovali vymáhateľnosť pravidiel a zásad špecifikovaných v bezpečnostnej politike a ich praktickú aplikáciu a dodržiavanie (Koubek, 2015).

V rámci nášho prieskumu sme zisťovali, ako je oblasť informačných technológií a systémov začlenená do štruktúry organizácie a na akej hierarchickej úrovni je riešená informačná bezpečnosť. Niemenej podstatné sú aj očakávania, ktoré sú kladené na pracovníkov venujúcich sa IS/IT a informačnej bezpečnosti.

Graf 1: Má vaša firma samostatný útvar zabezpečujúci počítačové služby?



Zdroj: Vlastné spracovanie.

Útvar zabezpečujúci výhradne oblasť informačných technológií a systémov vo všeobecnosti, majú väčšinou stredné podniky, u malých je tento podiel malý. Väčšinou majú len osobu, ktorá je na pozícii tzv. správcu siete, ktorý sa stará o chod informačných systémov v podniku. Čo sa týka pracovníkov, ktorí sa výhradne venujú informačnej bezpečnosti ako hlavnej pracovnej náplni, sú zastúpení v necelých 10 % spoločností, prevažne stredných podnikov. Bežnou praxou je zlučovanie funkcie informačnej bezpečnosti s IS/IT oddelením. Podniky, ktoré nemajú takýto útvar alebo správcu, majú tieto služby zabezpečované externou firmou. Za samotnú bezpečnosť IS najmä u malých podnikov, ktoré využívajú externé IS/IT služby nezodpovedá nikto (žiadny útvar). Podniky, využívajúce správcu siete, prenášajú zvyčajne zodpovednosť na ekonomický a finančný útvar.

Prieskum odhalil aj fakt, že informačná bezpečnosť nie je integrovaná do biznis procesov spoločností. V prípade separátneho riešenia informačnej bezpečnosti a manažmentu rizík môže dochádzať k neadekvátnemu využitiu zdrojov firmy a nepokrytiu obchodných rizík, ktoré idú ruka v ruku s rizikami bezpečnosti na úrovni informačných systémov (PSIB SR, 2006).

Pri porovnávaní najviac cenených a naopak najviac chýbajúcich znalostí a schopností pracovníkov z oblasti zabezpečenia informačných systémov sme zistili výraznejší nedostatok znalostí a vedomostí pracovníkov z oblasti finančného riadenia podniku, čo však nepovažujeme za tak významný faktor v oblasti IS/IT. Horšie je to v oblasti technologických znalostí IS/IT a prezentačných a manažérskych schopností, ktoré patria medzi kľúčové znalosti pracovníkov IS/IT. Znalosti cudzích jazykov pracovníkov v oblasti informačnej bezpečnosti sa oproti predchádzajúcim obdobiam vylepšili, i keď ešte chýbajú v 23 % spoločností.



Zdroj: Vlastné spracovanie.

Ako najviac cenené znalosti a schopnosti určili respondenti prieskumu technologické znalosti IS/IT, vecnú znalosť problematiky informačnej bezpečnosti a flexibilitu a konštruktívny prístup k riešeniu problémov. Výraznejší prepád oproti minulému prieskumu zaznamenala schopnosť efektívnej komunikácie s vedením organizácie, čo pravdepodobne súvisí s narastajúcimi zručnosťami pracovníkov v tejto oblasti, nakoľko úmerne poklesol aj ich nedostatok.

Čo sa týka zastúpenia pracovníkov IS/IT v organizácii, 1/4 podnikov považuje existujúci stav za nepostačujúci. Výraznú fluktuáciu týchto pracovníkov zaznamenalo v priemere 10% podnikov. Zhoda medzi odbornosťou a požiadavkami je u 2/3 podnikov. Zvyšná 1/3 podnikov považuje znalosti a zručnosti za nepostačujúce, alebo len čiastočne zodpovedajúce požiadavkám.

Jedným z dôvodov tohto stavu môže byť aj finančné ohodnotenie týchto pracovníkov. Ohodnocovanie pracovníkov, ktorí sa v organizácii venujú problematike IS/IT kopíruje vývoj miezd na Slovensku. Z časového hľadiska je evidentný posun z nižších platových ohodnotení pracovníkov zodpovedných za informačnú bezpečnosť do vyšších. Nemôžeme však tvrdiť, že by dosahovali nadštandardnú úroveň, ako je to v iných vyspelých ekonomikách, čo vedie k neustálemu nedostatku tejto kvalifikovanej pracovnej sily, respektíve k jej fluktuácii. Príjmy nad 2000 € sme zaznamenali v odvetí Doprava a Obchod.

Tabuľka 1: Hrubé mesačné finančné ohodnotenie pracovníkov IS/IT

Mzda	2008	2012	2015	2017
do 500 €	42%	24%	16%	21%
501 – 1 000 €	37%	35%	34%	23%
1 001 – 1 500 €	11%	22%	31%	31%
1 501 – 2 000 €	6%	12%	14%	24%
nad 2000 €	4%	7%	5%	1%

Zdroj: Vlastné spracovanie

Bezpečnostná politika organizácie vo vzťahu k ľudským zdrojom

Pri hodnotení bezpečnostnej politiky organizácie vo vzťahu k „pasívnym užívateľom“ sme vybrali len základné kritériá, ktoré považujeme z hľadiska bezpečnosti IS/IT za východiskový predpoklad fungovania bezpečnostnej politiky tak v stredných, ako aj v malých podnikoch. Pri zamestnancoch z oblasti IS/IT, ktorí sa venujú problematike bezpečnosti, považujeme plnenie týchto hodnotiacich kritérií za samozrejmé.

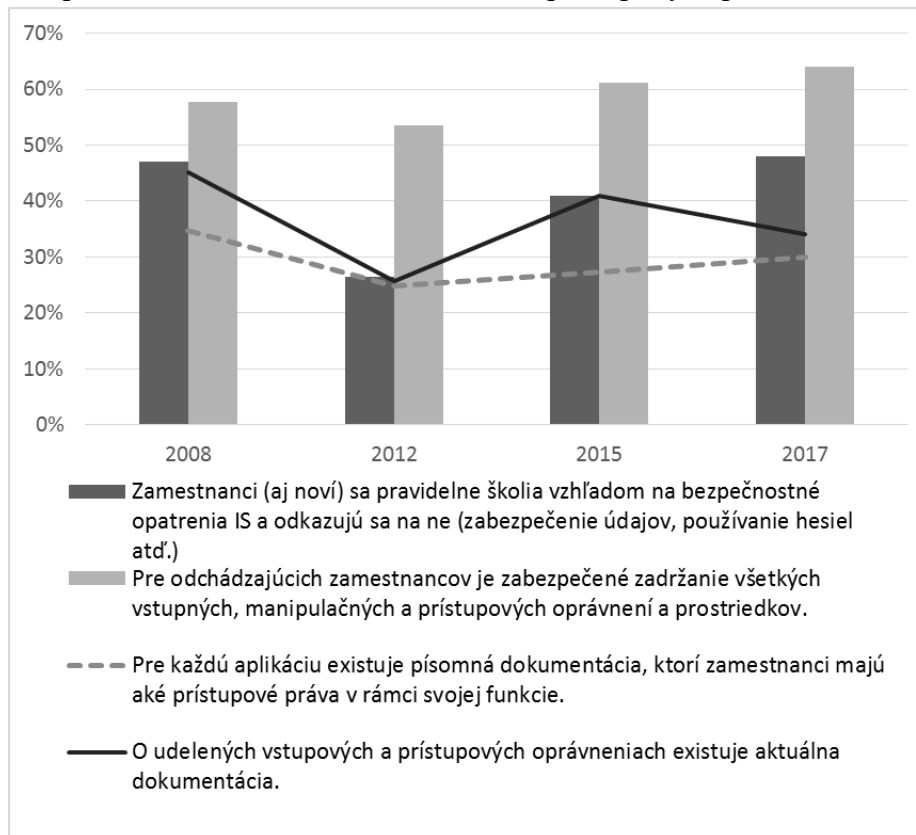
Prvým hodnotiacim kritériom sú školenia. Základnou úlohou školenia vo všeobecnosti je zvýšiť povedomie zamestnancov o možných rizikách a poučiť ich, ako týmto rizikám predchádzať, prípadne ako sa zachovať, keď daný stav/problém nastane. S ohľadom na bezpečnosť IS/IT hovoríme o pravidlách bezpečného používania HW a SW organizácie, o bezpečnej manipulácii s dátami v informačnom systéme, ich ochrane, politike hesiel a pod. Takéto školenie by mali zamestnanci absolvovať minimálne pri nástupe do zamestnania. Vhodné je však školenia bezpečnosti organizovať pravidelne, optimálny interval je jeden rok. Podľa nášho prieskumu (2017)

organizuje školenia o zabezpečení údajov a používaní hesiel 39% malých a 56% stredných podnikov.

V rámci bezpečnostnej politiky je potrebné riešiť aj odchádzajúcich zamestnancov, u ktorých je potrebné zadržať všetky vstupné, manipulačné a prístupové oprávnenia a prostriedky, resp. zmeniť prístupové heslá, ktoré mal zamestnanec k dispozícii. Ako môžeme vidieť na grafe. 3, pri odchádzajúcich pracovníkoch je percento podnikov, ktoré tak konajú, v priemere o 15% vyššie ako pri školeniach.

Čo sa týka vedenia písomnej dokumentácie o udelených vstupných a prístupových oprávneniach zamestnancov k jednotlivým aplikáciám, tu je naopak situácia horšia. Pri týchto výsledkoch stojí za zmienku fakt, že takmer vo všetkých sledovaných ukazovateľoch v oblasti bezpečnosti nastáva v roku 2012 pokles oproti roku 2008. Tento jav dávame do súvisu s vtedy prebiehajúcou hospodárskou krízou, kedy sa podniky snažili znížiť náklady a tendencia bola najmä znížiť náklady na bezpečnosť.

Graf 3: Bezpečnostné školenia a dokumentácia o prístupových právach a zabezpečení údajov



Zdroj: Vlastné spracovanie

Signifikantom prístupu organizácie a jej zamestnancov k informačnej bezpečnosti je prístupové heslo. Je to najjednoduchší, najlacnejší a najúčinnější bezpečnostný prvok zabráňujúci neoprávnene preniknúť do systému. Prax však ukazuje, že podniky neprikladajú tvorbe hesiel a definovaniu prístupových práv v rámci bezpečnostnej politiky takú vážnosť, ako by si táto problematika zaslúžila. Pravidlá tvorby hesiel sú vnútornou záležitosťou každej organizácie a

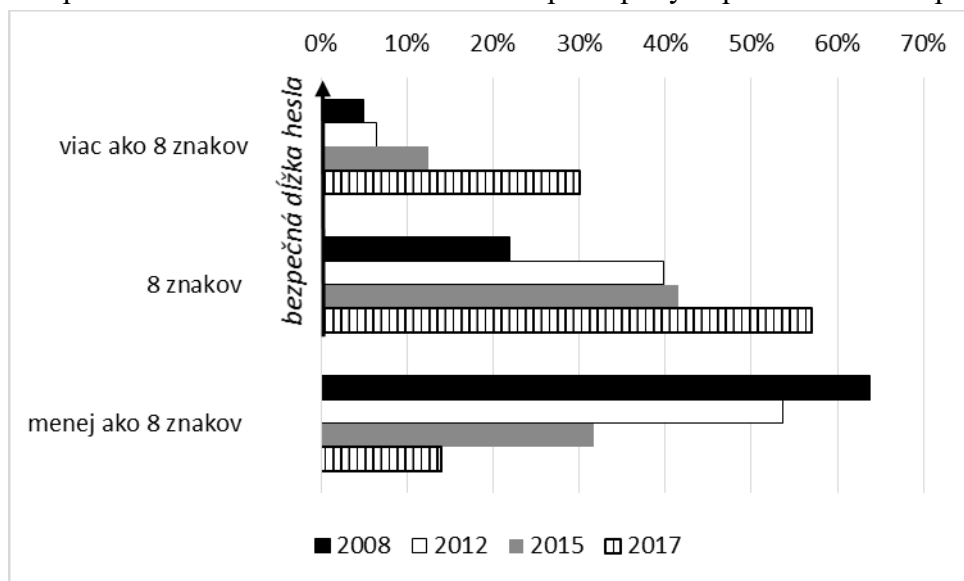
zásady, ktoré treba pri vytváraní silného a zapamätateľného hesla dodržiavať, by mala určovať interná smernica podniku. S jej obsahom by mali byť zamestnanci oboznámení minimálne pri ich nástupe do zamestnania. Častým javom býva, že zamestnanci majú v rámci aplikácií rovnaké prístupové práva alebo tieto prístupové práva nie sú písomne špecifikované v rámci ich funkcie. Preto sme sa problematike tvorby hesiel, ich forme a manipulácii s nimi osobitne venovali.

Z prieskumu vyplynulo, že viac ako 80% užívateľov má prístupové heslo. Potvrdilo sa nám však, že až polovica používa rovnaké prístupové heslo do viacerých aplikácií, takže hrozí, že pri odhalení jedného prístupového hesla môžu byť narušené dáta následne aj v ďalších programoch. Taktiež nie všetky aplikácie si vyžadujú zadanie vstupného hesla. Hlavným problémom pri tvorbe hesiel je, že nemajú dostatočný počet znakov a zloženie znakov, ktoré by zaručovalo neprelomenie hesla.

V roku 2008 sa najčastejšie sa používalo heslo s dĺžkou 5 až 6 znakov. Pozitívnym trendom je že, v roku 2017 už viac ako polovica užívateľov používala heslo s ôsmymi znakmi (graf 4). Podniková prax totiž ukázala, že bezpečnostným štandardom neprelomiteľného hesla vo všetkých podnikových aplikáciách je preddefinovaný formát hesiel pre serverové operačné systémy Windows firmy Microsoft, ktorý vyžaduje minimálne 8 znakov, 1 malé písmeno, 1 veľké písmeno a jedu číslicu. My sme zloženie hesla neskúmali, ale ako môžeme vidieť, už 30% podnikov používa heslo dlhšie ako 8 znakov. Podľa odborníkov na počítačovú bezpečnosť iba o 2 znaky dlhšie heslo vykompenzuje chýbajúce veľké písmená, čísla a náhodné znaky v hesle.

Bezpečné heslo by sa malo v pravidelných intervaloch meniť. Odporúčaným intervalom sú dva mesiace. Podniková prax však ukazuje, že toto bezpečnostné pravidlo organizácie nedodržiavajú. Až v dvoch tretinách nami oslovených podnikov nie sú heslá menené počas celého chodu systému a nie je zvyklosťou, že by sa pokusy o neoprávnený vstup a prekročenie oprávnenia monitorovali a protokolovali.

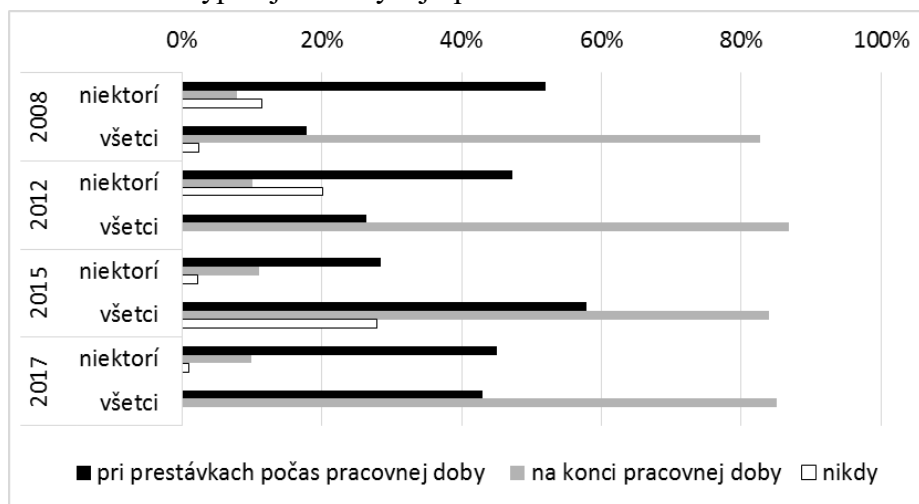
Graf 4: Bezpečnostné školenia a dokumentácia o prístupových právach a zabezpečení údajov



Zdroj: Vlastné spracovanie

Aj to najdokonalejšie heslo nemá význam, ak zamestnanci nevyužívajú funkciu, na ktorú bolo vytvorené. Zvykom totiž je, že pracovníci sa odhlasujú a vypínajú počítače až na konci pracovnej doby, a nerobia tak automaticky vždy, keď opúšťajú svoje pracovné miesto, napr. počas obedňajšej prestávky. V rokoch 2008 – 2015 sme sa stretli aj so skupinou pracovníkov, ktorí počítač nevypínali vôbec. Tento trend bol však klesajúci a v roku 2017 sa už nevyskytoval. Stále však zostáva veľká skupina pracovníkov, ktorí sa počas neprítomnosti na pracovnom mieste neodhlasujú, čím vytvárajú priaznivé podmienky pre únik a manipuláciu s informáciami vo vnútri organizácie. Podľa našich zistení zaznamenalo nepovolený prístup z vnútra až 65% organizácií.

Graf 5: Zamestnanci vypínajú/uzamykajú počítač



Zdroj: Vlastné spracovanie

Zhrnutie

Riziká informačnej bezpečnosti sú zapríčinené najrôznejšími hrozbami, ktoré pôsobia na zraniteľné miesta informačných a komunikačných systémov podnikov. V článku sme sa venovali jednému z nich – ľudskému faktoru. Konkrétne nás zaujímalo, ako podniky riešia kybernetickú bezpečnosť vo vzťahu k vlastným zamestnancom. Uskutočnený prieskum prináša viacero poznatkov a záverov pre oblasť manažmentu informačnej bezpečnosti so zameraním sa na ľudské zdroje. Vychádzajúc zo súčasného stavu poznania problematiky konštatujeme, že 41% podnikov vytvára len základnú štruktúru manažmentu informačnej bezpečnosti, čo sa odzrkadľuje aj na výbere zamestnancov v tejto oblasti a celkových nárokoch na bezpečnostné povedomie a správanie zamestnancov ako takých. 13% podnikov nevyvíja v tejto oblasti žiadne aktivity.

Ak podniky chcú dosiahnuť primeranú úroveň bezpečnosti svojich informačných aktív, potrebujú aktivizovať a efektívne prepojiť všetky procesy manažmentu, riadenie ľudských zdrojov nevynímajúc. Aby organizácia spĺňala nové nároky, musí zmeniť najmä základné ponímanie svojho fungovania. Organizačná štruktúra sa musí prestať brať ako základ, ako pevne definované rozdelenie činností, vzťahov a právomocí, z čoho vyplývajú doterajšie zodpovednosti a odmeňovanie. Zamestnanci informačnej bezpečnosti sa musia pevne začleniť do štruktúry, ich

funkcie nemôžu byť kumulované alebo nahrádzané inou pracovnou pozíciou. Ich rozhodovacie právomoci je potrebné rozšíriť a primerane tomu zvýšiť ich finančné ohodnotenie.

Čo sa týka zamestnancov všeobecne, ako aj pri ostatných manažérskych disciplínach, nie je ani pri riadení ľudí a formovaní bezpečnostného povedomia jednoduché zostaviť univerzálny návod, podľa ktorého sa má postupovať, aby bol zaručený úspech. Je to ovplyvnené mnohými faktormi, ako je veľkosť podniku, zameranie, štruktúra zamestnancov a iné. My sme vybrali, podľa nášho názoru, základné aspekty a zásady, ktoré by mali dodržiavať všetky typy organizácií. Ako môžeme vidieť z výsledkov, podniky majú ešte výrazné pri efektívnom uplatňovaní bezpečnostnej politiky vo vzťahu k zamestnancom.

Pokiaľ je nám známe, prieskum informačnej bezpečnosti v malých a stredných podnikoch Slovenska nerealizovala v takomto rozsahu a s takýmto zameraním žiadna iná organizácia a nemáme vedomosť o tom, že by podobný prieskum prebiehal v niektorej inej krajine. Preto nemáme možnosť nami dosiahnuté výsledky porovnať s iným obdobným prieskumom. Dosiahnuté výsledky nepredstavujú ukončenie výskumnej činnosti v oblasti manažmentu informačnej bezpečnosti, ale poskytujú ďalšie poznatky na rozpracovanie tejto témy a následné vyhodnotenie v nasledujúcich obdobiach.

Kapitola bola spracovaná v rámci grantu VEGA 1/0309/18.

1.2 Kybernetická bezpečnosť údajov o bezpečnosti a ochrane zdravia pri práci zamestnancov v malých a stredných podnikoch

Od apríla roku 2018 má Slovenská republika v platnosti nový zákon o kybernetickej bezpečnosti, ktorý do praxe priniesol niekoľko kľúčových zmien a nových povinností. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NBÚ, 2018). Ešte donedávna bola celá táto oblasť neregulovaná. Cieľom tejto regulácie je zvýšenie koordinácie medzi členskými štátmi EÚ a zvýšenie bezpečnosti v kybernetickom priestore.

V podnikovej praxi sa z predmetného zákona zavedené povinnosti v súčasnosti týkajú napríklad poskytovateľov služieb v oblastiach bankovníctva, dopravy, energetiky, farmaceutického, hutníckeho a chemického priemyslu a zdravotníctva. V budúcnosti by sa tieto povinnosti mohli uplatňovať napríklad aj v automobilovom priemysle, ktorý čelí čoraz väčším kybernetickým rizikám (Schweizer, 2018).

V rámci Slovenskej republiky, východiskovým strategickým dokumentom je Národná stratégia kybernetickej bezpečnosti, ktorá komplexne určuje strategický prístup Slovenska k zabezpečeniu kybernetickej bezpečnosti. Národnú stratégiu kybernetickej bezpečnosti pripravuje Národný bezpečnostný úrad v spolupráci s ostatnými zodpovednými ústrednými orgánmi. Aktuálne strategické dokumenty pre oblasť kybernetickej bezpečnosti tvoria Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a Akčný plán realizácie zmieňovanej Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020 (NBÚ, 2018).

Z dôvodu predchádzania spomínaných kybernetických rizík a hrozieb súčasnosti, podľa Národného bezpečnostného úradu (2018) jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie takýchto kybernetických bezpečnostných incidentov, ktorý zaisťuje systematické získavanie, sústredovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch a taktiež centrálny systém včasného varovania, ktorý zaisťuje včasnú výmenu informácií o hrozbách, kybernetických bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a subjektom, ktoré majú prístup k neverejnej časti jednotného informačného systému. Subjekty, ktoré sú zo zákona (§ 19 a § 22) povinné poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti ich musia poskytovať bezodplatne a bezodkladne po tom, ako sa dozvedia o skutočnosti zakladajúcej túto povinnosť.

Do dvoch rokov od účinnosti vyššie uvedeného zákona, t.j. do 1. apríla roku 2020, majú prevádzkovatelia základnej služby i povinnosť prijať a dodržiavať všeobecné bezpečnostné opatrenia. A to najmenej v rozsahu bezpečnostných opatrení zákona a ak sú prijaté, tak aj sektorové bezpečnostné opatrenia. Bezpečnostné opatrenia sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej

bezpečnosti počas životného cyklu sietí a informačných systémov. Cieľom bezpečnostných opatrení je predchádzať kybernetickým bezpečnostným incidentom a minimalizovať ich vplyv na kontinuitu prevádzkovania služby. Zároveň sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie (Slov-Lex, 2018).

Na prijatie týchto opatrení musia ale dotknuté subjekty automaticky naviazať aktualizáciu bezpečnostnej dokumentácie. Ďalšia veľmi dôležitá povinnosť sa viaže na situáciu, keď prevádzkovateľ základnej služby nebude v pozícii reálneho prevádzkovateľa sietí a informačných systémov, od ktorých ale bude poskytovanie jeho služby závislé. Pôjde teda o prípad, keď v tomto postavení bude vystupovať externá firma. S touto treťou stranou musí prevádzkovateľ základnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Prakticky len outsourcuje povinnosti vyplývajúce zo zákona (Schweizer, 2018).

Je dôležité vymedziť si oblasti pre prijatie bezpečnostných opatrení. Sú nimi organizácie informačnej bezpečnosti, riadenia aktív, hrozieb a rizík, personálnej bezpečnosti, riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, technických zraniteľností systémov a zariadení, riadenia bezpečnosti sietí a informačných systémov, riadenia prevádzky, riadenia prístupov, kryptografických opatrení, riešenia kybernetických bezpečnostných incidentov, monitorovania, testovania bezpečnosti a bezpečnostných auditov, fyzickej bezpečnosti a bezpečnosti prostredia, či riadenia kontinuity procesov (Slov-Lex, 2018).

Podľa Schweizer (2018) by týmto zo zákona uvedeným povinnosťami mali podniky resp. prevádzkovatelia základných služieb venovať náležitú pozornosť a to aj z dôvodu pokuty, ktorá môže dosiahnuť výšku 300 000 eur pri porušení ustanovení vyššie spomenutého zákona.

Kybernetická a informačná bezpečnosť údajov o bezpečnosti a ochrane zdravia pri práci zamestnancov v malých a stredných podnikoch

Kybernetická a informačná bezpečnosť je aktuálnou súčasťou bezpečnostnej kultúry jednotlivých podnikov. Malé a stredné podniky spracúvajú najrôznejšie údaje o svojich zamestnancoch. Dôvodom spracúvania týchto informácií a osobných údajov je plnenie povinností zamestnávateľa vyplývajúce z uzatvorenia pracovnej zmluvy a osobitných zákonov. Počas trvania pracovného pomeru tak malé a stredné podniky ako zamestnávatelia spracúvajú osobné údaje svojich zamestnancov na základe toho, že spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, teda zamestnanec (čl. 6 bod 1 písm. b/ GDPR), alebo je spracúvanie osobných údajov nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa, teda zamestnávateľa – daného podniku (čl. 6 bod 1 písm. c/ GDPR).

Dôležitou oblasťou, ktorú často malé a stredné podniky podceňujú je spracúvanie osobných údajov po skončení pracovného pomeru zamestnanca. Zamestnanec už síce pre podnik nepracuje, ten však naďalej archivuje jeho osobné údaje a informácie, ktoré získal počas trvania pracovného pomeru. Podnik ako zamestnávateľ si musí byť vedomý, že takýto postup môže byť v rozpore s GDPR a novým zákonom o ochrane osobných údajov, v dôsledku čoho mu môžu hroziť nemalé pokuty. Pokiaľ zanikli všetky účely pre spracúvanie osobných údajov bývalého zamestnanca,

zamestnávateľ ich musí po skončení pracovného pomeru bezodkladne vymazať. Vymazanie osobných údajov znamená, že zamestnávateľ musí nielen fyzicky zlikvidovať všetky papierové dokumenty obsahujúce osobné údaje, ale tiež vymazať osobné údaje vedené elektronicky zo všetkých elektronických systémov vrátane záloh. Výmaz osobných údajov je tiež potrebné realizovať bez možnosti ich obnovenia (Pohorelá, 2019).

Pre malé a stredné podniky je aj z tohto dôvodu obzvlášť významné nielenže zaviesť, ale aj riadiť kybernetickú a informačnú bezpečnosť. Do bezpečnostnej kultúry podniku patria rôzne oblasti. Jednotlivé zložky bezpečnostnej kultúry podniku nefungujú oddelene, ale sú navzájom úzko prepojené. Do bezpečnostnej kultúry patrí napríklad aj ochrana know-how, či dobrého mena zamestnávateľa resp. podniku. Avšak významnou oblasťou, ktorá patrí do bezpečnostnej kultúry malých a stredných podnikov je aj oblasť bezpečnosti a ochrany zdravia zamestnancov pri práci¹. Táto oblasť zahŕňa napríklad požiaru bezpečnosť, fyzickú bezpečnosť, ale aj kybernetickú a informačnú bezpečnosť, kam patrí ochrana osobných údajov vrátane evidencie a archivácie pracovných úrazov a chorôb z povolania zamestnancov, ktorých podnik zamestnáva (Špindl, 2018).

Podnik ako zamestnávateľ je povinný v rámci BOZP viesť evidenciu pracovných úrazov (v minulosti to bola kniha drobných úrazov). Evidencia pracovných úrazov (pozri bližšie: Szarková a kol., 2013) musí podľa zákona o BOZP (§ 17, odsek 8, písm. a) obsahovať všetky údaje, ktoré sú potrebné na spísanie registrovaného pracovného úrazu v prípade, že by sa následky úrazu prejavili neskôr. Sú to napríklad údaje ako: Poradové číslo; Meno a priezvisko poraneného; Dátum a čas úrazu; Miesto udalosti; Pracovná neschopnosť - počet dní; Meno, priezvisko a podpis vedúceho zamestnanca, ktorý vykonal zápis; Popis poranenia; Prijaté a vykonané opatrenia; Svedok. Predpísaný záznam o registrovanom pracovnom úraze zamestnávateľ vypisuje len pri registrovanom pracovnom úraze a povinnosť uchovávať záznam trvá desať rokov od vzniku úrazu. Rovnaká lehota platí aj pre uchovávanie evidencie pracovných úrazov. Aby zamestnávateľ mohol vyplniť záznam o registrovanom pracovnom úraze, musí mať k dispozícii niektoré osobné údaje zamestnanca. Zákon o BOZP však neupravuje spracúvanie osobných údajov bez súhlasu dotknutej osoby. Tieto údaje musí zamestnávateľ spracúvať v súlade so zákonom č. 428/2002 Z. z. o ochrane osobných údajov (je potrebné, aby mal zamestnávateľ písomný súhlas zamestnanca na spracúvanie jeho osobných údajov).

Dôvodom, prečo je kybernetická a informačná bezpečnosť v podniku tak dôležitá je aj to, že informácie o podnikoch a ich zamestnancoch tvoria cenný zdroj intelektuálneho kapitálu malých a stredných podnikov. Mnohé z osobných údajov a informácií v oblasti bezpečnosti a ochrany zdravia pri práci - napríklad informácie o dodržiavaní bezpečnostných princípov a noriem v pracovnom procese, evidencia a archivácia pracovných úrazov a chorôb z povolania

¹ Pozn. BOZP - Bezpečnosť a ochrana zdravia pri práci je vymedzený ako stav pracoviska (pracovných podmienok, pracovného prostredia) resp. pracovného procesu, ktorý poskytuje vysokú mieru istoty, že pri dodržaní bezpečnostných požiadaviek (predpisov, pravidiel, pokynov, technologických a pracovných postupov a pod.) platných pre príslušné pracovisko, resp. pracovný proces a bez pôsobenia nepredvídateľných vonkajších vplyvov bude možnosť ohrozenia života a zdravia osôb, poškodenia alebo zničenia hospodárskych hodnôt znížená na akceptovateľnú úroveň (Hatina a kol., 2006).

zamestnancov v podniku sú v súčasnosti sprostredkúvané pomocou e-komunikačných nástrojov a sú uložené v elektronických databázach podnikov. Práve to však so sebou nesie aj rôzne typy hrozieb a rizík nakoľko podľa Špindla (2018) je kybernetický priestor nebezpečný a môže priamo ohroziť samotný chod podniku.

Zabezpečenie jednotlivých podnikov v kontexte kybernetickej bezpečnosti má vplyv aj na samotnú spokojnosť zamestnancov (Krásna, 2015) keďže súvisí so systémom starostlivosti o zamestnancov. Štatistický prieskum spoločnosti Ponemon Insitute (In Schweizer, 2018) so vzorkou 3 000 IT odborníkov poukázal na to, že 47 % svetových finančných inštitúcií, ktoré utrpeli prienik do svojich systémov, nemali nainštalované aktualizácie, aj keď boli už v tom čase dostupné. Pritom až 37 % týchto inštitúcií vedelo, že sú zraniteľní.

Jeden z významných krokov v riadení kybernetickej bezpečnosti malých a stredných podnikov je analýza samotných rizík. Analýzu rizík je nutné realizovať hneď na začiatku. V podnikoch môže totiž nastať strata, poškodenie, zničenie, alebo i krádež údajov a informácií. Straty z kybernetických útokov dosahujú priam galaktické hodnoty. Trend je taký, že počet útokov rastie a ich riziko sa stále zvyšuje. Ak k takejto situácii vo firme dôjde, je dôležité čo najviac dôsledne a presne určiť a vyčíslieť hodnotu údajov (Špindl, 2018). Pokiaľ podnik nedisponuje dostatočnými internými kapacitami a know-how na riešenie technicko-právnych rizík odporúča sa podnikom obrátiť na skúsených poradcov, právnikov spôsobilých v oblasti kybernetickej a informačnej bezpečnosti.

Zhrnutie

V súčasnosti sa veľká časť obchodu malých a stredných podnikov presunula do online priestoru. Zvyšovanie úrovne kybernetickej bezpečnosti je preto jednou z aktuálnych výziev podnikov, ktorej tempo musí byť úmerné tomuto trendu. Nový zákon v oblasti kybernetickej bezpečnosti vyzýva malé a stredné podniky na zavedenie množstva nových opatrení, ktoré musia mať v praxi pevné miesto a pravidelný režim. Jednou z oblastí, ktoré patria do bezpečnostnej kultúry podniku patrí oblasť bezpečnosti a ochrany zdravia zamestnancov pri práci. Mnohé z osobných údajov a informácií v oblasti bezpečnosti a ochrany zdravia pri práci - informácie o dodržiavaní bezpečnostných princípov a noriem v pracovnom procese, evidencia a archivácia pracovných úrazov a chorôb z povolania zamestnancov v podniku sú v súčasnosti sprostredkúvané pomocou e-komunikačných nástrojov a sú uložené v elektronických databázach podnikov. Tieto informácie a dáta obsahujú osobné údaje zamestnancov a tvoria cenný zdroj a súčasť intelektuálneho kapitálu malých a stredných podnikov. Z tohto dôvodu je v súčasnosti podstatné venovať čoraz väčšiu pozornosť a opatrnosť ich kybernetickej a informačnej bezpečnosti. V podnikoch môže dôjsť k strate, poškodeniu, zničeniu, alebo krádeži osobných údajov a informácií a preto v dôsledku ich nedostatočného zabezpečenia môže byť ohrozený celý chod podniku. Pre malé a stredné podniky akéhokoľvek oboru je preto v súčasnosti nesmierne dôležité nielen zaviesť, ale aj riadiť kybernetickú a informačnú bezpečnosť a to nielen v oblasti BOZP. Vypracovať a klasifikovať jednotlivé informácie, určiť ich zraniteľnosti, hrozby a z toho plynúce riziká,

navrhnuť a implementovať organizačné a technické opatrenia a neustále vyhodnocovať, či vzdelávať v tejto oblasti. V neposlednom rade je tiež významné nezabudnúť na previazanosť s GDPR a elektronickou identitou.

Kapitola je výsledkom projektu VEGA č.1/0309/18.

1.3 Ochrana osobných údajov v kontexte judikatúry Súdneho dvora EÚ

Svetová ekonomika sa stáva stále viac integrovanou a vzájomne prepojenou prostredníctvom obchodu. (Milošovičová et al., 2015). Tomuto procesu napomáha aj formovanie digitálneho trhu v rámci Európskej únie, ktorý patrí medzi priority ustanovené v Stratégii Európa 2020 (Stratégia Európa 2020). Digitálne technológie sa stali prostriedkom podporujúce rozvoj nielen hospodárskych vzťahov, investičných vzťahov, ekonomiky digitálnych služieb, ale aj sociálnych a kultúrnych vzťahov. Obdobie, v ktorom žijeme, je obdobím dynamického vývoja vedecko-technického pokroku, rozvoja telekomunikačných technológií, ktorý neustále napreduje. V rámci tohto procesu sú spracovávané na rôznych úrovniach aj osobné údaje, pričom je potrebné klásť dôraz aj na ich bezpečnosť a ochranu. Prierezovo sa problematika ochrany údajov týka viacerých oblastí a to bezpečnostnej politiky a práva, ako aj hospodárstva, sektora komunikácie, vzdelávania a zdravotníctva, verejnej správy alebo ochrany spotrebiteľov a práva na súkromie. (Ú .v, EÚ C 391/2012). Právo na ochranu osobných údajov nie je absolútne právo, musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami. (Recitál 4 nariadenie EÚ 2016/679). Ochrana osobných údajov úzko spolu súvisí s právom na súkromie, ktoré je chápané ako jedno z najuniverzálnejších práv z osobnostných práv, pretože v dôsledku zásahu do súkromia človeka dochádza zároveň aj k postihnutiu jeho ďalších osobnostných práv (Mates, 2002). Z hľadiska zaradenia a formovania práva na súkromie patrí toto právo do prvej generácie ľudských práv a slobôd, čiže medzi práva osobnostné a politické. Vedecká štúdia v prvej časti obsahuje právny rámec ochrany osobných údajov. V druhej časti sa autorky zamerali na objasnenie kompetencií Súdneho dvora Európskej únie a na analýzu sporov riešených Súdnyim dvorom Európskej únie. V záverečnej časti sú syntetizované poznatky a vzťahy majúce zásadný význam z hľadiska ochrany osobných údajov fyzických osôb pre právnu prax a pre občanov. Vedecká štúdia má teoretický charakter a je založená na sekundárnom výskume. Pri spracovaní danej témy sme použili deskriptívno-analytickú metódu. Použili sme aj analýzu káuz na vysvetľovanie súvislostí, javov a vzťahov týkajúce sa ochrany osobných údajov. Informácie k získaniu prehľadu o súčasnom stave problematiky boli čerpané hlavne zo slovenskej právnej úpravy, z právnej úpravy Európskej únie, z vedeckej literatúry, z faktografických údajov riešených sporov na Súdnom dvore Európskej únie a z internetových zdrojov.

Právny rámec ochrany osobných údajov

Základným medzinárodným právnym rámcom ochrany osobných údajov je článok 8 ods. 1 Charty základných práv Európskej únie a článok 16 ods. 1 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“). Uvedené ustanovenia primárnej právnej úpravy Európskej únie explicitne ustanovujú, že: „každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.“ Obsahom tohto priznaného práva na úrovni Európskej únie je, že ochrana dát fyzických osôb sa vzťahuje na spracúvanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. V danej

súvislosti považujeme za vhodné zdôrazniť, že osobné údaje sa dotýkajú výhradne fyzickej osoby, jednotlivca, človeka. Dané základné právo je aj úzko spojené s právom na rešpektovanie súkromného a rodinného života, zakotveným v článku 7 Charty základných práv Európskej únie. Osobné údaje sú vstupnou bránou do súkromia každého človeka. *Sféra súkromia je však omnoho širšia a možno ju definovať ako určitý ohraničený priestor každého človeka, za ktorý nesmie nikto zasahovať bez súhlasu danej osoby alebo bez oprávnenia stanoveným zákonom.* (Mates, 2002). Ustanovenie článku 16 ods. 2 ZFEÚ splnomocňuje Európsky parlament a Radu, aby prijali opatrenia týkajúce sa ochrany fyzických osôb pri spracúvaní osobných údajov a pravidiel týkajúce sa voľného pohybu osobných údajov. Za týmto účelom boli prijaté sekundárne akty (nariadenia a smernice), ktoré tvoria nový modernizovaný právny rámec ochrany osobných údajov so zreteľom na zabezpečenie rešpektovania základných práv a slobôd. V rámci spracúvania osobných údajov inštitúciami a orgánmi EÚ je ich ochrana zabezpečená prostredníctvom nariadenia Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001). Na základe uvedeného nariadenia bol v roku 2004 vytvorený Európsky dozorný úradník na ochranu údajov. Neskôr bolo prijaté nariadenie Európskeho parlamentu a Rady (EÚ) č. 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. (Ú. v. EÚ L 119, 4.5.2016) *Uvedený právny predpis ustanovuje pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a pravidlá týkajúce sa voľného pohybu osobných údajov.* Vzhľadom na právnu povahu nariadenia, predmetné nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch (článok 99). Súčasne s týmto nariadením bola prijatá aj smernica Európskeho parlamentu a Rady (EÚ) č. 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. (Ú. v. EÚ L 119, 4.5.2016). Na Slovensku bola smernica transponovaná do nového zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Vychádzajúc z §1 zákona o ochrane osobných údajov, právna úprava sa vzťahuje na osobné údaje **systematicky spracúvané úplne alebo čiastočne automatizovanými prostriedkami** spracúvania alebo inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme. Zákon o ochrane osobných údajov ustanovuje ochranu práv fyzických osôb, práva, povinnosti a zodpovednosť subjektov pri spracúvaní osobných údajov a postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky. Aj ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov upravuje ochranu osobných údajov. Konkrétne ide o ustanovenie článku 22 odsek 1, ktorý garantuje ochranu osobných údajov slovami „listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú.“ Subjektom takejto ústavnej ochrany je každý (Peráček, Mucha, Kočišová, 2017). V praxi to znamená, že takúto ochranu požíva ktorákoľvek fyzická osoba alebo právnická osoba bez ohľadu na štátnu príslušnosť alebo sídlo. Podľa odbornej literatúry (Gregušová et al., 2016)

však ide o duplicitné ustanovenie k článku 19 odsek 3 Ústavy Slovenskej republiky, ktoré každému zabezpečuje právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

Pôsobnosť Súdneho dvora Európskej únie

V rámci inštitucionálneho systému Európskej únie v zmysle článku 13 Zmluvy o Európskej únii významné miesto patrí Súdnu dvoru Európskej únie (Luxemburg). „*Súdny dvor EÚ zaručuje, aby právo Európskej únie dodržiavali členské štáty a orgány a inštitúcie Európskej únie, a zaručuje, aby sa právo Európskej únie dodržiavalo pri výklade a uplatňovaní zmlúv zakladajúcich Európsku úniu a právnych noriem prijatých orgánmi Európskej únie.*“ (Bérešová, 2013). Jeho právomoci sú vymedzené v článku 19 a v článku 40 Zmluvy o Európskej únii (Ú. v. EÚ C 83, 30.3.2010), v článkoch 251 až 281 ZFEÚ (Ú. v. EÚ C 83, 30.3.2010) a v článku 136 Zmluvy o založení Európskeho spoločenstva pre atómovú energiu. Svojou činnosťou *de facto* prispieva k precedenčnému systému práva. Slovenské významné osobnosti, Mazák a Klučka (2004) uvádzajú, že: „*rozsudky Súdneho dvora sú záväzné pre súdy všetkých členských štátov a hoci Súdny dvor svoju právnu silu odvodzuje z primárneho práva (čo by zodpovedalo skôr sekundárnej povahe jeho rozhodnutí), na druhej strane sa jeho rozhodnutiami rozvíja a dotvára aj primárne právo.*“ Rozhodnutia európskych súdov patria k prameňom práva Európskej únie. V zmysle článku 19 ods. 3 písm. b) Zmluvy o Európskej únii a článku 267 Zmluvy o fungovaní Európskej únie Súdny dvor Európskej únie má právomoc vydať prejudiciálne rozhodnutie o výklade práva Európskej únie a o platnosti aktov prijatých inštitúciami, orgánmi, úradmi alebo agentúrami Únie. V tejto súvislosti môžeme hovoriť aj o priamej forme spolupráce národných súdnych orgánov so Súdny dvorom Európskej únie, pričom iba súd členského štátu je oprávnený klásť otázky a určiť ich obsah.

Súdnu dvoru EÚ prináleží právomoc podľa ustanovenia článku 263 ZFEÚ preskúmať zákonnosť legislatívnych aktov, aktov Rady, Komisie a Európskej centrálnej banky okrem odporúčaní a stanovísk a preskúmať aj zákonnosť aktov Európskeho parlamentu a Európskej rady, ktoré majú právne účinky vo vzťahu k tretím stranám. V zmysle článku 17 Zmluvy o Európskej únii Európska komisia je označovaná ako „*strážkyňa zmlúv Európskej únie*“. Jej úlohou je monitorovať uplatňovanie primárneho a sekundárneho práva EÚ a zabezpečovať jeho jednotné uplatňovanie vo všetkých členských štátoch EÚ. Ustanovenie článku 258 ZFEÚ ju oprávňuje predložiť vec na Súdny dvor Európskej únie, ak si členský štát nesplní povinnosti, ktoré mu vyplývajú z práva Európskej únie. Súdny dvor EÚ podľa článku 265 ZFEÚ rozhoduje aj spory o nečinnosti niektorých inštitúcií EÚ. Rozhodnutia a nálezy sú zverejňované v plnom znení na internetovej stránke tejto súdnej inštitúcie.

Spomedzi rozhodnutí Súdneho dvora Európskej únie týkajúcich sa ochrany osobných údajov je potrebné upozorniť na rozhodnutie v právnej veci C-362/14 M. Schrems. Maximillian Schrems, občan Rakúskej republiky patrili k používateľom sociálnej siete Facebooku od roku 2008 spustenej Markom Zuckerbergom. Tak ako dáta všetkých používateľov Facebooku žijúcich na území členských štátov EÚ, aj dáta poskytnuté pánom Schremsom spoločnosti Facebook boli prenášané sčasti alebo v celom rozsahu z írskej dcérskej spoločnosti Facebook na servery, ktoré sa

nachádzajú na území Spojených štátov amerických, kde sú spracovávané. Pán Schrems túto skutočnosť nepovažoval za správnu a začal iniciovať opatrenia, aby bola spochybnená legitimita prenosu dát na územie iného štátu. V predmetnej veci Súdny dvor Európskej únie rozhodol, že: „*právna úprava, ktorá neupravuje nijakú možnosť osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov, zasahuje **podstatu obsahu základného práva na účinnú súdnu ochranu**, pričom takáto možnosť je súčasťou existencie **právneho štátu**.*“ (Tlačové komuniké č. 117/15). Dané rozhodnutie malo zásadný vplyv na prijatie nového opatrenia na úrovni Európskej únie za účelom zabezpečenia prenosu dát európskych používateľov Facebooku do Spojených štátov amerických, pretože nevhodným spôsobom zabezpečovali úroveň ochrany osobných údajov. (Bezpečný prístav).

Pre našu hlbšiu analýzu sme vybrali dva rozsudky. Uvedené rozhodnutia sú zverejňované a dostupné na internetovej stránke Súdneho dvora Európskej únie. (curia.europa.eu.juris).

V právnej veci C-582/14 Patrick Breyer v. Spolková republika Nemecko v rámci prejudiciálneho konania sa Súdny dvor EÚ zaoberal zapisovaním a uchovávaním adresy internetového protokolu - „IP adresy“ pána Breyera, ktorý prehliadal viaceré internetové stránky nemeckých spolkových orgánov. Nemecké národné authority v súčasnosti sú oprávnené zaznamenávať a uchovávať dátum, čas prehliadania, aj IP adresy osôb, ktoré stránky prehliadajú. S cieľom národnej bezpečnosti oprávnené národné authority zaznamenávajú určité dáta ohľadom prehliadania internetových stránok nemeckých spolkových orgánov osobami. P. Breyer sa domáhal spravodlivosti na nemeckých súdoch v domnienke, že bolo porušené právo na ochranu jeho osobných údajov. Nemecký Spolkový súdny dvor (Bundesgerichtshof) využil právo prejudiciálneho konania a požiadal Súdny dvor EÚ o objasnenie (výklad), či „dynamické“ IP adresy predstavujú pre daného prevádzkovateľa internetovej stránky osobné údaje, a či sa na takéto údaje uplatňuje inštitút ochrany osobných údajov. Podľa bodu 15 rozhodnutia v právnej veci C-582/14 IP „*adresy tvoria číslce, ktoré boli pridelené počítačom pripojeným do internetu, aby bola umožnená ich komunikácia v ich sieti. Pri prehliadaní si internetovej stránky je IP adresa vyvolávajúceho počítača sprostredkovaná serveru, na ktorom je prehliadaná stránka uložená. Táto komunikácia je nevyhnutná na to, aby bolo možné preniesť prehliadané údaje správne adresátovi.*“ V danej súvislosti sa rozlišujú „statické“ IP adresy, alebo „dynamické“ IP adresy (adresy sa menia pri každom novom pripojení na internet). Tak ako je uvedené v bode 16 rozhodnutia C-582/14 dynamické IP adresy neumožňujú vytvoriť spojenie na základe verejne prístupných súborov medzi určitým počítačom a fyzickým pripojením do siete používanej poskytovateľom internetového prístupu. (Tieto definície uvádzame v pôvodnom znení).

Vtedajšia právna úprava, t. j. smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov v ustanovení článku 2 písm. a) uvádza, že: „*osobné údaje znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby ("údajového subjektu"); identifikovateľná osoba je osoba, ktorú možno identifikovať, priamo alebo nepriamo, najmä pomocou overenia identifikačného čísla alebo jedného alebo viacerých faktorov špecifických pre jeho fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu.*“ Podľa Maštalku (2008) „*požiadavku na určenosť/identifikovanosť konkrétnej osoby je možné interpretovať aj ako potrebu a nevyhnutnosť odlišenia príslušnej osoby od iných osôb. Odlišiť túto osobu je možné na základe viacerých faktorov. K naplneniu identifikovanosti však dôjde až vtedy, keď sú tieto faktory také jednoznačné, že sa táto osoba na základe nich stáva aj*

vyhladateľná. Na základe toho musíme byť schopní túto osobu poznať a kontaktovať, a to po celú dobu držania tejto informácie/osobného údaju o danej osobe“. V kontexte širších súvislostí musíme poukázať na skutočnosť, že smernica bola zrušená a nahradená už spomínaným nariadením (EÚ) 2016/679. Napokon Súdny dvor EÚ vo svojom rozhodnutí zo dňa 18. októbra 2016 konštatoval, že: „dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prehliadaním si určitou osobou internetovej stránky, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle ustanovenia 2 písm. a) smernice 95/46, ak má k dispozícii právne prostriedky, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby.“ Z uvedeného vyplýva, že IP adresa patrí medzi identifikátory fyzickej osoby. Fyzickú osobu je možné identifikovať na základe jedného alebo viacerých dostupných údajov o danej osobe, čím sa odlišuje od iných osôb v danom informačnom systéme, kde sa osobné údaje spracúvajú. Aj keď definícia pojmu osobný údaj je pomerne široká, je potrebné brať do úvahy charakteristiky alebo znaky určujúce fyzickú osobu, podľa ktorých je možné identifikovať fyzickú osobu (fyzická, fyziologická, psychická, mentálna, ekonomická, kultúrna, sociálna identita). Miera, do akej sú identifikátory v danom prípade postačujúce na identifikovanie konkrétnej fyzickej osoby, závisí od posúdenia dostupných údajov v ich vzájomnej súvislosti a zároveň aj situácie ako celku. (Metodické usmernenie 1/2013). V našom prípade je možné podľa IP adresy identifikovať fyzickú osobu, ktorá navštívila internetovú stránku. Pomerne vhodnú a jednoduchú definíciu pojmu osobný údaj uvádza Mates (2002) vo svojom diele s názvom „Ochrana osobných údajov“. Mates definuje osobný údaj „ako každý údaj, ktorý má určitý vzťah k fyzickej osobe a na jeho základe je možné túto osobu identifikovať.“ Váľková et. al. (2013) tvrdia, že „pojem osobný údaj môžeme subsumovať akýkoľvek druh údajov a charakteristik, ktoré je možné priradiť ku konkrétnej fyzickej osobe. Má relatívnu povahu, pretože to, či ide o osobný údaj, závisí od komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti a zároveň od celkovej situácie.“

Následne sa Súdny dvor EÚ zaoberal aj otázkou, či členský štát môže mať takú právnu úpravu, podľa ktorej môže poskytovateľ online mediálnych služieb zhromažďovať a používať osobné údaje týkajúce sa návštevníka bez jeho súhlasu. Nemecká platná právna úprava ustanovuje, že účel zabezpečenia celkovej funkčnosti online mediálnych služieb nemôže byť predmetom zváženia záujmov týkajúcimi sa základných práv a slobôd týchto návštevníkov. Súdny dvor EÚ následne zdôvodnil vo svojom rozhodnutí, že článok 7 písm. f) smernice 95/46 sa má vykladať v tom zmysle, že bráni právnej úprave členského štátu, podľa ktorej môže poskytovateľ on-line mediálnych služieb zhromažďovať a používať osobné údaje týkajúce sa používateľa týchto služieb bez jeho dovolenia len vtedy, keď je toto zhromažďovanie alebo používanie nevyhnutné na umožnenie využitia on-line média týmto používateľom a jeho zúčtovanie, bez toho, aby účel zabezpečenia celkovej funkčnosti týchto služieb mohol odôvodniť použitie údajov.“ Súdny dvor EÚ vo svojom rozhodnutí zdôraznil, že podľa práva Európskej únie je spracovanie osobných údajov zákonné najmä vtedy, ak je nevyhnutné na účely legitímnych záujmov, ktoré plní prevádzkovateľ, alebo tretia osoba alebo tretie osoby, ktorým sú údaje odhalené, s výnimkou prípadu, ak takéto záujmy sú prevýšené záujmami týkajúcimi sa základných práv a slobôd dotknutej osoby. Nemecký súdny dvor následne argumentoval, že poskytovatelia online mediálnych služieb môžu v zmysle § 15 ods. 1 zákona o telemédiách (26.2.2007) zhromažďovať a používať osobné údaje používateľa len v rozsahu nevyhnutnom na umožnenie využitia online média používateľom a jeho zúčtovanie.

(bod 27 C-582/14). V tejto právnej veci sa Súdny dvor EÚ zameriaval na subjektívnu stránku identifikácie osoby zo strany konkrétneho správcu. V zásade rozhodnutie jasne signalizuje nielen p. Breyerovi, ale všetkým subjektom, ktoré spracovávajú akýmkoľvek spôsobom prostredníctvom elektronickej komunikácie identifikátory, že ich činnosť musí byť legálna a legitímna. Zaujímavá je skutočnosť, že hoci v roku 2016 bolo prijaté modernizované nariadenie GDPR, ale ustanovenie článku 4 ods. 1 tohto nariadenia neustanovuje explicitne, že IP adresa, či už dynamická alebo statická je za každých okolností osobným údajom. Právny pojem osobný údaj je preto rovnako ako súkromie významovo otvorený.

V druhom prípade analyzujeme určenie rozhodného práva a rozsah právomocí maďarského dozorného orgánu voči realitnej obchodnej spoločnosti. Obchodná spoločnosť Weltimmo, s.r.o. so sídlom v Komárne bola zaregistrovaná v Obchodnom registri Slovenskej republiky v roku 2002 za účelom prevádzkovania internetovej stránky, kde boli zverejňované informácie o predaji nehnuteľností nachádzajúce sa v Maďarsku. Stručne možno povedať, že to bola realitná kancelária, ktorej konatelia a aj štatutárni zástupcovia boli z Maďarska a činnosť aj koordinovali z Maďarska. Podľa údajov zverejnených v Obchodnom registri Slovenskej republiky obchodná spoločnosť zanikla v roku 2018. V rámci svojej ekonomickej činnosti prišla spoločnosť resp. jej pracovníci do styku aj s osobnými údajmi fyzických osôb, ktoré prostredníctvom nej ponúkali na predaj svoje nehnuteľnosti. Znamená to, že v rámci tohto procesu spracúvala spoločnosť aj osobné údaje inzertujúcich osôb. V danej súvislosti musíme poukázať na skutočnosť, že zverejňovanie inzerátov bolo počas jedného mesiaca bezplatné a následne ich zverejňovanie bolo spoplatňované. Viaceré osoby, ktoré ponúkali na predaj svoju nehnuteľnosť prostredníctvom daného subjektu požiadali e-mailom obchodnú spoločnosť, aby odstránila z internetu jej inzerát, resp. ponuku nehnuteľnosti na predaj, pokiaľ bol zverejnený bezplatne. Zároveň požiadali aj o výmaz svojich osobných údajov. Obchodná spoločnosť nevyhovela požiadavkám inzertujúcich osôb a nevykonala výmaz osobných údajov osôb z internetu, popritom im aj fakturovala platbu za poskytnuté služby. Vzhľadom na to, že inzertujúce osoby neuhradili finančné čiastky uvedené vo faktúrach, obchodná spoločnosť Weltimmo, s.r.o. požiadala inú obchodnú spoločnosť, ktorá sa zaoberala vymáhaním pohľadávok, aby vymohla od inzertujúcich osôb vzniknuté finančné pohľadávky, t. j. aby dosiahla úhradu nezaplatených faktúr. Inzertujúce osoby v záujme ochrany svojich osobných údajov podali sťažnosť na dozorný orgán v Maďarsku. Dozorný orgán na ochranu osobných údajov v merite veci rozhodol, že v zmysle platnej právnej úpravy (§ 2 ods. 1 zákona o ochrane osobných údajov) zhromažďovanie osobných údajov dotknutých osôb sa uskutočnilo na území Maďarska. Maďarský dozorný orgán ako hlavný argument uvádzal, že Weltimmo, s.r.o. má v Maďarsku zástupcu zapísaného v slovenskom obchodnom registri, ktorý má bydlisko v Maďarsku.

V kontexte širších súvislostí zhromažďovanie osobných údajov sa chápe aj ako spracovanie osobných údajov alebo správa osobných údajov. Vzhľadom na to, že existovali viaceré dôkazné prostriedky, dozorný orgán v rámci svojich kompetencií uložil obchodnej spoločnosti Weltimmo, s.r.o. pokutu vo výške 10 mil. maďarských forintov. Obchodná spoločnosť Weltimmo, s.r.o. s nevôľou prijala dané rozhodnutie podala na Fővárosi Közigazgatási és Munkaügyi Bíróság v Budapešti (Správny a pracovný súd) žalobu. Daný súdny orgán v predmetnej veci zrušil rozhodnutie maďarského dozorného orgánu. Weltimmo, s.r.o. na svoju obranu použili argumenty,

že spoločnosť nemá sídlo a ani stálu prevádzkareň na území Maďarska a preto nie je dozorný orgán oprávnený mu ukladať pokuty. Celá kauza sa dostala až na Najvyšší súd, ktorý využil inštitút prejudiciálneho konania podľa článku 267 ZFEÚ a položil Súdnemu dvoru viacero otázok. Súdny dvor Európskej únie v predmetnej veci rozhodol 1.októbra 2015. V záujme dôveryhodnosti uvádzame výrok Súdného dvora Európskej únie v pôvodnom znení, takže ide o citát. Sme toho názoru, že rozhodnutia súdnych inštitúcií, najmä závery by mali byť uvádzané v pôvodnom znení a nemali by byť interpretované ako vlastné názory. Vo veci Weltimmo, s.r.o., výrok Súdného dvora Európskej únie znie: „*V prípade, ak by dozorný orgán členského štátu, na ktorý bola podaná sťažnosť podľa článku 28 ods. 4 smernice 95/46, došiel k záveru, že právom uplatniteľným na spracovanie dotknutých osobných údajov nie je právo tohto členského štátu, ale právo iného členského štátu, mal by sa článok 28 ods. 1, 3 a 6 tejto smernice vykladať v tom zmysle, že tento dozorný orgán môže vykonávať efektívne intervenčné právomoci, ktoré mu boli priznané článkom 28 ods. 3 uvedenej smernice iba na území svojho vlastného členského štátu. Nemôže teda na základe práva tohto členského štátu uložiť sankcie prevádzkovateľovi spracúvajúcejmu tieto údaje, ktorý nie je usadený na tomto území, ale na základe článku 28 ods. 6 tejto smernice musí požiadať dozorný orgán členského štátu, ktorého právo je uplatniteľné, aby zakročil.*“

Podľa nášho názoru, dozorný orgán v Maďarsku mal požiadať Úrad na ochranu osobných údajov na Slovensku a ten mal uložiť aj pokutu subjektu, pričom mohol ako argumenty použiť informácie, ktorými disponoval už dozorný orgán v Maďarsku. V danej súvislosti nesmieme zabúdať, že právomoci priznané dozorným orgánom musia byť vykonávané v súlade s procesným právom ich členského štátu (územná právomoc). Inými slovami povedané, nemôže dozorný orgán uložiť sankcie prevádzkovateľovi spracúvajúcejmu osobné údaje, ktorý nie je usadený na tomto území, ale musí požiadať dozorný orgán členského štátu, kde má obchodná spoločnosť sídlo, aby v danej veci konal. Vo veci objasnenia pojmov správa osobných údajov a spracovanie osobných údajov Súdny dvor Európskej únie zaujal jednoznačné stanovisko, že: „*smernica 95/46 sa má vykladať v tom zmysle, že pojem „adatfeldolgozás“ (správa údajov) použitý v maďarskej verzii tejto smernice, najmä v jej článku 4 ods. 1 písm. a) a v jej článku 28 ods. 6, sa má chápať v rovnakom zmysle ako výraz „adatkezelés“ (spracúvanie údajov).*“ Z uvedeného vyplýva, že pojmy správa údajov a spracúvanie údajov je potrebné chápať v rovnakom zmysle, t. j. majú rovnaký význam. Ochrana údajov fyzických osôb sa vzťahuje na spravovanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. Súdny dvor Európskej únie vytvoril precedens, na základe ktorého pojem správa údajov a spracúvanie údajov v kontexte smernice 95/46 majú rovnaký význam a preto akákoľvek interpretácia zo strany národných autorít by mala byť v súlade s výkladom Súdného dvora EÚ. Slovenská právna úprava v ustanovení § 5 písm. e) ustanovuje, že: „*spracúvaním osobných údajov sa chápe spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.*“ Podobná formulácia je upravená aj

v článku 4(2) nariadenia EÚ 2016/ 679. V danej súvislosti nesmieme zabúdať, že pre spracúvanie osobných údajov sa vyžaduje súhlas dotknutej osoby.

Zhrnutie

Na základe uvedených faktov možno konštatovať, že ochrana osobných údajov sa stáva aj agendou Súdneho dvora Európskej únie. Pomerne často je využívaný inštitút prejudiciálneho konania. Podľa Výročnej správy Súdneho dvora EÚ za rok 2017 bolo až 447 prejudiciálnych konaní riešených na súdnom dvore Európskej únie. V oblasti ochrany osobných údajov bolo riešených až 8 sporov. Súdna činnosť európskych súdov v oblasti ochrany osobných údajov napomáha súdnym autoritám členských štátov a iným orgánom pri uplatňovaní práva Európskej únie. Na konkrétnych dvoch prípadoch sme poukázali na význam prejudiciálneho konania, považovaného za základný mechanizmus práva Európskej únie, ktorého účelom je poskytnúť súdom členských štátov prostriedok na zabezpečenie jednotného výkladu a uplatňovania tohto práva v rámci Európskej únie (Odporúčania, 2012). Význam daných rozhodnutí spočíva v tom, že právo Európskej únie je jednotne uplatňované vo všetkých členských štátoch EÚ. Súdny dvor takýmto spôsobom formuluje významné aplikačné princípy práva Európskej únie. Rozhodnutia európskych súdov ovplyvnia aj správanie sa subjektov, prevádzkovateľov webových stránok na Slovensku. Ak takéto subjekty ukladajú IP adresy, v plnom rozsahu musia rešpektovať rozhodnutie vo veci C-582/14 a musia zaobchádzať s IP adresou ako s osobným údajom. V prípade Weltimmo, s.r.o. Súdny dvor Európskej únie vyplnil medzeru vo vymožitelnosti práva Európskej únie v oblasti ochrany osobných údajov a určil rozhodné právo a rozsah kompetencií dozorného orgánu.

The current publication is created within the project “INtroduction of the data protection reFORM to the judicial system” (INFORM). The project is funded by the European Union’s Justice Programme (2014-2020) under Grant Agreement № 763866. The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

1.4 Dôveryhodnosť informácií distribuovaných prostredníctvom internetu

Orientácia práce na tému dôveryhodnosti informácií distribuovaných prostredníctvom internetu v kontexte kybernetickej bezpečnosti poskytuje celkový náhľad od rozboru základnej zložky informácie v podaní matematickej aplikácie až po navrhnutie nového oddelenia policajného zboru. Prvá kapitola definuje komunikáciu pomocou základnej matematickej logaritmickej funkcie, nakoľko základnou časťou online komunikácie sú jednotky elektrického impulzu známeho ako strojový kód. Strategickým cieľom kapitoly je však analýza online komunikácie, jej relevantnosti a celkovej sily pôsobenia keďže informácie šírené online priestorom ovplyvňujú verejnú mienku obyvateľstva.

Analytická časť práce pozostáva zo skúmania spôsobu šírenia informácie a jej dopad na Policajný zbor SR pretože je z dlhodobého hľadiska je potrebné, aby si aj ozbrojená zložka udržala správnu komunikáciu s civilným obyvateľstvom. V závere práce načrtujeme možného riešenia - východiska pre Policajný zbor SR ako ozbrojenú zložku v možnosti komunikácie s obyvateľstvom pomocou online komunikácie. Ďalším prínosom je riešenie komunikačných problémov radových policajtov, ktorí tiež výrazným spôsobom ovplyvňujú postoj verejnosti k polícii.

Čiastkovým cieľom práce je odpoveď na výskumnú otázku „Sú správy distribuované online formou, ktoré sú zamerané na činnosť policajného zboru dôveryhodné?“ Vo vyústení práce sa bude modelovať návrh ideálneho policajného špeciálneho reportážno - tlačového oddelenia v ktorom budú stanovené jeho schopnosti vytvárania pravdivých a úplných informácií. Zdrojom informácií by mali byť aj jednotliví príslušníci vykonávajúci svoju službu na „ulici“. Ponúkané riešenia sa sústreďujú na komunikáciu vytvárania pozitívneho pohľadu verejnosti budovaním pravdivých informácií. Systém by mal vytvárať úplné informácie a zamedzovať dezinformáciám, či vytváraniu poloprávd v online sieti.

Distribúcia informácií

Distribúcia predstavuje súbor operácií, prostredníctvom ktorých sa produkt z oblasti výroby odovzdáva k dispozícii spotrebiteľovi alebo užívateľovi v správnom množstve, kvalite, cene, mieste a čase. Jednoducho povedané, prostredníctvom distribučného kanála prichádza tovar od výrobcov k spotrebiteľom. Kanál preklenuje priestorové, časové a vlastnícke rozdiely, ktoré vystupujú medzi sférou výroby a sférou spotreby, a to z makroekonomického, ako aj mikroekonomického hľadiska. Z makroekonomického hľadiska pojem distribúcie obsahuje v sebe „všetky aktivity, ktoré umožňujú prechod fyzického a hospodárskeho práva disponovať s materiálными a nemateriálnymi produktmi z jedného hospodárskeho subjektu na iný. Z mikroekonomického hľadiska distribúcia znamená : a) „všetky rozhodnutia, ktoré súvisia s cestou produktov od výrobcu ku konečnému spotrebiteľovi a týkajú sa fyzického pohybu produktov a výberu sprostredkovateľov“ b) „špeciálne marketingové aktivity, ktoré sa týkajú ciest prenosu produktu“ (Loydlová, 2013).

Základným pojmom zákona o slobode informácií je pojem „informácia“. Zákon neobsahuje výslovnú definíciu tohto pojmu, ale význam pojmu „informácia“ jednoznačne vyplýva z kontextu ustanovení zákona a z iných právnych predpisov (Peráček, 2011).

V odbornej literatúre možno nájsť určité definície pojmu „informácia“. Podľa odbornej literatúry je informácia „každé oznámenie obohacujúce vedomie príjemcu“ (Madar a kol., 1995) alebo „akýkoľvek energetický či hmotný prejav, ktorý môže mať zmysel buď pre toho, kto ho oznamuje, alebo pre toho, kto oznamované prijíma“ (Mates a Matoušková, 1997). V praxi slovenských súdov sa často používa nasledujúca definícia pojmu „informácia“: „Informácia je správa, údaj, poučenie, ktorú fyzická osoba alebo právnická osoba odovzdáva inej fyzickej alebo právnickej osobe. Informácia je základom komunikácie. Človek ňou získava nové poznanie a komunikuje s inými ľuďmi.“

Najznámejším nástrojom na šírenie a uchovávanie informácií je internet, respektíve jeho služba www (World Wide Web). Obsah webových stránok tvorí text, hypertextové prepojenia, obrázky a iný multimediálny obsah, teda akékoľvek informácie, ktoré sa oplatí zdieľať v rámci tímu. Klasické webové stránky umožňujú prezerat' svoj obsah a odkazujú sa na iné stránky, čím sa skraca čas potrebný na vyhľadanie súvisiacich informácií. Veľkou výhodou webových stránok je ich nenáročná tvorba a možnosť určiť príjemcu. Stránky môžu byť verejne dostupné na internete alebo dostupné iba v rámci intranetu danej spoločnosti alebo tímu. Intranetová webová sieť poskytuje bezpečný prístup k informáciám, nezávisle od toho, či členovia tímu pracujú na jednom mieste, budove, meste alebo sa nachádzajú v rôznych častiach sveta.

Sociálne siete sa za posledné roky stali novým komunikačným kanálom, cez ktorý sa spoločnosti snažia vytvoriť o najväčšie spojenie spotrebiteľa so značkou. Nejde o klasické stránky, ale určité aplikácie, na ktorých prebieha virtuálna konverzácia, zdieľajú sa fotky, videá, hudba, poskytuje sa priestor pre publikovanie vlastnej tvorby, budujú sa vzťahy medzi užívateľmi. Medzi najznámejšie sociálne siete používané slovenskými užívateľmi patrí predovšetkým Facebook, slovenský popec, My Space, YouTube, Flickr, LinkedIn, Twitter i Wikipedia. Sociálne siete sa v rámci marketingu využívajú s cieľom budovania si PR a dobrého mena firmy, vytvára sa na nich komunita vašich priaznivcov, umožňuje aktívne s nimi komunikovať, podporujú sa na nich reklamné kampane spoločnosti (8688, 2014). Najznámejšia sociálna sieť Facebook je fenoménom tejto doby a hovorí sa, že kto tam nie je, ako keby neexistoval.

Využitie internetu k distribúcii informácií zameraných na činnosť Policajného zboru Slovenskej republiky.

Policajný zbor SR je ozbrojenou zložkou štátu a preto je pod drobnohľadom médií. V dnešnej dobe absencie tlačených – fyzických informácií sú v dlhodobom horizonte na ústupe. Do popredia sa za posledné roky dostáva distribúcia informácií prostredníctvom elektronických médií predovšetkým internetu. Pozorovaním z praxe je možné rozdeliť informácie šírené online na pozitívne a negatívne. Medzi hlavné pozitíva informácií šírených elektronicky môžeme zaradiť, dostupnosť, cenu a rýchlosť. Naopak negatívami sú dôveryhodnosť, ovplyvňovanie (pozmeňovanie) a nutnosť zaobstarat' potrebný hardware

Policajný zbor SR využíva na šírenie správ aj tradičné metódy ako tlačové konferencie. Avšak pre potrebu neustáleho informovania obyvateľstva využíva aj prepojenie siete internet. Na vytváranie webových stránok využíva externých dodávateľov, ktorí vytvoria jednorázovú úlohu – zriadenie dátového centra. Oddelenie informatiky má hlavne správcovskú úlohu. A slúži hlavne na údržbu informačných technológií.

Informácie sa občanom dostávajú cez www.minv.sk, čo je oficiálna web stránka ministerstva vnútra SR, na ktorej sú zverejňované potrebné informácie. Avšak udalosti, ktoré by viedli k popularizácii policajného zboru – využitie na „propagačné“ účely takmer úplne absentujú. Prevládajú strohé informačné správy obsahujúce nevyhnutné kontakty či už z prezídia, alebo krajských riaditeľstiev. Zapojenie iných médií, či iných online vydavateľstiev je taktiež minimálne (Králik, Králiková, 2016).

Z dlhodobého hľadiska značne absentuje využitie sociálnych sietí ako Facebook, či twitter. Je zrejmé, že informácie všetkého druhu sa Policajný zbor SR snaží akumulovať a utajovať, aby nedošlo k dezinformáciám závažnejších tém, či postupov, ktoré by mohli ovplyvniť riadnu funkčnosť Policajného zboru SR. Avšak informovanie civilného obyvateľstva o „drobných hrdinstvách príslušníkov zboru“ nie sú vôbec nikde k dispozícii. Tento problém je dlhodobého charakteru.

Správy, ktoré by viedli k informovaniu obyvateľstva o záslužnej činnosti, či hrdinských skutkoch členov polície nie sú zverejňované dovtedy, pokiaľ niekto vyslovene nezavolá televíznych reportérov. Ak sa udalosť spropaguje a teda zverejní v médiách, nastáva zverejnenie správy ako takej. O danej skutočnosti (napr. záchrana ľudského života) sa kompetentní policajní vyššej inštalácie dozvedia až z médií.

Na základe mediálneho tlaku nastáva v krátkom čase odmenenie príslušníka za dobre vykonanú prácu. K pozitívnemu ohodnoteniu spravidla nedochádza iným spôsobom. Funkcionári nižšej inštalácie mimoriadnu záslužnú činnosť neoznamujú vyšším funkcionárom a nijako sa ani nezasadzujú o odmenenie pracovníka. Televízne spravodajstvo využíva pochopiteľne aj online komunikáciu s divákmi. Reportáže si môžu pozrieť na webovej stránke danej televízie. Ostatné „online noviny“ správy prevezmú a taktiež informujú a udalosť postupujú ďalej k svojim čitateľom.

Faktory ovplyvňujúce dôveryhodnosť informácie z praxe

Svetová sieť nazývaná Internet je voľným prostriedkom komunikácie. Informácie je možné šíriť z akéhokoľvek miesta a v akomkoľvek čase za použitia komunikačnej technológie. Základnými technologickými prostriedkami komunikácie poznáme zariadenia ako klasické PC, notebook, tablet, smartfóny. Prostredníctvom bežných prostriedkov je možné šíriť informácie. V dnešnej dobe za pomoci sociálnych sietí ako hlavne Facebook, Twiter, ale aj lokálnych ako Azet.

Sociálne siete pomáhajú zdieľať naše myšlienky napísané v kybernetickom priestore (textové programy ako napr. Word) alebo špecifické pre písanie online článkov (Andraško a kol, 2018).

Šírenie audiovizuálnej stránky nie je nijako osobitne limitované a k textu nie je problém pridať fotografiu a video. S využitím smartfónov máme záznamové zariadenie stále na blízku

a vedia ho použiť okamžite. Klasické televízne reportáže sú obohacované práve amatérskymi záznamami, ktoré boli vyhotovené priamo počas vzniku informácie (katastrofa, konflikt, výrok známej osobnosti)

Takto získané informácie pokiaľ sú zaznamenávané v súkromí a bez súhlasu dotknutej osoby, sú nezákonne získanými dôkazmi, ktoré však majú v médiách vysokú cenu.

V súčasnej dobe využívajú online priestor na šírenie informácie rôzne subjekty ako súkromné osoby, organizácie, vojenské rozvedky, či ozbrojené zložky ktoré audio a vizuálny záznam môžu rovnako aj zneužiť a upravovať, alebo vytrhávať z kontextu. Takto upravená „pravda“ môže spôsobiť aj neistotu v informáciách, ktoré si rôzne osoby môžu vyčítať z kybernetického priestoru z rôznych uhlov pohľadu. Policajný zbor SR je mimoriadne sledovanou zložkou ako v klasických printových médiách, tak i v online priestore. Policajný zbor najčastejšie a legálne zasahuje do základných práv a slobôd osôb. Niektoré osoby bez dostatočných vedomostí a zo svojho uhla pohľadu to môžu brať v určitých prípadoch konanie polície za zneužitie právomoci (Gregušová, Halászová, 2018). V malom množstve sa také neoprávnené zásahy aj potvrdili. Niektoré zo sťažností boli potvrdené získaním nahrávok vytvorených najčastejšie mobilnými telefónmi. Takéto nahrávky najčastejšie v prípade policajného zboru skončia na internete v rôznych bulvárnych článkoch ako aj v renomovaných spravodajských stránkach (Novotný a kol., 2017). Pri takto získaných a online priestorom šírených správ je potrebné si však uvedomiť nasledovné negatíva:

- ✓ nahrávka alebo snímok môže byť vytrhnuté z kontextu,
- ✓ informácia a teda aj text môže byť podaný jednostranne (z jedného uhla pohľadu),
- ✓ nie je jasné, čo udalosti predchádzalo.
- ✓ sympatizovanie s určitou stranou (nadržiavanie kamarátom, rodine, hnutiu...),
- ✓ vyslovene vytvorená klamlivá správa s cieľom vyvolať rozruch prípadne jej schopnosť výnosného predaja,
- ✓ zaujatosť (voči konkrétnej osobe, organizácii, zlé predošlé skúsenosti),
- ✓ neoverenie si komplexných skutočností (vypočutie nestranných svedkov, overenie si udalosti v ucelenom kontexte, možnosť vyjadriť sa všetkým dotknutým stranám).

Z uvedeného je možné sa domnievať, že správa prijatá z neznámeho zdroja alebo súkromnej organizácie, či osoba by mala byť riadne preverená predtým, než sa začne šíriť online priestorom. V prípade zistenia, že správa je nepravdivá je nemožné ju odstrániť z kybernetického priestoru, nakoľko sa od uvedenia na svetovú sieť nekontrolovane šíri do celého sveta (Gábriš, 2014). Stopy po jej existencii sa môžu nachádzať na rôznych serveroch. Takýmto spôsobom môže byť nenávratne poškodená dotknutá osoba, nepravdivo vykreslená ale nepríjemnosti môže priniesť aj médiu, ktoré informáciu poskytlo.

Návrh zmien vo zvyšovaní dôveryhodností informácií šírených internetom

Policajný zbor sa vo svojej činnosti nemôže dlhodobo spoliehať na súkromné médiá, či bulvárne „plátky“, že prinesú relevantné správy o jeho fungovaní. Záujmom ozbrojenej zložky by

mala byť jeho dôstojnosť, dôveryhodnosť či pozitívny pohľad verejnosti v čo najvyššej miere. Pozitívny pohľad obyvateľstva môže byť získaný hlavne šírením a teda zverejňovaním aj pozitívnych správ z praxe polície (Kútik a kol., 2018). Pozitívne správy by mali pozostávať v zdôrazňovaní kvalitnej práce členov policajného zboru, ako aj využitií sily ozbrojenej zložky v praxi pre prospešnosť a ochranu obyvateľstva. Mnohé udalosti nie sú dlhodobo zverejňované, čo je na škodu práve Policajného zboru SR.

Dôvody nešírenia pozitívneho obrazu PZ vychádzajúc z praxe:

- ✓ neoznámenie pozitívnej správy, prípadne zákroku funkcionárom vyššej inštancie funkcionármi nižšej inštancie, ktorí o pozitívnom zákroku vedia,
- ✓ nezáujem manažmentu policajného zboru riešiť propagačné možnosti polície,
- ✓ dlhodobo neriešený problém šírenia správ len súkromnými médiami,
- ✓ slabá komunikácia so súkromnými médiami,

Riešenie dlhodobého problému musí byť postavené na kompletne novo vybudovanom informačnom systéme tvorenom skúsenými osobami, ktoré by mali byť policajtmí.

Možným riešením z dlhodobého hľadiska by bolo vhodné vytvorenie špeciálneho **reportážneho - tlačového oddelenia**, ktoré by:

- ✓ spracovávalo podnety zo súkromných médií,
- ✓ na ktoré by sa mohol obrátiť ktorýkoľvek policajt alebo obyvateľ v prípade potreby zverejnenia pozitívnej aj negatívnej správy,
- ✓ spätne preverovalo pravosť správy (z úradných záznamov, dodatočného vyťažovania dotknutých osôb),
- ✓ vytvorilo špeciálnu zložku na domovskej webovej stránke www.minv.sk, ktorá by obsahovala možnosť komunikácie s „policajnými redaktormi“ spravujúcich danú reportážnu sekciu,
- ✓ vytvorenia možnosti online reálneho chatu na danej stránke so skúseným policajným reportérom, ktorý by vedel odpovedať na otázky verejnosti a médií,
- ✓ písanie – vytváranie oficiálnych reportáží s potvrdenými a relevantnými správami, ktoré by boli k dispozícii pre obyvateľstvo ale aj voľne šíriteľné pre súkromné online noviny.

Zhrnutie

Na základe nášho bádania sme zistili, že online uverejňovanie rezortných správ by viedli k silnejšej distribúcii aj pozitívnejších alebo doplnujúcich správ kyber priestorom. V dlhodobom horizonte by to mohlo viesť k pozitívnejšiemu pohľadu na policajný zbor. Nakoľko ide o represívnu zložku, je potrebné si aj touto formou budovať pozitívny vzťah s obyvateľstvom, ktoré chráni a je pre neho k dispozícii. Reportážami by mali byť uverejnené aj staršie kauzy, ktoré boli len jednostranne v médiách medializované avšak policajný zbor sa k nim nevyjadril. V danej dobe to mohlo byť kvôli zamedzeniu úniku informácií v priebehu vyšetrovania avšak postupom času by mohli byť ozrejmene a teda pre laickú verejnosť podané.

Samotné získavanie dát a teda reportážnych článkov je náročným procesom. Policajný zbor SR má však výhodu celoplošného pokrytia. Ďalšou výhodou je 24h služba, pri ktorej sú radoví policajti privolaní k najrôznejším udalostiam. Najnovším systémom SOYTRON, ktorý pozostáva aj zo zabudovanej kamery, ktorá policajné zásahy elektronicky zaznamenáva. Dané videozáznamy sú pre vytvorenie online reportáže cenným zdrojom dôkazových materiálov.

Získavanie dát je náročnou činnosťou aj z pohľadu odosielania možných reportáží. Radoví policajti nie sú nijakým spôsobom motivovaní ba dokonca sú decimovaný vedením ohlasovať výnimočné udalosti. Z uvedeného vyplýva, že každý radový policajt by mal mať možnosť udalosť uverejňovať a to spôsobom kontaktovania **reportážneho - tlačového oddelenia**, ktoré by danú policajnú hliadku vyťažila a skutočnosti overila prostredníctvom úradných záznamov hliadky ako aj prípadnou fotodokumentáciou, ktorú by vykonali príslušníci polície na mieste udalosti. Reportážne tlačové oddelenie by malo byť samostatnou súčasťou polície, ktorá by sa zodpovedala ministrom vnútra SR.

Odbúrali by sa medzi stupne šírenia správ, ktoré by ich uverejňovaniu mohli zabrániť (napríklad priamy nadriadení, okresní, krajskí funkcionári, prípadne aj ich zástupcovia, alebo prezidiálni funkcionári rôznych inšancií). Uvedení funkcionári majú vyššie obavy, že by mohli radoví policajti poukázať aj na chyby nadriadených v rozhodovaní o daných udalostiach a z uvedeného dôvodu sú zaujímavé reportážne udalosti zdecimované a nedostávajú sa do online priestoru. Takáto cenzúra plynúca z nevedomosti o daných udalostiach funkcionármi by bola zamedzená. Navrhnutým zlepšením by sa docielilo aj reálnejšieho obrazu práce radových policajtov, pozitívneho vykreslenia zboru a hlavne možného pozitívneho ohodnotenia podriadených policajtov. Takto medializované zásluhy by nemohli byť pod mediálnym tlakom nepovšimnuté. Motivačné ohodnotenie policajta by bolo vo vyššej miere naplnené. Svojím spôsobom by sa aj z radových policajtov alebo dotknutých civilistov stali reportéri. Z praxe je známe, že vidina možnosti vyššieho ohodnotenia by viedlo k následnému vyššiemu nasadeniu policajných hliadok, pri riešení konfliktov.

Súkromné online médiá by mali mať zakaždým otvorenú komunikáciu s vytvoreným reportážnym oddelením. Z daného je možné sa domnievať, že by sa odstránili alebo aspoň minimalizované zavádzajúce správy, neúplné správy, domnienky. Reportáže, články umiestňované v kybernetickom priestore by vytvárali zázemie pre konštruktívnu komunikáciu s verejnosťou. Daným by sa odstraňovala nedôvera občanov k Policajnému zboru SR, ktorá v dnešných časoch je vytváraná nedostatočnou komunikáciou s verejnosťou.

2 Problémy využívání možností a služeb digitálního prostředí

2.1 Všeobecné základy cloudovej zmluvy ako inomínátneho kontraktu pri dodávke a prevádzke informačných systémov

Cloudové riešenia slúžia najmä na ukladanie dát a zdieľanie dát. Ekonomická výhodnosť, dostupnosť dát a bezpečnosť dát sa stávajú stredobodom pozornosti odborníkov. Vysoký stupeň informatizácie a dostupnosť správnych informácií sa stala kľúčovým komponentom pre dosahovanie konkurencieschopnosti subjektov vo sfére biznisu najmä zvýšením gramotnosti manažérov v oblasti IKT a vo využívaní informačných komunikačných systémov a technológií (Russev a kol., 2002, 2003).

Inomínatny kontrakt pri dodávke informačných systémov

Z hľadiska historických, spoločenských a ekonomických východísk samotné zmluvné právo v oblasti informačných technológií na území Slovenskej republiky začalo vznikať v deväťdesiatych rokoch minulého storočia. Prvotné zmluvné vzťahy boli iba jednoduchými zmluvami o dielo a licenčnými zmluvami. Dokonca aj v druhej polovici deväťdesiatych rokov, aj keď už boli v praxi realizované zložité dodávky informačných systémov, udržiavali sa zmluvné vzťahy k nim na pomerne primitívnej úrovni. Začiatkom nového storočia došlo k búrlivému rozvoju spoločenských vzťahov a tiež k búrlivému rozvoju technológií, pričom zároveň značne stúplo právne povedomie subjektov relevantného trhu. So zvyšujúcim sa stupňom zložitosti zmluvných vzťahov dochádzalo k vývoju právnej teórie v tejto oblasti. A to aj napriek tomu, že ide o rozvoj teórie mimo právnu vedu v akademickej oblasti (Cirák a kol, 2008).

Obchodnoprávna prax založila vznik troch zásadných zmluvných prúdov vo vzťahu k poskytovaniu informačných systémov. Tieto prúdy sa rozlišujú obvykle podľa toho, kto disponuje bezprostredne po dodaní informačného systému výhradnými autorskými majetkovými právami a konkrétnym stupňom možnosti s informačným systémom nakladať a aplikovať na neho právo odvodené od práva držby. Podstatným prvkom je tiež samotná štruktúra a povaha plnenia, či sa plnenie považuje iba za poskytnutú službu, alebo či je možné na plnenie nahliadať ako na dielo.

Prvým prúdom sú zmluvy, ktoré sa vzťahujú k poskytovaniu informačných systémov ako služby. V praxi sa na úpravu tohto zmluvného modelu vyvinuli cloudové zmluvy. Ide o najnovší zmluvný typ hybridného kontraktu, ktorý v sektore informačných systémov vznikol a bol zaužívaný pri poskytovaní plnenia v posledných rokoch.

Druhým zmluvným prúdom sú zmluvy, kde v rozsahu životného cyklu informačného systému dochádza k poskytovaniu informačného systému alebo jeho časti, ako plnenia vo forme diela, alebo v obdobnej forme. Pod tento druhý prúd spadajú zmluvy pri vývoji a dodávke informačných systémov ako zmluva o analýze, vývojovo-implementačná zmluva, a podobne.

Nakoľko informačný systém je zložitým plnením, pridružujú sa k týmto zmluvám v rôznych kombináciách rôzne licenčné zmluvy, kúpne zmluvy a iné.

Tretím prúdom sú zmluvy, kde síce nedochádza priamo k poskytovaniu informačného systému, ale dochádza k jeho prevádzke, údržbe a sú poskytované súvisiace plnenia. Do tejto kategórie patria zmluvy servisné a údržbové zmluvy, SLA a ich vzájomné kombinácie.

Okrem uvedených troch zmluvných prúdov je potrebné sa zaoberať aj vybranými spoločnými znakmi, ktoré sa prelínajú všetkými tromi zmluvnými prúdmi zavedenými obchodnoprávnou praxou. (Maisner a kol. 2011)

Spoločenské pomery a ich vývoj majú v posledných 20 rokoch za následok výrazný nárast komplikovanosti obchodných vzťahov, ako aj nákladov na vymáhanie práv v prípade, ak nedochádza k dobrovoľnému plneniu zo strany niektorého z účastníkov kontraktuálneho vzťahu. Preto je zo spoločenského aj ekonomického hľadiska, aby vznikol opis prinajmenšom unifikovaných obchodných zvyklostí, ktoré subjekty relevantného trhu považujú za obvyklé a teda záväzné (Lacko, 2011).

Inominátne kontrakty pri dodávke informačných systémov v domácej a zahraničnej literatúre

Je nutné konštatovať, že rozpracovanie tohto vedeckého problému v literatúre prakticky neexistuje. Existuje literatúra, ktorá opisuje tzv. "best practise" pri riadení projektov informačných systémov, avšak žiadna literatúra sa prakticky nezaoberá zmluvnými vzťahmi k informačným systémom. Jedinou oblasťou vo vzťahu k informačným systémom, ktorá je v literatúre rozpracovaná, je oblasť autorského práva. Avšak aj táto rozpracovanosť sa týka primárne počítačových programov, okrajovo ostatných druhov plnení, avšak v podobe informačných systémov nie je táto oblasť rovnako nijako rozpracovaná. Podľa nášho názoru aktuálny stav v odbornej literatúre je možné odôvodniť tým, že právnici spravidla dokážu popisovať právne vzťahy k hmotnému plneniu, prípadne k majetkovým právam, nakoľko toto si nevyžaduje žiadnu hlbšiu technologickú vedomosť a postačuje schopnosť zovšeobecnenia vzťahov. Myslíme si, že v oblasti informačných technológií je pre schopnosť právnej analýzy nevyhnutné mať rovnako špecifické vedomosti v oblasti právnej vedy a zároveň technologické vedomosti a poznanie. Táto kumulatívna podmienka je splnená u iba veľmi malého počtu osôb. A spravidla ide o osoby prevažne mimo Slovenskej republiky. Do istej miery existuje táto problematika rozpracovaná v zahraničnej literatúre, avšak v rámci systému angloamerického práva, ktoré je v stanovenej oblasti do tej miery odlišné od kontinentálneho právneho systému, že nie je možné teórie zo zahraničia aplikovať na podmienky práva v Slovenskej republike. Podľa nás existujúce publikácie sa spravidla v podmienkach Slovenskej republiky obmedzujú na iba strohé preberanie znenia existujúcich právnych noriem a nemajú snahu žiadnym spôsobom uskutočňovať právnu úvahu v rozsahu dispozitívnej oblasti, alebo aplikácie zmluvnej voľnosti.

Cloudová zmluva ako inomínatny kontrakt pri dodávke a prevádzke informačných systémov

Cloudová zmluva je praxou zavedený názov pre kontrakt, ktorý v sebe zahŕňa kombináciu viacerých nominálnych a inomínatných zmluvných typov, ktoré vo vzájomnej kombinácii tvoria jeden zmluvný bilaterálny alebo multilaterálny právny úkon, na základe ktorého je poskytovaná a

využívaná služba cloud computingu, ktorý je zmluvno-realizačný model vzťahov a plnenia, kde poskytovateľ služby umožňuje užívateľovi používať zdieľaný dátový priestor a prostriedky výpočtovej techniky, vrátane diel s povahou počítačových programov a to prostredníctvom dátovej siete, ktoré vyčleňuje poskytovateľ služieb pre užívateľa, pričom výpočtové prostriedky a výpočtové zdroje, vrátane diel s povahou počítačových programov poskytuje formou služby (Gregušová a kol., 2005; Jansa a Otevřel, 2011; Závodný a kol., 2012).

Právna prax pri uzatváraní kontraktov na poskytovanie cloudovej služby narazila na problém členenia cloud computingovej služby z hľadiska identifikácie poskytovateľa služby a identifikácie užívateľa služby, nakoľko pri poskytovaní cloud computingovej služby dochádza v niektorých prípadoch ku kumulácii subjektov zmluvného vzťahu na strane tak poskytovateľa, ako aj užívateľa služby. Na základe čoho právna prax ustálila rozdelenie cloud computingovej služby pre zmluvné účely do 4 základných kategórií:

- A. Súkromný cloud computing - súkromná cloud computingová služba je prevádzkovaná iba pre jedného užívateľa, alebo pre uzatvorený okruh užívateľov s rovnakou sadou práv a povinností a to buď samotnou organizáciou zastrešujúcou okruh užívateľov na základe iného zmluvného vzťahu (napr. pracovný pomer) alebo poskytovateľom, ktorý je voči užívateľom treťou stranou, avšak okruh užívateľov služby ostáva a naďalej uzatvorený.
- B. Verejný cloud computing - verejný cloud computing je služba cloud computingu poskytovaná jedným poskytovateľom, alebo združením poskytovateľov služby pre neurčitý neobmedzený okruh užívateľov služby, ktorí si výpočtové zdroje a dátový priestor ako službu dynamicky zdieľajú medzi sebou v rozsah do maximálnej kapacity poskytovanej služby.
- C. Hybridný cloud computing - služba hybridného cloud computingu je poskytovaná ako kombinácia súkromného cloud computingu a verejného cloud computingu, pričom na strane poskytovateľa vystupujú minimálne dvaja a viacerí poskytovatelia, pričom pomocou technológií sa užívateľom služby javí služba ako jednotná a ako by bola poskytovaná jediným poskytovateľom.
- D. Spoločenský cloud computing - model pre spoločenský cloud computing je postavený na tom, že infraštruktúra cloudu je zdieľaná medzi niekoľkými uzatvorenými skupinami užívateľov, kde v rámci jednotlivých skupín má každá vlastnú sadu práv a povinností, pričom jednotlivé skupiny užívateľov majú spoločné prvky relevantné pre zmluvný vzťah (napr. Spoločná bezpečnostná politika, odborové zameranie...).

A pre samotný realizačný model právna prax ustálila tieto základné realizačné modely cloud computingovej služby:

- ✓ Cloud typu SAAS
- ✓ Cloud typu PAAS
- ✓ Cloud typu IAAS

Aby bolo možné vytvoriť cloudovú zmluvu, ktorá pozostáva obvykle v jednom právnom úkone z viacerých zmluvných typov, ktoré spolu tvoria kontrakt, je nevyhnutné dodržanie presného postupu, ktorý je do značnej miery jedinečný práve pre vytvorenie cloudovej zmluvy:

- ✓ Zadefinovať do ktorej skupiny cloudových zmlúv bude kontrakt patriť SAAS, PAAS, IAAS ...
- ✓ Vytvoriť procesný model realizácie služby.
- ✓ Spracovať model a popis práv, povinností a sankcií.
- ✓ Vytvoriť ochranné mechanizmy rizík a zadať pravidlá nároku na náhradu škody a zmluvné pokuty.
- ✓ Roztriediť jednotlivé atribúty z predošlých bodov podľa ich povahy pod jednotlivé nominátne zmluvné typy.
- ✓ Nezatriedené atribúty považovať za inominátny kontrakt.
- ✓ Vytvoriť jednotlivé nominátne zmluvné typy a vzájomne ich skombinovať.
- ✓ Skombinovať nominátne zmluvné typy s atribútmi inominátneho kontraktu.
- ✓ Odstrániť duplicity práv, povinností a aplikovaných sankcií.
- ✓ Aplikovať všeobecné a záverečné ustanovenia.

Alternatívne, pri posudzovaní cloudovej zmluvy pre potreby jej aplikácie v rozsahu definovania práv, povinností a sankcií na jednotlivé povahy plnenia cloud computingovej služby, je vhodné postupovať týmto spôsobom:

- ✓ Vyhľadať znaky patriace pod známe nominátne zmluvné typy.
- ✓ Na základe znakov určiť nominátne zmluvné typy.
- ✓ Ustanovenia ktoré ostali navyše budú posudzované ako osobitný inominátny kontrakt.
- ✓ Stanoviť povahu plnenia.
- ✓ Jednotlivé povahy plnenia priradiť k príslušným zmluvným typom.
- ✓ Aplikovať príslušné ustanovenia na konkrétne čiastkové plnenia.

Aj keď ide de facto iba o jednu kontrakt, z právneho hľadiska ide o kombináciu viacerých viazaných zmlúv vyjadrených jedným komplexným prejavom vôle zmluvných strán. Tj. nie je možné, aby zanikla iba niektorá časť cloudovej zmluvy. Väzba medzi jednotlivými zmluvami kontraktu je priama a obojsmerná.

Každá cloudová zmluva ako semihybridný kontrakt obchodného práva má svoje špecifiká. V niečom vychádza zo štandardných obchodných zvyklostí, niektoré práva sú upravené Obchodným zákonníkom, prípadne inými právnymi normami a niektoré práva a povinnosti sú v zmluvách upravené na báze obchodných zvyklostí závislých od konkrétneho typu, povahy a špecifikácie plnenia. Ďalej bude analyzovaná cloudová zmluva pre privátny cloud typu IAAS.

Cieľom cloudovej zmluvy je taký stav, kedy užívateľ cloudovej služby môže nerušene a riadne využívať na obvyklý účel výpočtový výkon cloudovej služby, ktorý bude prevádzkovaný na cloudovej infraštruktúre v súlade s príslušnými metrikami.

Účelom cloudovej zmluvy je úprava vzájomných práv a povinností a režim ich uplatnenia medzi zmluvnými stranami tak, aby táto zodpovedala ich slobodnej a vážnej vôli relevantnej k dátumu uzatvorenia cloudovej zmluvy.

Predmetom plnenia cloudovej zmluvy je povinnosť poskytovateľa zabezpečiť poskytovanie cloudovej služby počas celej doby jej platnosti a účinnosti v rozsahu podľa popisu, ktorý tvorí spravidla prílohu cloudovej zmluvy, alebo iný dokument, na ktorý sa cloudová zmluva odvoláva.

Predmetom plnenia cloudovej zmluvy je tiež povinnosť poskytovateľa realizovať plnenie po uplynutí platnosti a/alebo účinnosti cloudovej zmluvy v rozsahu na ktorý sa splnenie alebo možnosť zániku viaže na okamih realizovania takéhoto plnenia. *Predmetom plnenia cloudovej zmluvy* je tiež povinnosť užívateľa platiť poskytovateľovi zmluvnú odplatu za realizovanú cloudovú službu podľa cloudovej zmluvy. *Predmetom plnenia cloudovej zmluvy* je zároveň povinnosť užívateľa poskytnúť poskytovateľovi súčinnosť podľa cloudovej zmluvy pre naplnenie cieľa a účelu cloudovej zmluvy a na základe cloudovej zmluvy. *Predmetom plnenia cloudovej zmluvy* je ďalej povinnosť užívateľa prijať plnenie od poskytovateľa po uplynutí platnosti a/alebo účinnosti cloudovej zmluvy v rozsahu na ktorý sa splnenie alebo možnosť zániku viaže na okamih realizovania takéhoto plnenia.

Rovnako je predmetom cloudovej zmluvy povinnosť oboch zmluvných strán zachovávať mlčanlivosť.

Objektom cloudovej zmluvy sa rozumie cloudová služba, ktorá spĺňa metriky podľa cloudovej zmluvy. Ide o službu poskytnutia výpočtového výkonu v rozsahu metrík poskytovateľom užívateľovi.

Metrikami sa rozumujú také technické merateľné parametre cloudovej služby, v takom rozsahu a s takou definíciou, aby bolo možné presne definovať rozsah a povahu poskytovanej cloudovej služby formou kvantifikovateľných ukazovateľov a priebeh jej poskytovania kvantifikovať, monitorovať a vykazovať. Spravidla sa do výpočtu metrík sa nezapočítava krátkodobé prerušenie v poskytovaní cloudovej služby, ktorému sa tiež hovorí systémová odstávka. Ide o odstávku v poskytovaní cloudovej služby na nevyhnutne dlhú dobu za účelom údržby, prípadných opráv zariadení poskytovateľa, infraštruktúry, informačných systémov, vrátane priebežnej aj jednorazovej profilaxie, pričom pre každú kategóriu metrík je tento čas ohraničený maximálnou hranicou stanovenou v počte hodín za jeden prevádzkový rok. V cloudovej zmluve sa obvykle upraví pre najcitlivejšiu kategóriu metrík maximálna systémová odstávka definovaná v hodinách za rok.

Miestom plnenia sa pri cloudovej zmluve určuje relatívne ťažko, nakoľko ide o distribuovaný výpočtový výkon na väčší počet lokalít. Preto sa zvykne pre účely cloudovej zmluvy uplatňovať princíp určenia miesta poskytnutia služby v zmysle definície Zákona o dani z pridanej hodnoty. Podľa tohto sa pre účely dane z pridanej hodnoty rozumie miestom poskytnutia služby sídlo užívateľa. Nakoľko ide o službu realizovanú prostredníctvom elektronických komunikačných prostriedkov, služba musí byť poskytovaná takým spôsobom, aby bola dostupná odkiaľkoľvek z územia lokality definovanej cloudovou zmluvou. Miestom prevádzky cloudovej služby musia byť také priestory na zmluvou definovanom území, ktoré spĺňajú príslušné metriky.

Časom plnenia sa pre účely cloudovej zmluvy rozumie obdobie počas ktorého poskytovateľ poskytuje užívateľovi cloudovú službu. Časom plnenia sa rozumie obdobie totožné s účinnosťou cloudovej zmluvy. Toto neplatí pre plnenia, na ktoré zánik účinnosti a/alebo platnosti cloudovej zmluvy nemá vplyv.

Poskytovateľ je povinný plniť cloudovú službu prostredníctvom elektronických komunikačných prostriedkov a dátových sietí a to tak, že cloudová služba je užívateľovi prístupná v čase plnenia cloudovej zmluvy v rozsahu podľa metrík špecifikovaných cloudovou zmluvou. Užívateľ má právo, avšak nie povinnosť, využívať cloudovú službu.

Shrnutí

Podľa nášho názoru najväčším problémom právnej úpravy v oblasti IKT je, že neexistuje žiadna postačujúca špecializovaná právna úprava k tejto špecifickej obchodnej a technickej činnosti, neexistuje ani príslušný zákon v miere, postačujúcej v aktuálnej právnej praxi (Smejkal a kol., 2004). V každej zmluve musí byť jej predmet dostatočne špecifikovaný tak, aby rozsah záväzkov bol nepochybný a špecifikácia plnenia termínov v zmluve záväzne definovaná.

2.2 Služby poskytované digitálnymi platformami

Kolaboratívne hospodárstvo otvára nové podnikateľské možnosti pre každého a zároveň vytvára možnosti pre vznik nových nekonvenčných obchodných modelov. Podľa Európskej komisie sa odhaduje, že príjmy vytvorené pôsobením kolaboratívnych platforiem v Európe dosiahli v roku 2015 takmer 4 bilióny EUR a sprostredkovali transakcie vo výške až 28 biliónov EUR. (Európska komisia, 2016/356) Poskytovatelia služieb za prenájom svojho hmotného a nehmotného majetku, ktoré nevyužívajú alebo ich majú nadbytok získavajú finančný benefit. Nie vždy je zámerom poskytovateľa služby dosahovanie zisku, ale niekedy pri službách peer-to-peer je služba poskytovaná iba za odmenu na pokrytie nákladov, ktoré poskytovateľovi služby alebo majiteľovi vzniknú. V správnom vyjadrení ide o požičiavanie existujúceho majetku na určitý čas, ktoré vlastní určitá osoba. Tento vzťah sa pomerne často nazýva aj spoluspotrebitelstvo. Botsmanova R. (2015) pojem spoluspotrebitelstvo definuje ako „oživenie tradičného trhového správania sa - prenajímaním, požičiavaním, zdieľaním, darovaním- pomocou technológií, realizovaných tými spôsobmi a v tej miere, ako to pred vznikom internetu nebolo možné.“ Daná forma poskytovania služieb sa takýmto spôsobom odlišuje od tradičných ekonomických štruktúr a podnikateľských aktivít. Podľa Vebera model zdieľaného využívania vecí k rastu HDP jednoznačne neprispieva (Veber et al., 2016).

Teoretické východiská kolaboratívneho hospodárstva

Globalizácia, rozvoj technológií a nástup priemyslu 4.0 napomohli vzniku a rozvoju kolaboratívneho hospodárstva. Kolaboratívne hospodárstvo je ekonomickým modelom medzi makroekonomickou úrovňou a mikroekonomickou úrovňou, kde sú využívané moderné technológie umožňujúce zdieľanie majetku (statkov). Súčasná teória a prax nepozná jednotnú definíciu pojmu kolaboratívne hospodárstvo, ktorej ekvivalentom je aj pojem zdieľaná ekonomika (v anglickom jazyku sharing economy). Systém kolaboratívneho hospodárstva fungoval v niektorých štátoch v minulosti. Už v roku 1978 Marcusem Felsonem a Joe L. Spaethem v spoločnej štúdii s názvom *Community Structure and Collaborative Consumption* popisujú zdieľanie automobilov tzv. *carsharing* a používajú pojem *collaborative consumption*, čo možno preložiť do slovenského jazyka ako spoluspotrebitelstvo (Felson, 1978).

Teória o kolaboratívnej ekonomike sa postupne vyvíjala a viacerí autori začali prezentovať svoje názory vo vedeckých dielach. Zo širokého spektra sme vybrali iba niektoré. Botsmanová a Rogers (2010) definujú zdieľanú ekonomiku ako „spôsob ekonomického usporiadania, v ktorom účastníci preferujú zdieľaný prístup k tovarom a službám, skôr než individuálne vlastníctvo. Ide zároveň o systém, ktorý je riadený webovou technológiou umožňujúcou zdieľanie a zmenu aktív od priestorov až po automobily, a to takým spôsobom, ktorý doteraz nebol možný.“ (Botsmanová et al., 2012)

Podľa Matofsku „zdieľaná ekonomika je sociálne – ekonomický ekosystém založený na zdieľaní ľudských a prírodných zdrojov. Zdieľanie zahŕňa vytváranie hodnôt, výrobu, distribúciu, obchod a spotrebu tovarov a služieb rôznymi osobami a organizáciami.“ (Matofska, 2016) Tento systém, umožňuje získať prístup k veciam za finančnú úhradu, ktoré vlastní niekto iný

prostredníctvom platformy - jednoduchej aplikácie na mobilnom zariadení. S modernejšou definíciou v roku 2016 prišli Veber a kolektív (Veber et al., 2016), podľa ktorých *„zdieľaná ekonomika je ekonomickým modelom, kedy prostredníctvom technologických platforiem sa prepájajú dodávatelia ochotní prenajímať svoje aktíva spotrebiteľom na dočasné použitie. Aplikácie pre mobilné telefóny sú typickým nástrojom pre prístup k technologickej platforme spájajúcej spotrebiteľa s dodávateľom.“*

V teórii sa pomerne často poukazuje na názor Sundararajana (2016), že: *„zdieľaná ekonomika je nová forma organizovania hospodárskych činností založených na kapitalizme.“* V danom prípade možno polemizovať, pretože nie vždy ide o organizovanú hospodársku činnosť.

V kontexte širších súvislostí by sme nemali zabúdať ani na Bendu (2016), ktorý vo svojom článku Perspektívy sdílené ekonomiky uvádza, že: *„zdieľanú ekonomiku môžeme chápať ako poskytovanie a najímanie si služieb, prípadne užívanie statkov prostredníctvom digitálnych platforiem, ktoré redukovujú transakčné náklady a zvyšujú úžitkovosť statkov, mnohokrát určených iba na osobné využitie.“* Takáto forma poskytovania služieb oslabuje postavenie veľkých podnikateľských subjektov a do popredia sa dostávajú malí a strední podnikatelia alebo aj samostatne zárobkovočinné osoby a neprofesionálni poskytovatelia služieb.

Podľa nášho názoru najvhodnejšia definícia kolaboratívneho hospodárstva je upravená v *Oznámení Európskej komisie* týkajúce sa Európskej agendy pre kolaboratívne hospodárstvo (2016). V záujme správnosti, formou priameho citátu objasňujeme pojem kolaboratívne hospodárstvo z pohľadu Európskej únie (Európska komisia, 2016/356): *„Na účely tohto oznámenia sa pod pojmom kolaboratívne hospodárstvo rozumejú obchodné modely, v rámci ktorých sú obchodné činnosti podporené kolaboratívnymi platformami vytvárajúcimi otvorený trh pre dočasné využívanie tovarov a služieb, ktoré sú často poskytované súkromnými osobami.“* Európska komisia zavádza aj pojem kolaboratívne platformy, z čoho je zrejmé, že sa bude meniť systém ekonomických vzťahov a aj právnych vzťahov, najmä vo väzbe na ochranu práv spotrebiteľa a na daňovú politiku.

Ide o novú formu socio-ekonomických vzťahov, t. j. vzťahov kolaboratívnej platformy, ktoré sa odlišujú od tradičných ekonomických vzťahov. Podstatný rozdiel je v tom, že kolaboratívne hospodárstvo je založené na moderných technológiách resp. na on-line platformách. Vytvárajú sa tu možnosti pre profesionálnych podnikateľov a neprofesionálnych podnikateľov, na zjednodušené zdieľanie hmotného a nehmotného majetku. Avšak nevýhodou kolaboratívneho hospodárstva je, že práva spotrebiteľa alebo príjemcu služby nie sú dostatočne chránené. Táto forma umožňuje ľahší prístup k využívaniu statkov v plnom rozsahu. Moderné technológie umožňujú spájanie ľudí do komunity, čo nie je obvyklé v trhovej ekonomike, kde je preferovaná anonymita a individualizmus. Z tradičného modelu ekonómie sa stáva ekonomika sociálnych sietí, spolupráce a efektívneho využívania statkov, aj keď nie na zmluvnom základe. Subjektami týchto vzťahov sú sprostredkovateľ, poskytovateľ služby a príjemca služby, tak ako je to uvedené v *Oznámení Európskej komisie* z roku 2016. Sprostredkovateľom je on-line platforma, ktorá umožňuje zjednodušenou formou poskytovanie služby prostredníctvom webovej stránky alebo aplikácie. Inými slovami povedané, služby sú vykonávané prostredníctvom automatizovaných funkcií, ktoré vykonáva počítačový algoritmus. V zmysle slovenskej právnej úpravy

prevádzkovatelia týchto sprostredkovateľských platforiem sú považovaní za poskytovateľov elektronických komunikačných sietí a elektronických komunikačných služieb podľa zákona č. 351/2011 o elektronických komunikáciách. Pasívnu platformu sprostredkovania možno vyjadriť vzťahom C2B2C, t.j. consumer-to-business-to-consumer. Sprostredkovateľ okrem prevádzkovania on-line platformy môže byť zároveň aj priamym poskytovateľom služieb na danej platforme a daný vzťah je vyjadrený B2C consumer-to-business (Analýza zdieľanej ekonomiky, 2017). Poskytovateľom služby je vlastník majetku, ktorý nie je v pozícii podnikateľa a jeho právny status je niekde medzi podnikateľom a spotrebiteľom, pričom nemá žiadnu zodpovednosť. Ak berieme do úvahy definičné znaky podnikateľa upravené v § 2 ods. 2 Obchodného zákonníka, že „*podnikateľom je osoba zapísaná v obchodnom registri, osoba, ktorá podniká na základe živnostenského oprávnenia, osoba, ktorá podniká na základe iného než živnostenského oprávnenia podľa osobitných predpisov, fyzická osoba, ktorá vykonáva poľnohospodársku výrobu a je zapísaná do evidencie podľa osobitného predpisu,*“ tak tu nastáva problém, pretože mnoho subjektov poskytujúcich služby v rámci kolaboratívneho hospodárstva nemožno zaradiť medzi podnikateľov v zmysle platnej právnej úpravy. Z tohto dôvodu hovoríme aj o neprofesionálnych poskytovateľoch služieb. Následne tu vyvstáva aj problém s postavením dodávateľa, ktorý podľa § 52 ods.3 Občianskeho zákonníka je osobou, *ktorá pri uzatváraní a plnení spotrebiteľskej zmluvy koná v rámci predmetu svojej obchodnej alebo inej podnikateľskej činnosti*. Ako uvádza Kočišová et. al. (2018), v právnom poriadku Slovenskej republiky ide o nový pojem súkromného práva, ktorý nepozná ani Obchodný zákonník a nie je možné ho zamieňať ani s pojmom podnikateľ. V rámci kolaboratívneho hospodárstva nie všetky dodávateľsko- spotrebiteľské vzťahy sú upravené na zmluvnom základe. Prijemca služby, ktorý využíva službu za nižšiu cenu, nekladie dôraz na to, aby mu bola poskytovaná služba na zmluvnom základe (krátkodobý nájom nehnuteľností). V zásade ide o nový ekonomický systém, ktorý sa vyvíja a je založený na spoločnom využívaní majetku. Súčasná prax pozná dva typy zdieľania a to *business-to-consumer (B2C) a peers-to-peers (P2P)* (Stephany, 2015) V rámci kolaboratívneho hospodárstva sa bude meniť aj správanie zákazníka, pretože príjemcovia služby alebo spotrebiteľia sa nebudú riadiť tradičnými marketigovými nástrojmi, ale svojimi skúsenosťami, kvalitou služby, dostupnosťou a cenou. Sami sa budú rozhodovať a nenechajú sa ovplyvňovať tradičnými marketingovými praktikami.

Regulácia právnych vzťahov v rámci kolaboratívneho hospodárstva

Globálna ekonomika vstupuje do novej etapy, súčasťou ktorej je aj nové kolaboratívne hospodárstvo vyznačujúce sa charakteristickou črtou zdieľania a spolupráce naprieč všetkými oblasťami hospodárskeho a spoločenského života.

Právne vzťahy súvisiace s podnikaním, ako aj právne formy obchodných spoločností sú upravené v Obchodnom zákonníku a v živnostenskom zákone. Tu vyvstáva práve otázka, či v zmysle § 2 Obchodného zákonníka (zákon. č. 513/1991) a § 2 zákona č. 455/1991 Zb. o živnostenskom podnikaní skutočne môžeme hovoriť o podnikaní, či živnostenskom podnikaní. Vilčeková et al. (2018) poukazuje na to, že novelou Obchodného zákonníka a živnostenského zákona účinnou od 1. mája 2018 pod pojmom podnikanie a živnosť rozumieme *sústavnú činnosť vykonávanú samostatne podnikateľom vo vlastnom mene a na vlastnú zodpovednosť za účelom*

dosiahnutia zisku alebo za účelom dosiahnutia merateľného pozitívneho sociálneho vplyvu, ak ide o hospodársku činnosť registrovaného sociálneho podniku podľa zákona o sociálnom podniku a za podmienok ustanovených zákonom. Ako ďalej uvádza Milošovičová et al. (2018) vzťah medzi podnikaním a živnosťou je možné vyjadriť slovami, *že každá živnosť je podnikaním, ale nie každé podnikanie je živnosťou. Subjekt, ktorý takúto hospodársku činnosť vykonáva sa nazýva podnikateľ*. Z tohto dôvodu nový model podnikania v kolaboratívnom hospodárstve môžeme nazývať aj *ad hoc modelom podnikania*. Súčasťou tejto formy podnikania je síce aj jeden z aspektov podnikania – dosahovanie zisku, ale nejedná sa o sústavnú hospodársku činnosť. Základom tohto vzťahu je vlastníctvo majetku *de iure* (podľa práva) a *de facto* (podľa skutočného stavu). Vlastníctvo majetku (predmetu, veci) *de iure* znamená právne vlastníctvo a skutočné vlastníctvo majetku, ktorý je určený na osobnú spotrebu znamená skutočné – reálne vlastníctvo (*de facto*). Práve takýto majetok môže byť predmetom obchodného vzťahu v rámci kolaboratívneho hospodárstva a je zdieľaný aj inou osobou ako je jeho samotný majiteľ. Zapojením digitálnych platforiem v rámci poskytovania služieb kolaboratívneho hospodárstva sú veci (majetok) využívané za poplatok. Práve kolaboratívna ekonomika má tendenciu podporovať zmeny týkajúce sa nákupného správania príjemcov služby. Z uvedeného vyplýva, že súčasná právna úprava týkajúca sa podnikania v zmysle Obchodného zákonníka a živnostenského zákona by mala byť novelizovaná, pretože ide o novú formu podnikania prostredníctvom on-line komunikačných nástrojov a platforiem.

Zrejme slovenská právna úprava bude ovplyvnená aj regulačným rámcom Európskej únie, ktorá už v danej oblasti prijala viacero dokumentov. Práve rozhodnutie Súdneho dvora Európskej únie vo veci taxislužby Uber malo zásadný vplyv na prijatie novely zákona č. 56/2012 Z. z. o cestnej doprave v znení neskorších predpisov v roku 2018. Cieľom právnej normy bolo zefektívnenie kontrolných mechanizmov a zjednodušenie podmienok prevádzkovania taxislužby s cieľom eliminovať nelegálnu činnosť v taxislužbe. Daná právna norma upravuje konkrétne podmienky pre osoby poskytujúce taxislužby aj formou digitálnej platformy. Zároveň sú daným právnym predpisom vytvorené spravodlivé podmienky pre poskytovanie taxislužby, kde všetci účastníci majú rovnaké práva a povinnosti, bez nadštandardného zaobchádzania. Právna regulácia zohľadňuje aj nové spôsoby zabezpečovania kvalitnej a bezpečnej služby pre zákazníkov.

Pozitívnu skutočnosťou v oblasti zdaňovania je, že na Slovensku je riešená už otázka zdaňovania subjektov, ktoré vykonávajú služby prepravy a ubytovania na území Slovenskej republiky aj formou digitálnej platformy od 1. 1. 2018 (Zákon č. 344/2017, ktorým sa mení a dopĺňa zákon č. 595/2003 Z. z. o dani z príjmov). V súvislosti s príjmami plynúcimi zo zdieľanej ekonomiky bolo pozmenené ustanovenie § 16 ods. 2 zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov. Podstatná zmena sa okrem iného dotýkala úpravy definície trvalého miesta, keďže ide o novú formu podnikania založenú na poskytovaní sprostredkovateľských služieb v oblasti prepravy a ubytovania prostredníctvom digitálnych platforiem, ktoré sa na rozdiel od tradičných foriem podnikania vyznačujú absenciou fyzickej prítomnosti daňovníka s obmedzenou daňovou povinnosťou na území štátu, v ktorom sú poskytované služby (Dôvodová správa k návrhu zákona, 2017). Novela zákona o dani z príjmov upresňuje základné pojmy (v §2 písm. ag). Zákon o dani z príjmov definuje digitálnu platformu ako „*hardvérovú platformu alebo softvérovú platformu potrebnú na vytvorenie aplikácií a správu aplikácií*.“ V danej súvislosti nesmieme zabúdať, že ide o zákonnú definíciu a preto je potrebné, aby nedochádzalo k rôznym iným nepresným interpretáciám alebo interpretáciám rôznych autorov, najmä vo väzbe k politike

zdaňovania na Slovensku. Podľa zákona č. 595/2003 Z. z. o dani z príjmov, daňovníci, ktorí využívajú na sprostredkovanie predaja svojich služieb zahraničné digitálne platformy sú povinní zrážať daň z platieb za sprostredkovanie plateným zahraničným operátorom digitálnej platformy. V zmysle § 43 ods. 2 zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov daň sa zráža vo výške 19% alebo vo výške 35%, ak sú prijímateľom platby daňovníci z nezmluvných štátov (zmluvy o zamedzení dvojitého zdanenia). Operátori digitálnych platforiem zahraničných subjektov sprostredkujúci služby prepravy a ubytovania na území Slovenskej republiky majú zákonnú povinnosť registrovať svoju stálu prevádzkareň (§ 49 a ods. 5 zákon o dani z príjmov postupom uvedeným v § 67 ods. 1 zákona č. 563/2009 Z. z. o správe daní). V prípade, ak správca dane zistí, že operátori digitálnych platforiem si nesplnili povinnosť zaregistrovať v Slovenskej republike stálu prevádzkareň, správca dane ho vyzve na splnenie povinnosti. Ak daný subjekt nekoná v súlade so zákonnými povinnosťami, správca dane zaregistruje ich stálu prevádzkareň z úradnej moci.

Poskytovanie taxislužieb – prípad Uber

V rámci kolaboratívneho hospodárstva sú poskytované rôzne druhy služieb. Keďže neexistuje žiadna oficiálna databáza týchto služieb zamerali sme sa na služby, ktoré sú poskytované na území Slovenskej republiky prostredníctvom digitálnej platformy. Tieto informácie sme získali z dostupných webových stránok a skutočne sú poskytované. Možnože existujú aj iné formy služieb, ale my sme vychádzali z dát zverejnených k 1.1.2019. V nasledujúcej tabuľke ilustrujeme segmenty služieb kolaboratívneho hospodárstva, ktoré sú poskytované.

Tab. č. 2 Prehľad segmentov kolaboratívneho hospodárstva na Slovensku

Práca	Príležitostná práca, konzultačno-poradenská práca
Cestovanie	Ubytovanie, sprievodcovstvo, prehliadky
Finančné služby	Pôžičky, poistenie
Doprava	Autá, bicykle
Sociálne služby	Opatrovanie starších ľudí a detí
Služby	Poskytovanie služieb – reštauračné, obsluha, záhradné slávnosti, doručovacie služby, práca v domácnosti, taxislužby
Móda	Oblečenie muži, ženy, deti
Nájom priestorov	Kancelárske priestory, obchodné priestory, byty

Zdroj: vlastné spracovanie 2019

Z uvedenej tabuľky č. 2 vyplýva, že na Slovensku sú poskytované služby v rôznych oblastiach formou on-line platformy. Univerzálnym princípom týchto služieb je, že platí zákaz akejkoľvek diskriminácie z dôvodu štátnej príslušnosti, t. j. je zavedený inštitút rovnoprávnosti pre všetkých účastníkov na trhu. Ďalším princípom je, že väčšina služieb v rámci kolaboratívneho hospodárstva sa realizuje on-line platformou. Tento zavedený systém dodávateľsko-spotrebiteľských vzťahov nie je vhodný pre všetky skupiny obyvateľstva, pretože sa vyžaduje určitá zručnosť v oblasti informačných technológií. Dôležitou črtou subjektov kolaboratívneho hospodárstva je, že poskytovatelia služieb stanovujú ceny v reálnom čase na

základe ponuky a dopytu v danej lokalite. Najviditeľnejší sektor v rámci kolaboratívneho hospodárstva je sektor ubytovacích služieb, dopravných služieb a preprava osôb. Nezanedbateľné sú aj finančné služby, t. j. poskytovanie pôžičiek (ide o alternatívu bánk).

V rámci sektora dopravných služieb môžeme hovoriť o dvoch kategóriách služieb: požičiavanie áut (carshering) a preprava osôb formou taxislužby. Tieto služby sú poskytované za úplatu. Na slovenskom trhu v oblasti prepravy osôb pôsobila obchodná spoločnosť Uber Slovakia s. r. o. od roku 2015. Táto obchodná spoločnosť vznikla ako technologický start-up v San Franciscu v roku 2009. V zásade ide o mobilnú aplikáciu poskytovania dopravnej služby osobám. Obchodná spoločnosť Uber poskytuje cca v 650 mestách sveta prepravné služby. V roku 2015 dosiahla obchodná spoločnosť Uber tržby v objeme 1,5 mld. USD a zamestnávala cca 6 700 zamestnancov. Zo sprostredkovania taxi služby si Uber ponecháva 20 %. Podľa tvrdenia spoločnosti PrivCo je hodnota Uberu cca 51 mld. USD (Veber et al., 2016). V Prahe vykonáva obchodná spoločnosť Uber rozsiahle podnikateľské aktivity: prevádzkuje cca 5 tisíc taxíkov a zamestnáva cca 1 000 partnerských vodičov.

Vo viacerých štátoch Európy má aj svojich konkurentov, napr. v Českej republike prepravu osôb zabezpečuje aj spoločnosť Liftago. Obchodnej spoločnosti Uber Slovakia, s.r.o. na Slovensku konkuruje aj slovenská taxi aplikácia HOPIN TAXI. Osobitosťou prevádzkovateľa s aplikáciou HOPIN TAXI je, že taxikári majú platnú taxi koncesiu a vodiči spĺňajú všetky legislatívne požiadavky súvisiace s podnikaním v preprave osôb, čiže majú požadované poistenia, psychotesty a servisné kontroly auta. Na Slovensku pôsobí Cech taxikárov, ktorý je Živnostenským spoločenstvom podnikateľov zabezpečujúcich výkon taxislužby v Bratislave. V roku 2017 cechové združenie evidovalo 279 členov fyzických osôb a 8 členov právnických osôb (<http://cechtaxi.sk/o-nas/>, 2018). Na slovenskom trhu pôsobia tradičné subjekty poskytujúce taxi služby na princípe telefonického objednávanía služby cez dispečing a niekoľko taxi-aplikácií (napr. Hopin, Liftago, Taxify).

Taxislužby poskytované prostredníctvom on-line platformy sú dynamicky sa vyvíjajúca oblasť avšak ich činnosť ovplyvnilo rozhodnutie Súdneho dvora Európskej únie vo veci C-434/15, Asociación Profesional Elite Taxi proti Uber Systems SpainSL. V roku 2014 Asociación Profesional Elite Taxi, profesijná organizácia združujúca taxikárov mesta Barcelona v Španielsku, podala žalobu na Obchodný súd č. 3 Barcelona (Španielsko), ktorou sa domáhala najmä uloženia sankcie obchodnej spoločnosti Uber Systems Spain, spoločnosti patriacej do skupiny, ktorá spravuje uvedenú platformu, za nekalú súťaž voči vodičom Elite Taxi. Vzhľadom na nejasnosť právnej úpravy v danej oblasti súd využil inštitút prejudiciálneho konania a predložil na Súdny dvor Európskej únie prejudiciálne otázky ohľadom výkladu článku 56 Zmluvy o fungovaní Európskej únie. Dané rozhodnutie ovplyvnilo aj poskytovanie taxislužieb vo viacerých členských štátoch Európskej únie. Súdny dvor Európskej únie skúmal poskytovanie sprostredkovateľskej služby, t. j. sprostredkovanie transakcie medzi vodičom využívajúcim svoje vlastné vozidlo a osobami, ktoré vyhľadávajú prepravu v rámci určitého mesta a služby prepravy osôb motorovým vozidlom. Súdny dvor Európskej únie v prípade sprostredkovateľskej služby poskytovanej prostredníctvom aplikácie pre smartfóny uviedol, že *v podstate zodpovedá kritériám kvalifikácie služby informačnej spoločnosti*. Tento druh služby má inú povahu ako služba individuálnej

prepravy osôb v meste a preto taxislužbu Súdny dvor Európskej únie kvalifikoval ako dopravnú službu v zmysle čl. 2 ods. 2 písm. d) smernice Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu (pozri v tomto zmysle rozsudok z 1. októbra 2015, *Trijber a Harmsen*, C-340/14 a C-341/14, EU:C:2015:641, bod 49).

Súdny dvor Európskej únie v predmetnej veci zaujal stanovisko, že subjekt poskytujúci služby v oblasti dopravy je povinný sa riadiť pravidlami poskytovania služby v zmysle článku 58 ods. 1 Zmluvy o fungovaní Európskej únie (ZFEÚ) a nie článkom 56 Zmluvy o fungovaní Európskej únie. Meritum spočíva v tom, že poskytovanie služby prostredníctvom on-line platformy za úplatu neprofesionálnym vodičom motorového vozidla sa považuje za dopravnú službu a preto sa na ňu vzťahujú pravidlá a normy týkajúce sa dopravy alebo prepravy osôb po cestnej komunikácii. Zároveň z tohto rozhodnutia vyplýva, že na poskytovanie služieb obchodnou spoločnosťou Uber sa nevzťahuje inštitút slobody poskytovania služieb ako na služby informačnej spoločnosti. Aj v podpornom stanovisku generálneho advokáta Súdneho dvora Európskej únie, *Macieja Szpunaru* z 11. mája 2017 v predmetnej veci sa uvádza, že: „služby poskytované platformou Uber musia byť klasifikované ako služby v oblasti dopravy.“ (Návrhy generálneho advokáta, 2017). Právne vety v uvedenom rozhodnutí sú založené na platnej právnej úprave, na presvedčivom odôvodnení a na právnej logike. Pre právnu argumentáciu aplikoval Súdny dvor Európskej únie ustanovenia Zmluvy o fungovaní Európskej únie, smernicu Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu a smernicu Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu. Judikatúra Súdneho dvora Európskej únie je prameňom poznania práva a v tomto prípade je aj právnym nástrojom na vyplňanie medzier v právnych predpisoch. Slovenský právny systém je ovplyvnený aj právnym systémom Európskej únie a preto nie je možné ponechať bez povšimnutia uvedené rozhodnutie, čo sa prejavilo aj na Uznesení Okresného súdu Bratislava I, ktorý ustanovil obchodnej spoločnosti Uber povinnosť zdržať sa prevádzkovania taxislužby spôsobom, ktorý nespĺňa požiadavky na takéto prevádzkovanie podľa zákona č. 56/2012 Z. z. o cestnej doprave v znení neskorších predpisov (Uznesenie Okresného súdu Bratislava I zo dňa 16. februára 2018). Ak by sme chceli vyjadriť v zjednodušenej forme výrok súdu, tak **ide o zákaz činnosti**. V danej veci je zaujímavá ešte aj skutočnosť, že spoločnosť Uber neprichádza na trh s novým produktom služby, ale preberá príjemcov služby od tradičných poskytovateľov taxislužby. Môžeme jednoznačne konštatovať, že cieľom Uberu bolo získať podiel na trhu za nerovnakých podmienok, pretože tradiční poskytovatelia taxislužieb museli splniť určité podmienky. V dôsledku tohto rozhodnutia bola prijatá už spomínaná novela zákona o cestnej doprave v roku 2018. Pre poskytovateľa taxislužieb na Slovensku je podmienkou, že musí byť odborne spôsobilý (musí mať koncesiu) na výkon taxislužby a musí byť bezúhonnou osobou. Globálny start-up Uber sa musí pri výkone činnosti prispôbiť danému právnemu rámcu, pretože z pohľadu európskeho práva akýkoľvek slovenský právny predpis má nižšiu právnu silu ako predpisy Európskej únie a judikatúra Súdneho dvora Európskej únie.

Zhrnutie

Poznatky sumarizované v tejto štúdii naznačujú, že kolaboratívne hospodárstvo vytvára nové možnosti pre poskytovateľov služieb a príjemcov služieb, avšak zároveň vyvoláva mnoho otázok týkajúcich sa poskytovania služieb. Aj keď sa zdá, že poskytovanie služieb v rámci kolaboratívneho hospodárstva je liberalizované a nie je obmedzený prístup na trh pre poskytovateľa služby alebo príjemcu služby, rozhodnutie Súdneho dvora Európskej únie vo veci Uber ovplyvnilo poskytovanie taxislužieb nielen v zahraničí, ale aj na Slovensku. S prihliadnutím na stupeň technologického rozvoja operátori digitálnych platforiem poskytujúci sprostredkovateľské služby v oblasti prepravy a ubytovania na Slovensku už majú upravené daňové povinnosti v novej právnej úprave z roku 2017 týkajúcej sa povinnosti registrácie stálej prevádzkarne. V merite veci daňová povinnosť vzniká daňovníkovi s obmedzenou daňovou povinnosťou, operátorovi digitálnej platformy, ktorý vykonáva činnosť a dosahuje príjem zo stálej prevádzkarne na území Slovenskej republiky.

Na základe analytických faktov sme dospeli k záveru, že vyvstáva mnoho problémov z hľadiska právnej regulácie, ktorá je základom správneho poskytovania služieb v rámci kolaboratívneho hospodárstva. Podľa nášho názoru je potrebné v obchodnom práve vymedziť inštitút podnikania formou kolaboratívnej platformy, postavenie podnikateľa a pod. Zároveň tu vyvstávajú aj problémy týkajúce sa živnostenského oprávnenia a v neposlednom rade aj v rámci pracovno-právnych vzťahov, pretože kolaboratívne hospodárstvo podporuje rast zamestnanosti, ale nevyriešené zostávajú podmienky zamestnávania a sociálne istoty osôb poskytujúcich služby. Vzhľadom na to, že ide o cezhraničné poskytovanie služieb bude potrebné upraviť aj vzťahy z pohľadu medzinárodného práva súkromného. Možnože v budúcnosti budeme svedkami aj nového právneho odvetvia - právo digitálnych služieb.

Kapitola bola spracovaná s podporou Agentúry na podporu výskumu a vývoja na základe Zmluvy č. APVV-16-0091.

2.3 Digitization and rural development - Clash or potential?

Digitization is threatening the rural space and is in contrast seen as the solution for challenges of rural regions. Digital solutions such as online-shopping and delivery services are challenging retail and other services in rural communities. But digitization is also seen as the chance to develop more flexible solutions that are able to solve problems of the rural communities, such as mobility, health services, retail and daily supply and labor. But still the threat seems to be larger than the challenges, because most digital solutions first and only address urban markets. The rural space as a market seems to be only an accidental by-catch.

We see a conflict in processes and structures of rural development and the focus and procedures of (digital) startups that hinders but at best case does not support the development of digital rural solutions. Based on a review of literature and current practices we want to answer three main questions: What is the state of digital solutions for the rural areas with a focus on digital startups? What are the drivers behind digital startups and why do they not address rural areas? What are the potentials for rural areas?

We start by discussing the current situation of the digital startup scene. In this context we put focus on the urban-rural gap and the reasons for the ongoing brain drain, and thus in many cases, decline of rural regions. Second we look into the standard strategies and cook books of digital businesses and startups and discuss the key factors for a successful product launch from the perspective of rural development. Finally, we want to discuss the potentials for rural areas by demonstrating a best practice example regarding digital startup scenes in remote areas, such as debating the ambivalence of our initial question “Digitization - clash or potential?”.

As digital startup approaches in rural regions still remain uncharted territories, we examined our best practice examples exclusively due to fieldworks studies. The resulting information is based upon interviews of case studies.

In addition to presenting various startup strategies and discussing the lack of digital innovation in rural regions, we want to put a special focus on the issue, if it was possible to narrow the urban-rural gap by creating a link between labor market and universities. Regarding a successful corporation of these components, we want to emphasize the high value of networking processes in particular.

The rural gap

I want to be part of it, New York, New York [...] I want to wake up in a city that never sleeps, and find I'm a number one, top of the list, king of the hill, a number one, proclaims Frank Sinatra in 1979 referring to the wide range of personal and professional opportunities big cities like New York stood for in the last century. But the late 70ies are history now and the age of digitization should enable entrepreneurs and startups "to be part of it" without travelling urban or metropolitan areas. The reason why the world of startups and young entrepreneurs still mainly concentrates on urban areas is because metropolitan areas seem to

provide open-mindedness, access to test markets and the possibility to connect to and communicate with like-minded people of the scene. It is also partially built on the cluster concept identified by Porter (Porter, 2003) and the Silicon Valley as a metropolitan high concentration of a creative scene.

Even though digital business models have quite a big impact on rural areas they never explicitly address the rural areas themselves as targets or primary markets. Rural areas are not perceived yet as a specific target market. This becomes even apparent regarding the existing specialist literature. The reading material about the process of developing digital startups in the course of evolving specific test markets in urban and metropolitan areas (e.g. beachhead market) seems to be complete and almost gapless - instead the shelves for approaches in rural areas remain gaping empty.

This seems quite contradictory regarding the actual influential role of rural areas in the German economy, as more than 50 percent of the gross domestic product are generated there. Moreover, more than half of the German population lives in rural regions.

But does this mean the breakdown for the rural areas in digitization? - No, because the keyword in this context is attractiveness of the area for possible startups. The aim is not about competing against metropolitan areas, but about identifying and highlighting the own potentials and strong points of our rural regions. The key question is, which offers can rural areas make to be recognized by startups or what is the task and potential of rural development in the digital age? From a regional development perspective, the region must be reflected on the one hand side as a location for startups to develop, but also as a market for digital products.

In order to stay competitive and economically strong in the long term, we need to tackle the development of attractiveness of rural regions in the future. Digital attractiveness of rural areas should not be understood any more as a metaphor for only creating broadband access - it implies much more. The key lies in attracting young entrepreneurs and startups by providing them space and opportunity to investigate their products. Good basic conditions, openness and esteem for startups and a positive attitude towards investigation and foundation processes are essential to lay down the tracks to narrow this rural gap. Furthermore, we see this process as a call for the municipalities to develop this emerging flow of creativity. It is their responsibility to promote a change of mentality, encouraging the acceptance and openness in politics and municipal administrations. Business development may no longer only focus on processes and projects relevant to the present day - furthermore business development needs to imply a future-oriented knowledge policy.

Strategies of digital companies and startups

Assuming that the appropriate framework such as high speed internet is given, we point out three different methods, startups make use of in order to achieve a successful product launch to open the discussion how regional development can incorporate this thinking and develop instruments to support startups in the rural space.

The first strategy we want to mention in this context is called "Lean Startup Strategy". The investigator, Eric Ries (Ries, 2012), describes his strategy with the simple words:

- ✓ Be more innovative.
- ✓ Stop wasting people's time.
- ✓ Be more successful.

According to his theory the reason for most startups failure lies not in their disability to create the product they intended to build, but in the fact that they built the wrong product and took too much time and money, launching a product, the market has no current demand for. They are literally putting the cart before the horse and begin their approach to work out an idea for a product they think the market asks for. Hence they pursue this idea in a time and money-consuming investigation process without ever showing the product to their prospective users. Due to the fact that these startups do not take the peoples' interests and demands into account, it is quite likely that the launch of the product on the market turns out to be a flop. To avoid product launching failures the lean startup strategy works according to the motto "work smarter not harder."

As the resources of a rising business are limited, the lean-up strategy blocks out the wide range of available markets, chooses one specific market and puts its focus on this so called Beachhead Market. The next step, the expansion of the range of products, does not happen before the product has received the market's acceptance. In case of a negative product launch,

the strategy provides a scientific approach to include customers' feedback straight into the managing and creating processes of startups. The question "How can we learn more quickly what works, and discard what doesn't?" represents the strategy's center piece. By presenting already the first steps - mostly already in a very rudimentary form - to the prospective users, they can react quickly on the markets' feedback and change the product regarding the users' needs and demands. By the time the product is fully developed, it is already partly established and known by various customers. Besides a successful product launch, the motivation of this strategy implies also to keep management and marketing processes as minimalistic as possible. Thus Eric Ries (2012) describes his lean startup strategy simply as a "just do it" approach.

So far, so good: but before the conquest of a niche market, startups need the prospective clients' attention and their interest and intention to buy the specific product. How do the startups establish their products and services successfully on the local market? To be honest, even though some rural regions have undergone a remarkable transformation in the last decade, they still cannot be considered a classic example how to think outside the box at all. The question in a rural space is, how regional development might support the development of startups by linking them to classical actors of regional development, which are mainly "pain" driven? Could this match making activity, as a classical task of regional development agencies, be the basic for a new digital regional development instrument? And may the network of regional development agencies be able to support startups to grow from one region as a beachhead market to other regions?

How do startups initiate a process of rethinking? How do they handle the challenge to smarten up - partly still - quite conservative areas with a touch of cosmopolitanism? Once again, the answer is easy - the clue is to kill the pain! And the easiest way to create a metaphorical pain

killer is to create habit-forming products or services that are linked straight to the user's daily routine and emotions. Companies increasingly see their economic value depending on the strength of the habit they create. Hence, the second strategy we want to introduce here is the Hook-Model by Nir Eyal (Eyal, 2014), a strategy that links a costumers' problem, "his pain", that frequently with a solution, until it converts into an habit. Our daily lives are filled with a great number of tiny stress factors. Normally we face them without consciously being aware of our reactions how we exactly handle them. We unconsciously make use of products or services to find stress reducing solutions.

Due to the Hook-Model strategy, startups make use of the customer's emotion by stirring them long enough with external triggers until this stimulus turns into an internal - and thus an emotionally-driven - trigger.

To illustrate this theory, we want to provide an example taken from every day's life:

Let's assume that it is Friday night and all of our friends are at some party. We are alone at home and feel bored and lonely. In the nowadays age of social media it is very likely that we intuitively start scrolling through Facebook, Twitter, Instagram, checking out new feeds, posts and messages. And that's the point. The external trigger has by now converted into the internal trigger. As the human being pursues for the elimination of pain, negative emotions cause often internal triggers. And in this case the pain is nothing more than "loneliness" or "desire for social contacts". Creating an habit-forming product, the entrepreneurs need to understand the connection between the customer's emotions and his internal trigger, in order to make smart use of external triggers -that are supposed to motivate the user to the intended action. Thus Facebook, Instagram, Twitter, etc. provide an immediate reduction of this pain. The user is, consequently, hooked by these companies without even being aware of it. Instead of relying on expensive marketing or promotion, these startups create step by step associations to their product as the source of relief to the customer's pain.

In analogy to broadband development in rural regions we need to be careful not to mix up technology and application. Broadband alone will not solve the problems of rural areas, because it first requires software and internet applications that use this technology. In analogy internet and software applications will not solve the problems, if we just consider them as a technical solution and disregard how software shapes our habits and lives. Which means that again the link between technology as a solution, entrepreneurs as its developers and providers and potential users in region would provide a new opportunity, how regional and rural development could develop new approaches how to use digitization of our society and develop new instruments by supporting startups to find the right hook and rural communities for testing the perception and potentials for growth.

In contrast to the Lean-Startup strategy and the Hooked-Model, the focus of the third and last approach we want to discuss lies not on the marketing or commercialization strategies, but on the creation process itself.

"Creativity cannot be used up. The more you use it, the more you get out of it", says Maya Angelou, an American professor and author of the early 21. century, and keeps the Design Thinking philosophy simply to the point: Complex problems require a complex way of thinking - and heterogeneous teams offer the best conditions to face them. Design Thinking is based on the

will and ability to corporate beyond the own horizon in interdisciplinary research centers. The strategy is simple but ingenious: Round tables with experts from many different horizons throw their knowledge together and develop investigations exclusively designed for the certain region. This clustered and interdisciplinary "made by many" corporation of researchers and engineers implies not only the end of the "era one man show", but contributes considerably to the local economic structural transformation. Moreover, the high level of interaction due to this cluster brain storming process, automatically implies a high level of relation to the target group. While design thinking is already a concept large parts of the startup economy builds upon, it could be also an instrument to foster digital regional development by rapidly develop possible solutions for already well defined problems of the rural community. By extending already existing local action groups of rural development and involving young entrepreneurs and tech-enthusiasts and applying design thinking principles might guide rural development towards digitization.

Best practice example

The theory of "Just do it" sounds relatively simple, but in practice the realization poses a quite tricky challenge. Our research leads us to the question whether there were any existing digital approaches that focus explicitly on how to build up remote areas. Indeed, there are. Arnar Sigurðsson and Arnhildur Lilý Karlsdóttir, an Icelandic entrepreneur couple, "just did it".

Iceland has been a blank spot on the world map until 2010, when the eruption of the volcano Eyjafjallajökull moved the island into the center of global attention. But even though the tourism sector has been growing exponentially ever since, regarding the global world scale Iceland still rates among the most remote countries on Earth. Þingeyri, a small village in the Westfjords of Iceland can be literally pointed out as the proverbial remoteness. Indeed, it is that isolated that even Iceland's famous ring road bypasses this region entirely, meaning that only ten percent of the, by now two million tourists per year, visit this place, generally speaking. During the last twenty years the little fishing village had faced the typical characteristics of rural decline such as a significant brain drain or an immense decrease in population. Literally speaking Þingeyri confronts a double remoteness: a tiny village on the remotest edge of an isolated island in the North Atlantic Ocean, almost 50 km away from the municipality's principal place Ísafjörður. Not really what we would call a typical location for a startup scene, wouldn't we? And exactly this is the place where Arnar Sigurðsson and his wife Arnhildur Lilý Karlsdóttir, both coming from a tech background, established their project Blábankinn, Blue Bank, an innovation hub and creative space, in the year 2017. The project faces the challenge that many remote villages in sparsely populated municipalities have to deal with in terms of decreasing local services. The purpose of Blue Bank is the creation of a multi-purpose site that combines public and private activities in order to provide new solutions to services. The goal is to provide a platform and Design-Thinking location for social and economic innovation. The aim lies not only in attracting new people to the society, but a lot more in bringing together the local community, creatives and entrepreneurs from the outside. Apart from being the main community and service center for the locals of Þingeyri, the goal of the Blue Bank is the creation of a hub for free-thinkers, of a high-tech, low-stress place for startups,

innovators, artists or creatives, where they can find the chance to disconnect from the any noise and distraction and focus explicitly on their ideas.

Despite of the limiting factors regarding remote areas such as issues concerning transportation and lack of services, Arnar and Lilý had to deal with the social and emotional challenge of convincing the local residents in order to establish Blue Bank successfully. In a place that has been facing decline for such a long period, they had to display both tact and sensitivity to generate a positive response from the locals. As there had been revitalization approaches in Þingeyri and its surrounding area in the past, the clue was not to act like "quick fix" experts from the capital. "We don't want to create some kind of elite", proclaims Lilý and thus emphasizes the high value of inclusion of local residents during the establishment of an interactive and innovative platform such as Blue Bank. Nevertheless, by explicitly addressing the locals via social media and integrating local kids in workshops about advantages of a global life, the local response to Blue Bank and the attendance at various events was right away entirely positive. Hence the successful launch of Blue Bank created, according to the Norwegian Ink Magazine, is the answer "to the lack of amenities in Þingeyri".

As we pointed out above, the key factor leading to success, lies in the creation of networks, in the corporation and exchange of different groups of people.

The approach makes for an interesting dynamic - on one hand, it's a social service that looks inwards, and on the other, an entrepreneurial society that looks outwards, seeing things on an international scale. (Arnar Sigurðsson)

Despite the establishment of a startup funding scenery, the aim of Blue Bank is to create a space to simplify access to public services and improve the communication between residents and the local government. Hence Blue Bank provides a bunch of services that result in a decisive step forward for the habitants of the area surrounding Þingeyri. Blue Bank's original use as a banking service for Landsbanki's cashier service has now been expanded. In its role as a local contact point for the municipality Ísafjarðarbær, Blue Bank plays an important role as a link between Þingeyri's residents and Ísafjörður Municipality concerning various municipal services. Furthermore, Blue Bank takes care for the questions regarding the services of the Workers' Union of Westfjords, Verk Vest, and in addition to that, provides an open link to the library in Ísafjörður where books can be ordered online. Facing the era of digital nomads and Blue Bank's role as an innovation hub, the project offers the possibility to rent out open office spaces and organizes community based events, lessons and workshops for certain target groups.

With regard to the question whether a blueprint of this would work out in any other remote area, the Blue Bank founders point out that the clue of any startup establishment lies in the amount of value it adds to the area. They consider Blue Bank as a long-term investment into the future of Þingeyri. According to Arnar it is the "whole package" - the smooth interaction of people, specific location, energy and atmosphere -, that paves the future way for the vision of a "Silicon Fjord" at one of the remotest places in the Northern Hemisphere.

New strategies for a digital rural development?

This best practice example underpins our assumption that it is possible to add value and create synergies by connecting the common approaches of regional management / regional development (e.g. different groups of actors/drivers, regional strategy processes, inter-municipal collaboration) with the approaches, support and development of digital startups (e.g. design thinking, lean startup, lean development)

This strategy requires the connection and cooperation between municipalities as well as tools of the regional management and a cooperation with the academic sphere. The Icelandic village Þingeyri is just one of many remote spaces dealing with the ongoing discussed emigration effect of academics and university graduates in rural areas which influences the economic structure of these rural regions significantly. Straight communication with students and scientists in universities is therefore indispensable in order to prevent this loss at an early stage. In order to counteract business shutdowns, migration effects and the loss of jobs involved, it is essential to initiate a dialogue with young scientists and pledge them support for the foundation of their businesses and startups.

As shown with the example of Blue Bank, a possible starting point could be the creation of virtual social networks, the establishment of points of interest in public buildings (town hall, library, etc.) in a central location or any other approach that encourages communication and exchange processes in rural regions. The key lies in communication - in whatever form.

One of our three main issues to be answered in the introduction of this paper is the question about the potential for rural areas. The potential of digitization in rural regions implies creating innovative solutions for the common problems, rural regions are dealing with - concept of mobility, access to education, local suppliers, health care, etc. As the activities provided by Blue Bank cover not only startup related services but also a wide range of municipal services, the institution is of potential interest for both academics and working class and thus addresses different target groups.

The initialization of communication processes between these multi-dimensional and heterogeneous networks (citizens of rural regions, political/municipal representatives, academics/representatives of technical universities) provides the base to investigate the actual requirements of rural regions. Knowledge about the specific market demands consequently supports startups to launch their business models dealing with the improvement of basic public services in rural regions successfully.

And the clue in this approach - returning to the topic of digitization - is that digital applications are given the technical capability and know-how to connect the required public services on a range of various levels.

Particularly with regard to this development of these networks, technical universities could play a leading role as an important local economic factor. This is even clearly stated in the Bavarian Higher Education Act (BayHSchG), which declares research and development as one of the main tasks of Bavarian technical universities. In practical terms technical universities literally may empower the establishment of research groups working on topics that are still largely unexplored and with no effective knowledge available yet. As mentioned above, this quite user-oriented way of research leads to the straight implementation of the research results in the relevant area. Thus this

strategy - the corporation with technical universities - could turn out to be not only a significant success and economic factor in urban areas but also for local businesses in a rural space. The corporation between local businesses and technical universities stimulates such a constructive dialogue and thus encourages the development of e.g. part-time master degree programs and highly qualified workplaces. In turn this increases the area's attractiveness for so called "home comers" - highly skilled young folks that had left to urban areas for university studies or employment issues.

We want to take the example of Technische Hochschule Deggendorf (THD) as a role model how to merge the two worlds of labor market and universities and how to narrow regional barrier between mostly urban located universities and the rural space (Dorner & Lemberger, 2013). THD is considered to be "a catalyst for regional development processes" and plays an important role in the regional management strategy of the area. In this particular case the county's business development, the technology transfer of the university and the planning processes of local management form a group and corporate constantly. Thus they succeeded to combine the local economy's know-how and experiences of application of funding. Meanwhile THD is involved in various research networks and connects involved actors with a pool of economic and regional management processes. The key in this approach is the inclusion of the classic tools of regional management, which implies basically the inclusion of municipalities. Municipalities interests' in rural regions are often mainly represented by small-scaled businesses and representatives from the working class. We want to emphasize here that the focus of this approach lies not solely on academics. In the case of THD, the aim of the regional management process is to improve the marketing of Deggendorf as an industry location, as well as the initiation of networks between university and economy in order to open access to governmental development funds. For everybody - regardless of the educational background. While Deggendorf as a city with 35,000 inhabitants is already very rural, this process was taken to extremes during the past 10 years. By building a set of research facilities in the districts around Deggendorf in the Bavarian Forest in cities and villages with 3,000 to 10,000 inhabitants with the so called Technology Campuses (German: Technologie Campi - TC). TCs are a new type of research facility as a regional and mainly rural branch of a university. 10 years ago THD established its first Campus in Freyung (7,000 inhabitants) followed by a second campus in Teisnach (3,000 inhabitants). The objective was to allocate special research groups closer to regional industries. Each campus has a thematic emphasis focused on the local industrial cluster and concentration of companies. While Teisnach is specialized in precision optics, Freyung already anticipated the development of Industry 4.0, established as a term three years later, by focusing on computer science as an overarching field for a broader range of industries. Although, challenged in the beginning as an over ambitious concept to establish technological research in rural municipalities, the concept had its main breakthrough already three to five years later. Both campuses outnumbered economic and academic expectations by far and opened the way to establish a network of 8 further campuses.

Conclusion and perspectives

Initially we raised the question whether digitization is threatening the rural space - clash or potential? Digitization is fundamentally changing our society. It offers a wide range of great

development potentials for rural regions. On the other hand, however, this transformation of rural areas also poses a threat to these regions. Rural development in its current state does not have the capability and instruments yet to address this problem, due to the lack of digital and entrepreneurial competence in regional management processes. As shown above we consider the combination of regional development strategies and startup approaches as a possible solution. Opening up for the various startup strategies such as the Design Thinking, including entrepreneurs and startups in the network of regional stakeholders, could be a step towards the creation of multidisciplinary groups. Moreover, this could lead to the establishment of synergetic effects as the entrepreneurs might consider regional development groups as an initial test market. Creation of startups as well as creation of rural centric digital solutions as software, web services and web applications could be the basis of a win-win situation a regional and rural development strategy could moderate and develop. Due to the fact that universities in rural areas present literally the core of a young, technology affine and entrepreneurial community, we see great potential and high value in a corporation of universities and rural development strategies.

2.4 Výzvy riadenia blokchainových technológií v európskom priestore

Význam technológie Distribution Ledger (ďalej skrátené DLT) a virtuálnych mien narastá, ich vývoj pokračuje, aj napriek nad'alej nedostatočnému riešeniu problému ich regulácie. Globálne centrálné banky, ktoré sú lídrami analyzujú možnosť zavedenia svojich digitálnych mien. (CBDC). Vývoj kryptografie, softvéru a výkonu počítača teoreticky umožňuje proces globálneho prechodu z fiat peňazí na virtuálnu menu. Tento proces treba dôkladne manažovať, aby nedošlo k ohrozeniu štátnej suverenity a nekontrolovanej globálnej koncentrácie informácií v rukách nedemokratických subjektov. V januári 2018 dosiahla globálna trhov'á kapitalizácia virtuálnych mien svoj historický vrchol 831 mld. USD. (Marketcap, 2018). V súčasnosti (začiatok apríla 2019) je trhov'ý strop po obrovskom poklese cien približne 93 miliárd USD. V porovnaní s globálnou trhovou kapitalizáciou svetových akciových trhov, ktorá je okolo 90 biliónov USD, je trh s kryptomenami stále príliš malý, avšak nie zanedbateľný. Celosvetové rizikové investície do blokchainu a start-upov podporujúcich blokchain podniky (okrem ICO- Initial coin offerings) v prvých šiestich mesiacoch roka 2018 vzrástli oproti rovnakému obdobiu roku 2017 o takmer 400%, čo predstavuje 1,3 miliardy USD (Rowley, 2018). Ekosystém Blockchain sa buduje vďaka pokroku v oblastiach uvedených v tabuľke 3.

Tabuľka 3: Predpoklady a východiská pre budovanie ekosystému blockchain.

IT hardvér a zdroje energie pre ťažbu virtuálnej meny	Cezhraničné prevody	Digitálne médiá
Medzibankové platobné systémy	Záznamy verejnej správy	Cloud- služby
Zúčtovanie a úhrady na finančných trhoch	Národné systémy OP	Integrácia Internetu vecí
Migrácia záznamov nehnuteľností	E-záznamy zdravotníctva	
IT služby pre presun existujúcich systémov do blokchainu	IT bezpečnostné systémy a služby	

Zdroj: Spracované podľa zdroja (Royal Bank of Canada, 2018)

Stav poznatkov v súčasnej literatúre

V roku 1992 Timothy May uverejnil svoj „Crypto Anarchist Manifesto“, parafrázujúci K. Marxa: „Strašidlo prenasleduje moderný svet, strašidlo kryptografickej anarchie“, ktorá za posledné desaťročie využíva metódy založené na šifrovaní transakcií pomocou verejného/vlastného kľúča, ich dešifrovaní príjemcom, na softvérových protokoloch pre interakciu, autentifikáciu a overovanie. Technológie Blockchain a kryptomeny, ako napríklad Bitcoin, Litecoin a Ethereum v posledných rokoch sú významným objektom skúmania. Bitcoin je najvýznamnejším príkladom kryptomeny založenej na systéme blockchain, hodnoty Bitcoin transakcií, zaznamenané v roku 2018, boli druhé najvyššie na svete doteraz 1,3 miliardy dolárov, čo je viac ako spoločnosť PayPal ale menej ako spoločnosť Visa. (Rowley, 2018).

Z hľadiska globálnej regulácie neexistuje jednotná, normalizovaná terminológia pre túto technológiu. Rôzne inštitúcie odvodzujú svoje vlastné definície. Novoprijatý zákon č.213/2018 Z.z. O poistnej dani na Slovensku určuje, ako oceniť virtuálnu menu, prepočítať a vykázať zisk z predaja alebo výmeny, ale nedefinuje virtuálnu menu, virtuálna mena sa klasifikuje ako obchodovateľný cenný papier t.j. kategória krátkodobého finančného majetku alebo nehmotný majetok. EBA definuje virtuálnu menu ako digitálnu reprezentáciu hodnoty, ktorá nie je vydaná centrálnou bankou alebo verejným orgánom, ani nevyhnutne spojená s fiat-menou, ale je akceptovaná fyzickými alebo právnickými osobami ako prostriedok výmeny a môže byť prevedená, uložená alebo obchodovaná elektronicky (EBA, 2014). ECB definuje virtuálnu menu ako typ neregulovaných, digitálnych peňazí, ktoré vydávajú a zvyčajne kontrolujú ich vývojári a používajú a prijímajú členovia konkrétnej virtuálnej komunity. (ECB, 2016) Tradičná definícia charakterizuje menu tromi hlavnými črtami: (i) slúži ako prostriedok výmeny, (ii) používa sa ako účtovná jednotka a (iii) umožňuje ukladať hodnotu, čo je v súčasnosti východisko pre definovanie virtuálnej meny. Použitie virtuálnej meny v súčasnosti ako platobného prostriedku je obmedzené, v dnešnej dobe je zatiaľ akceptovaná limitovaných počtom podnikov či podnikateľov na realizáciu platieb. Na to, aby bola mena uznaná za peniaze, Sysáková a Šlahor (2010) tvrdia, že mena musí spĺňať nasledujúce 3 funkcie:

1. musí to byť prostriedok, ktorý uchováva hodnotu (ne stráca hodnotu v čase),
2. je ľahko prenosný, teda funguje ako prostriedok výmeny, a
3. predstavuje zúčtovaciu jednotku (umožňujúcu porovnávanie cien tovarov a služieb).

Virtuálna mena je definovaná medzivládnu a jednou z najvplyvnejších finančných organizácií, ktorou je Finančná akčná skupina (FATF, 2014) ako digitálna reprezentácia hodnoty, ktorú možno digitálne obchodovať so spomínanými tromi klasickými tradičnými funkciami, ale nemá štatút zákonného platidla v žiadnej jurisdikcii. Peniaze vždy znamenali politickú moc v ekonomickej histórii sveta. Počnúc najdrahšími kovmi na razenie mincí, neskôr peniaze vytlačené v papierových bankovkách, spájajúce ich hodnotu s množstvom zlata v trezore centrálnej banky, spĺňali definíciu meny. Popularita používania elektronických peňazí v súčasnosti rastie, elektronické peniaze sú širším pojmom pre všetky peniaze, meny alebo majetok, ktoré nemajú fyzickú podstatu - môžu zahŕňať reprezentácie suverénnej meny alebo pohľadávky v reálnom svete. Štáty využívajú svoju politickú moc na reguláciu používania mien a určia jednu menu (zvyčajne tú, ktorú vydal štát) ako zákonné platidlo za záväzky na svojom území (Bariviera et al., 2017). Digitálne a virtuálne meny môžu byť buď centralizované alebo decentralizované. Centralizovaná mena je akákoľvek mena, ktorú vydáva a riadi centrálna skupina alebo organizácia (napr. ECB), na rozdiel od decentralizovanej meny.

Virtuálna mena sa odlišuje od fiat meny (skutočné peniaze alebo národná mena), t.j. mince a papierové peniaze krajiny, ktorá je určená ako jej zákonné platidlo. Odlišuje sa však aj od elektronických peňazí (digitálna reprezentácia meny fiat). Digitálna mena je digitálna reprezentácia virtuálnej meny (non-fiat) alebo e-money (fiat) a často sa zamieňa s pojmom „virtuálna mena“. Kryptomena predstavuje decentralizovanú virtuálnu menu na matematickom základe, ktorá je chránená kryptografiou (FATF, 2014). Bitcoin je digitálna mena bez centrálného

vydávajúceho orgánu alebo fyzickej formy, t.j. bitcoin je kryptomena, je podmnožinou digitálnych mien, ktoré používajú kryptografické techniky na riadenie šifrovacích protokolov, ktoré identifikujú vlastníctvo a overujú detaily transakcií. Protokol šifrovania bitcoinu jednoznačne identifikuje každý bitcoin v rámci ekonomiky Bitcoin. Každý vytiažený bitcoin alebo jeho zlomok môže byť predaný, použitý na platenie za nákupy a držaný ako investícia pre budúci predaj. Na zápis do blockchain databázy nie je požadovaný žiaden centrálny úrad, len ekvivalent čísla účtu príjemcu platby a súkromný kľúč majiteľa bitcoinov.

Tabuľka 4: Virtuálna mena

Elektronické peniaze – E – peniaze (E-money)			
Digitálna mena je digitálna reprezentácia z nasledujúcich dvoch mien, nazývaných:			
Fiat mena		Virtuálna mena (VM)	
Fiat mena (skutočné peniaze) Reálne peniaze, národná mena		Digitálna mena Centrálnej banky (CBDC)	Non-fiat mena (peniaze)
Centralizovaná			Decentralizovaná
Fiat peniaze – papierové peniaze, bankovky, mince“ – zákonné platidlo” oficiálne používaná mena v krajine	E-zlato	Kryptomena Centrálnej banky napr. Sovereign “SOV” (Marshall Islands), “Petro” (Venezuela)- CBCC	Kryptomena na matematickom základe, konvertibilná VM - Bitcoin

Zdroj: spracované autorom

Výskum v tejto oblasti sa rozbehol a naliehavou otázkou je, ako by sa v novovznikajúcom ekosystéme blockchain, ktorý súvisí s rozhodovaním o investíciách, stanovili ceny kryptomien. Dramatické cenové výkyvy na burzových trhoch v Bitcoine vyústili do rozsiahlych diskusií a pochybností (Li, Wang, 2016). Pieters a Vivanco (2017) tvrdia, že Bitcoin je homogénny, virtuálny tovar, úplne identický na všetkých online trhoch, na ktorých sa obchoduje. S Bitcoinom sa obchoduje na webových stránkach známych ako bitcoinové burzy, všetky nezávisle prevádzkované a prístupné non-stop globálnej klientele, s cenovými údajmi dostupnými okamžite a bezplatne komukoľvek na svete s prístupom na internet. Napriek týmto vlastnostiam zistíme, že ceny bitcoinov sa na trhoch líšia; nie všetky burzy dodržiavajú zákon jednej ceny (LOOP) - teóriu, že rovnaký tovar by sa mal predávať za identické ceny po zväžení nákladov s obchodovaním. Môže sa to zdať prekvapujúce, že úplne virtuálny tovar by si mohol udržiavať pozitívnu cenu. Dwyer (2015) ukázal, že tento jav vyplýva z obmedzenej dostupnosti a jedinečnej identifikácie každého bitcoinu. Luther (2016) vysvetľuje, že základným predpokladom dosiahnutia udržateľnej pozitívnej ceny sú nízke transakčné náklady. Halaburda a Gandal (2014) uvádzajú, že v počiatočnej etape je hodnota kryptomeny (napr. Bitcoin) určená konkurenciou s inými kryptomenami. To vytvára volatilitu v jej počiatočnej cene, ale neskôršie cenové správanie u kryptomien je v súlade s behaviorálnym aspektom finančného aktíva. Glaser a kol. (2014) zistili,

že správanie spotrebiteľov je v súlade s používaním Bitcoinu ako investičného nástroja. Brière et al. (2015) poukazujú, že na investičné účely Bitcoin je majetok, ktorý možno efektívne využiť na diverzifikáciu. Obchodovanie s bitcoinom sa považuje za paralelu obchodovania s tovarom odkedy maloobchodníci, vrátane obchodníkov Amazon, Windows, Dell, Overstock a darčkových kariet - začali akceptovať kryptomenu Bitcoin ako spôsob platby, hoci nie všetci používajú rovnakú metódu. Napríklad, spoločnosť Dell prijíma priame platby Bitcoinom, Amazon namiesto toho poskytuje digitálne darčkové karty, ktoré možno zakúpiť s bitcoinom a potom použiť na nákup tovaru na ich webových stránkach. Hoci rastúci počet dodávateľov akceptuje bitcoin, Ali et al. (2014) dospeli k záveru, že digitálne meny, ako napríklad Bitcoin, v súčasnosti nemajú dostatok používateľov, aby vystupovali ako všeobecná alternatíva pre nákupovanie (myslí sa na úhrady ako používanie fiat meny).

Ciele a metodológia

Výskumným objektom v centre pozornosti je virtuálna mena z pohľadu globálneho vývoja v posledných rokoch. Cieľom vedeckej štúdie je skúmať pojmovologicky obsah a základnú terminológiu a monitorovať problematické oblasti kryptomeny, najmä proces regulácie virtuálnych mien. Štúdia skúma regulačné dôsledky v Európe, a to tak v členských štátoch Európskej únie, ako aj v európskych nečlenských štátoch, analyzuje súčasnú situáciu a skúma možnosti Európskej únie pri jej implementácii. V kapitole sme použili vedecký prístup zmiešaných metód (syntéza, dedukcia, analýza, porovnanie) nazývaný sekvenčný vysvetľujúci návrh, v ktorom sa najprv spracúvajú kvantitatívne poznatky, teoretické východiská a potom nasleduje zber, analýza kvalitatívnych údajov umožňujúcich dôkladnejšiu interpretáciu dát.

Identifikácia hlavných problémov

Nie je zatiaľ jednoznačne určené, ako klasifikovať virtuálnu menu alebo kryptomeny v členských štátoch EÚ, takže spoločné definovanie virtuálnej meny je celosvetový problém. Prekvapujúcim a mätúcim aspektom virtuálnej meny je neustále pokračujúca rôznorodosť tvorby pomenovaní virtuálnej meny alebo kryptomien, ako napríklad krypto-aktívum, digitálna mena, virtuálna komodita, krypto-token, platobný tok, kybernetická mena, elektronická mena, virtuálny majetok, atď. Kryptomena je definovaná ako digitálna mena, ktorá využíva šifrovacie techniky na reguláciu tvorby menových jednotiek a na overovanie prevodu finančných prostriedkov, ktoré fungujú nezávisle od centrálnej banky. Keďže neexistuje jednotná klasifikácia virtuálnej meny v účtovníctve, objavuje sa ďalší problém, týkajúci sa otázok zdaňovania: virtuálna mena sa zdaňuje v rôznych krajinách rôzne, napr. zdaňovanie majetku, alebo finančných aktív, či cudzej meny. Virtuálna mena je predmetom dane z príjmov, či už vlastnená podnikmi (rôzne formy vlastníctva) dane sa platia z príjmov právnických osôb, fyzické osoby platia daň z príjmu, jednotlivci platia daň z kapitálových ziskov, čiže záleží u koho vo vlastníctve je virtuálna mena či kryptomena a ako je klasifikovaná.

Inštitúcie majú potenciál i povinnosť znížovať neistotu. Blockchain vytvára spoločnú realitu, ktorá umožňuje nedôveryhodným účastníkom overovať si a monitorovať svoje procesy bez pomoci úradov či inštitúcií, ktoré môžu byť nadbytočné. Vzniká ako interakcia viacerých faktorov,

ako je zvýšenie rýchlosti centrálnych procesorov (CPU), zníženie nákladov na ukladanie dát, vývoj kryptografie a kódovania. Blockchain databáza je špecifický druh zdieľanej knihy účtov „distributed ledger“ je databáza, ktorá je navrhnutá aby zaznamenala konečný počet transakcií a digitálne interakcie. So záznamami, akonáhle sú uložené, nemožno manipulovať bez zanechania stopy. Ich používanie by malo priniesť transparentnosť, efektívnosť, hospodárnosť a bezpečnosť pre podniky. Tieto vlastnosti sú nutné pre zabezpečenie dôvery, vystopovateľnosti a bezpečnosti v systémoch, kde dochádza k výmene dát a aktív. Blockchain identifikoval aj problémy súvisiace s jeho implementáciou a použitím, pri implementácii priemyslu 4.0 do praxe, ako je rozpracované v nasledujúcom texte.

a) Problémy škálovateľnosti (priepustnosť, latencia, kapacita a šírka pásma siete)

Priepustnosť- bitcoinová sieť spracováva v priemere len 1 transakciu za sekundu (tps) s teoretickým maximom 7 tps. Táto priepustnosť je neprijateľne nízka v porovnaní s počtom transakcií spracovaných spoločnosťou Visa (2 000 tps, typická hodnota 10 000 tps), siete Twitter (typická 5 000 tps, 15 000 tps), reklamných sietí (500 000 tps typických), obchodných sietí alebo e-mailových sietí (globálny objem e-mailov je 183 miliárd e-mailov / deň alebo 2 100 000 tps).

Latencia - každý blok na bloku bitcoinov trvá 10 minút. Pre porovnanie, transakcia v sieti Visa je schválená najviac v sekundách. Mnohé finančné aplikácie potrebujú latenciu 30 až 100 ms.

Kapacita a sieťové pásmo - blok Bitcoin je asi 185 GB. Stiahnutie celého blockchainu trvá už takmer deň. Ak by sa priepustnosť zvýšila o 2 000 na úroveň Visa, dodatočné transakcie by viedli k rastu databázy o 3,9 GB/deň alebo o 1,42 PB/rok. Pri 150 000 tps by blockchain narástol o 214 PB/rok (petabytes). (BitcoinEnergyConsumption.com, 2018).

b) Spotreba energie

Európsky parlament vo svojom uznesení z 3. októbra 2018 (P8_TA-PROV (2018) 0373) zdôraznil energeticky a environmentálne priaznivé projektované aplikácie, napr. zdôrazňuje možnosť podpory DLT pre elektrifikáciu chudobných vidieckych komunít, benefitujúc z alternatívnych platieb a mechanizmov dotácií, DLT môže pomôcť produkovať a konzumovať zelenú energiu, mohli by sa vytvoriť alternatívy k štátom podporovaným investičným programom do obnoviteľných zdrojov energie. Nikto však neprepočítal odhad spotreby energie DLT, ak by sa vykonali všetky aplikácie uvedené v uznesení. Spotreba energie vyžadovaná technológiou blockchain je enormná, technologický pokrok pokračuje a očakáva sa, že problémy so škálovateľnosťou budú vyriešené a vylepšené.

Zaujímavé informácie sú uvedené v tabuľke 5 týkajúcej sa energetických záležitostí.

Tabuľka 5: Bitcoin a spotreba energie

Súčasná odhadovaná ročná spotreba elektrickej energie Bitcoinu (TWh)	73,12 TWh
Súčasná minimálna ročná spotreba elektrickej energie Bitcoinu (TWh)	58,01 TWh
Ročné globálne výnosy z ťažby	\$4 716 318 065
Ročné odhadované globálne náklady na ťažbu sú	\$3 656 073 069
Percento aktuálnych nákladov	77,52%
Krajina najbližšia k Bitcoinu z hľadiska spotreby elektrickej energie	Rakúsko
Predpokladaná spotreba elektriny za predchádzajúci deň (KWh)	200 332 771 KWh
Implikované wattly na GH /s (Implied Watts per GH/s)	0,145 W/ na GH/s
Celková sieťová rýchlosť (Hashrate) v PH/s (1,000,000 GH/s)	57 391 PH/s
Spotreba elektriny na transakciu (KWh)	783 KWh na transakciu
Počet domácností v USA, ktoré by mohli byť na jeden deň poháňané elektrinou spotrebovanou na jednu transakciu	26,47 US domácností
Spotreba elektrickej energie Bitcoinu ako percento svetovej spotreby elektrickej energie	0,33%
Ročná uhlíková stopa (kt CO ₂)	35 830
Uhlíková stopa na transakciu (kg CO ₂ /1 transakcia)	383,84kg /1transakciu

Zdroj: <https://digiconomist.net/bitcoin-energy-consumption>

c) Nedostatok regulácie, štandardov a foriem certifikácií, nejasné právne otázky

Nedostatočná regulácia - hlavnými prekážkami implementácie technológie blockchain sú regulačné obmedzenia (56%), potom nezrelá technológia, nedostatok jasnej návratnosti investícií, nedostatočné zručnosti pracovnej sily, nedostatočná výkonnosť a skúsenosti exekutívy v danej oblasti. (IBM, 2017). Regulácia na celom svete sa snaží udržať krok s touto novou technológiou. Hlavnou prekážkou pre ďalšiu implementáciu DLT zostáva pretrvávajúce nejasné regulačné prostredie. Právne riziká sú kľúčovými inhibítormi všetkých účastníkov ekosystému DLT (vývojári aplikácií, operátori), pričom poskytovatelia infraštruktúry sú na treťom mieste. (Hileman, Rauchs, 2017). DLT využíva najmä finančný sektor (30% bankovníctvo a financie, 13% vláda, 12% poistenie), napr. 72% bánk, 56% spoločností FinTech, 47% poisťovní testovali a snažili sa aplikovať DLT.

d) Otázky bezpečnosti

Všetci aktéri používajúci DLT sa venujú otázkam bezpečnosti danej technológie. Subjekty z verejného sektora, centrálné banky, vládne agentúry, rôzne regulačné orgány sú v úplne novej situácii v histórii, pretože vládne bezpečnostné agentúry môžu monitorovať, ale aj oni sami môžu byť monitorovaní. Môže byť dôvera založená na matematických modeloch? Kryptografia tiež vyvíja zlepšenie spoľahlivosti kryptografie, ale absolútna bezpečnosť nemôže existovať. Hacking súkromných kľúčov je pre tento systém kľúčovou výzvou. Prijemcami budú tí, ktorí najlepšie zvládnu kryptografiu. Tí, ktorí majú kontrolu nad obrovskými dátovými centrami, majú

kontrolu nad informáciami. Ak sa informácie využijú nekontrolovateľným spôsobom, koncentrácia moci z titulu vlastníctva množstva informácií môže viesť ku katastrofe.

e) Sociálno-ekonomické dôsledky

Sociálno-ekonomické dôsledky - pokrok v technológii blockchainu pri realizácii prináša revolučné zmeny v mnohých sektoroch - napríklad: a) bankový a finančný sektor (prevod peňazí, poskytovanie peer-to-peer pôžičiek, prevod cenných papierov), poistenie (automatické plnenie zmlúv) , b) vládny sektor (správa občianskych preukazov, daňové správy, riadenie štátnej pomoci, riadenie rozvojovej pomoci, elektronické hlasovanie, dodržiavanie predpisov), c) vzdelávanie - posilnenie a inovácia študijných programov, podpora vzdelávania smerom k modernej technológii DLT a kryptomene v spolupráci s reálnymi podnikmi, d) rezort zdravotníctva by mal mať prospech zo sledovania transakcií týkajúcich sa zdravotných záznamov pacientov a identifikácie prístupu, e) médiá a oblasť duševného vlastníctva (priama distribúcia hudby, videí alebo iného obsahu). Blockchain sa už používa v mnohých sektoroch - bankovníctve a financiách (30%), vládnych a verejných statkoch (13%), poistení (12%), zdravotníctve (8%), médiách, zábave a hrách (8%), v generických službách (6%), technologických službách (6%), odborných službách (4%), energetike a verejných službách (3%), priemyselnej výrobe (3%) a iných (7%). Benefity sú prospešnosť pre ľudí a spoločnosť a zabránenie zneužívania vykonávania transakcií amorálnymi ľuďmi pre vlastnú prosperitu. Vyriešenie týchto fundamentálnych princípov pre úspech aplikácie blockchainu je výzvou pre budúcnosť. (WEF, 2015)

Výsledky a diskusia

Inštitúcie EÚ zdôrazňujú problémy pri riešení otázok regulácie. Uznesenie Európskeho parlamentu z 3. októbra 2018 o distribuovaných technológiách a blockchain technológii: budovanie dôvery cez sprostredkovanie (2017/2772 (RSP)) nabáda Komisiu a príslušné kompetentné vnútroštátne orgány k budovaniu a posilneniu technických odborných znalostí a regulačných kapacít, ktoré umožnia tvorbu rýchlych legislatívnych alebo regulačných opatrení. Zdôrazňuje vyhodnotenie a rozvoj európskeho právneho rámca. EP vidí potenciál technológie blockchain pri zavádzaní do praxe. Navyše, môže zabezpečiť koncepčný rámec transparentnosti, redukovať korupciu, odhaľovať daňové úniky, umožniť sledovanie nezákonných platieb, uľahčiť procedúry proti praniu špinavých peňazí a odhaľovať spreneveru majetku, podporuje pseudonymizáciu používateľov, ale nie ich anonymizáciu. Vo finančnom sektore existujú možnosti začlenenia kryptomien do európskeho platobného systému.

Tabuľka 6: Postoje Inštitúcií Európskej Únie

ECB je zodpovedná za vykonávanie menovej politiky pre EMU	Európska komisia (EK) výkonný orgán EÚ zodpovedný za vykonávanie rozhodnutí Európskeho parlamentu a Rady	Európska autorita pre bankovníctvo (The European Banking Authority - EBA) nezávislý orgán EÚ
A. ECB odmieta: 1. zavedenie národných kryptomien 2. Členské štáty EÚ zavádzajú svoju vlastnú menu namiesto eura 3. kryptomeny ako spôsob platby B. Nemá žiadnu právu moc regulovať kryptomeny C. Skúma vplyv krypto-meny na hospodárstvo ² .	Blockchain je jednou z prelomových technológií s veľkým potenciálnym vplyvom vo finančnom sektore atď. 1. Pomoc EK pri podpore nebankového financovania, t.j. FinTech spoločnosťami, prostredníctvom legislatívnych opatrení v rámci iniciatívy: Únia kapitálových trhov Úloha Observatória EU Blockchainu prostredníctvom tendra: 2. zmapovať a monitorovať vývoj 3. budovať odborné znalosti 4. propagovať už zrealizované prípady	Funkcie EBA ³ : 1. zabezpečenie účinnej a konzistentnej obozretnej regulácie a dohľadu v bankovom sektore v Európe. 2. vytvorenie európskeho súboru jednotných pravidiel pre bankovníctvo - European Single Rulebook : harmonizované pravidlá obozretného podnikania pre finančné inštitúcie v celej EÚ.

Zdroj: Spracované autorom

EBA navrhuje vytvorenie subjektu, ktorý sa bude zodpovedať regulátorovi. Nutnou požiadavkou pre schému virtuálnej meny je jej regulácia ako finančnej služby a možnosť spolupracovať s existujúcimi regulovanými finančnými službami. Subjekt by sa nazýval Úrad (autorita) riadenia systému, ktorý je mimovládny subjektom, ktorý vytvára a riadi pravidlá používania konkrétnej schémy virtuálnej meny (EBA, 2014), inými slovami centrálna banka pod iným menom. Niektoré európske centrálné banky zareagovali negatívne, napríklad francúzska centrálna banka, Banque de France (BdF). Predpovedajú riziká spojené so vznikom virtuálnych mien: príklad bitcoinov. Definujú bitcoin ako neregulovanú virtuálnu menu, ktorá je navrhnutá ako alternatíva k oficiálnym menám, ale bez záruky kompenzácie. Nemôže byť klasifikovaná ako zákonné platidlo, keďže momentálne platí, že každý obchodník môže bitcoin odmietnuť ako platbu „, bitcoin považujú v podstate za špekulatívny koncept“ (Banque de France, 2013).

² Draghiho reakcia na projekt e-peňazí Estónska na spustenie národnej kryptomeny nazwanej „estcoin“ (September 2017)

³ v roku 2014 EBA zverejnila prvé analytické stanovisko o virtuálnych menách (VC), v ktorom definuje 89 rôznych rizík a ich 20 možných príčin rozdelených do 13 kategórií.

Tabuľka 7: Postoje Inštitúcií mimo Európskej Únie

MF	Vedúca úloha USA pri formovaní úverových, dozorných a poradenských operácií MMF. A. dozorná funkcia dohliadajúca na medzinárodný menový systém a monitorovanie hospodárskej a finančnej politiky členských krajín; B. nevykonateľná bez dôveryhodných inštitúcií. Mrs. Lagarde, výkonná riaditeľka MMF, uznáva, že technológia nepozná hranice, jednotlivci a komunity majú schopnosť formovať technologickú a ekonomickú budúcnosť, ktorá funguje pre všetkých. Vyslovila aj skepticizmus v akom rozsahu sa dá DLT využiť vo finančnom sektore. (Lagarde 2017). Rok neskôr Lagarde zdôraznila na stretnutí v Singapore, že štáty budú musieť premýšľať nad vydaním digitálnych mien centrálnych bánk. (Lagarde, November 2018, jej prejav in Singapore)
IS	The Bank for International Settlements - Banka pre medzinárodné zúčtovanie - organizácia centrálnych bánk, medzinárodná finančná inštitúcia, vlastnená centrálnymi bankami (60-členov) zastupujúcimi krajiny na celom svete, ktoré spolu tvoria cca 95% svetového HDP.

Zdroj: spracované autorom

BIS je významnou inštitúciou s vysokým stupňom diskurzívnej sily a regulačného vplyvu. Vo svojom Quarterly Review uverejnenom v septembri 2017 autori v spojitosti s kryptomenami centrálnych bánk (CBCC) nadnášajú do diskusie problém, či by centrálna banka mala poskytovať digitálnu alternatívu k hotovosti, obzvlášť je to naliehavá otázka v krajinách, ako napr. Švédsko, kde používanie hotovosti rýchle klesá. Všetky centrálné banky sa budú musieť rozhodnúť, či má zmysel emitovať kryptomenu CBCC pre vlastné potreby. (Bech, Garratt, 2017). Národné kryptomeny centrálnych bánk by mohli predstavovať isté riešenie blockchainovej vlny.

Finančné technológie predstavujú inovácie finančného sektora, konkurujú tradičným finančným inštitúciám pri poskytovaní finančných služieb pomocou nových technológií. FinTech v spojitosti s rýchlym progresom digitálnych technológií môže predstavovať pre tradičné podniky obrovskú hrozbu alebo naopak veľký prínos. Aj RegTech patrí k FinTech spoločnostiam s cieľom rozvíjať regulácie. Regulačné koncepcie, ktoré podporovali vývoj viacerých foriem FinTech, najmä RegTech boli: AML (pranie špinavých peňazí), KYC (poznaj svojho zákazníka), GDPR, MiFID II (smernica o trhoch s finančnými derivátmi), Bazilej III (na posilnenie regulácie, dohľadu a riadenia rizík Basel III - pravidlá kapitálovej primeranosti (pilier I a II, kapitálové rezervy cenných papierov, riadenie rizika a požiadavky na likviditu), Solventnosť II (smernica regulujúca podnikanie v poisťovníctve - riadenie rizík, dohľad a reporting) a AIFMD (smernica o riadení alternatívnych investícií) fondy, harmonizovaný režim pre fondy kolektívneho investovania). Regulácia ICO t.j. "Initial coin offerings" (vstup určitej meny na obchodovanie na burze) zaostáva, pretože otvoreným problémom je určenie či emisie cenných papierov sa realizuje na ICO, problém s definovaním virtuálnej meny vyvstáva opäť. FCA - Financial Conduct Authority (UK) používa RegTech, ktorá definuje RegTech ako podmnožinu FinTech, ktorá sa zameriava na technológie umožňujúce uľahčenie efektívnejšieho dopracovania regulačných požiadaviek v porovnaní s existujúcimi možnosťami. (FCA, 2016)

EÚ je aktívna pri podpore a uzákonení opatrení na podporu aj fintech spoločností, ktoré predstavujú konkurenciu pre bankový sektor. PSD2 - Smernica o platobných službách² je smernica Európskej Komisie na reguláciu platobných služieb a poskytovateľov platobných služieb

v celej Európskej únii a Európskom hospodárskom priestore. PSD2 umožňuje bankovým zákazníkom, spotrebiteľom aj podnikom, využívať na riadenie svojich financií poskytovateľov služieb od tretích strán. Platby môžu vykonávať iné tretie strany a majúce vlastné peniaze bezpečne umiestnené na vlastnom bežnom bankovom účte. Banky sú však povinné poskytnúť týmto nebankovým poskytovateľom finančných služieb prístup k bankovým klientom prostredníctvom otvorených rozhraní API (rozhranie aplikačného programu). To im umožní ponúkať finančné služby nad rámec údajov a infraštruktúry bánk. Európska komisia sa usiluje o rozšírenie inovácií, ochranu zákazníkov posilnením právnych predpisov a zlepšenie bezpečnosti internetových platieb a prístupu na účet v rámci EÚ a EHP. Uvádza do finančnej oblasti nových aktérov: PISP (Poskytovateľ platobných iniciačných služieb) a AISP (Poskytovateľ informačnej služby). PSD2 zvyšuje konkurenciu na platobnom trhu, čo by malo priniesť výhody pre spotrebiteľa. Riadenie účtov platieb pre tretie strany je regulované a kontrolované, aby sa obmedzilo riziko pre spotrebiteľov a vytvorila sa dôvera voči týmto službám. (Deloitte, 2018)

Trh a kryptoburzy na trhu s kryptomenou

Krypto-menový trh, hoci ešte nie je bežný, nemožno považovať za nedostatočne rozvinutú, vzdialenú platformu, od 1. novembra 2017 bolo na 6319 trhoch 1244 kryptomien. Cena Bitcoinu dosiahla 6512,44 USD, teraz sa pohybuje na hodnote okolo 5000 USD za bitcoin V roku 2017 boli v priemere 248K denné transakcie, bitcoinová trhovú kapitalizácia / (cena 1,0 BTC) x (celkové bitcoiny v obehu) / 184 mld. s dominantným postavením na trhu 58,7% (coinmarketcap, 2017).

Pozoruhodná je aj dostupnosť pre každodenné použitie vyjadrená v počte bankomatov na bitcoiny. Dňa 1. januára 2014 bolo 5 ATMs, o rok neskôr 328 bankomatov, na konci roka 2016 už 505 a od 20. októbra 2017 to bolo 1,680 - 31,34% z nich sú obojsmerné (mince, bankomaty a radary). Na súčasnom zozname je 32 vstupov na burzu s kryptomenami (ďalej len ICO). Iba v roku 2017 bolo prostredníctvom ICO (Initial coin offerings) získaných o 1 962 mld. USD viac v porovnaní s rokom 2016 (62 mil. USD) (Icwatchlist, 2017). Kryptomena prekonala každú štátnu menu a takmer každú komoditu. V súčasnosti bitcoin vstupuje na etablované trhy futurít - Chicago Mercantile Exchange a Chicago Board of Trade, popredný svetový trh s derivátmi (CME Group), oznámili, že uvedú na trh futurity na bitcoin. Bitcoin sa má stať novou triedou aktív. (Chicago Mercantile Exchange, 2017). Viac ako 1 000 aktív je už obchodovateľných na trhu s kryptomenami.

Obchody na burze s kryptomenami poznamenali aj početné negatívne udalosti- krádeže bitcoinov, nedostatočné overovania, žiadne bezpečnostné vklady, komplikované transakcie s fiat menou, cenová manipulácia, beh predom (prax, ktorá spočíva v zadávaní objednávok predtým, ako niekto iný to urobí na základe pokročilých znalostí o ich transakciách), netransparentná tvorba cien, problém latencie (obchodníci s dobrými kontaktmi mohli vidieť objednávky objednávok okamžite a tak reagovať bezodkladne). (News BTC 2017). Existujúce burzy kryptomien nie sú regulované. Tieto problémy boli riešené v poslednej dobe technicky aj prakticky na Legolas Exchange, burza s kryptomenou, ktorej protokol obsahuje decentralizovanú účtovnú knihu v rámci svojej vlastnej centralizovanej platformy s cieľom neutralizovať praktiky „beh predom“, zaručiť

nemennosť, časovú presnosť a transparentnosť knihy objednávok a zabezpečiť spravodlivé prostredie pre bezpečné a spoľahlivé obchody.

FinTech sú konkurenciou pre finančný a bankový sektor v oblasti služieb zákazníkom. Chatboty podporované umelou inteligenciou AI, ktoré redukujú náklady na zamestnancov a vybavujú väčšie množstvo požiadaviek oveľa rýchlejšie predstavujú inovácie pre interakcie zákazníkov s finančnými spoločnosťami. Internet banking je sofistikovanejší. Prístup k bankovým účtom umožňujú telefóny, počítače a tablety. Progres AI umožnil odhaliť a identifikovať podvodné transakcie robotom, a to prehliadaním histórie transakcií obete a výpočtom pravdepodobnosti podvodu na základe predchádzajúcich modelov. K identifikácii zákazníka cez telefón slúži hlasová biometria a celkovo bio-metrická bezpečnosť sa každým rokom posúva na novú úroveň.

Zhrnutie

Na základe monitorovania vývoja kryptomien uskutočňovaných Európskou centrálnou bankou a Radou pre finančnú stabilitu (FSB) v priebehu roka 2018, Európska komisia posúdi potrebu regulačných opatrení na úrovni EÚ. EK ďalej žiada o prevádzkovanie inovačných centier, regulačných priestorov a šírenie informácií o inovačných technológiách. Dokument osobitne rieši otázku potenciálu technológie blockchain a jeho zavedenia do finančného sektora. Komisia EÚ bude hostovať laboratórium EÚ FinTech Lab, v ktorom sa bude uskutočňovať spolupráca medzi poskytovateľmi technologických riešení a európskymi orgánmi. Akčný plán predstavuje kombináciu podporných opatrení pri zavádzaní riešení FinTech a proaktívnych opatrení, ktoré majú za úlohu stimulovať tvorbu nových riešení a riešiť vznikajúce riziká. Prístup britskej agentúry FCA (Financial Conduct Authority) zdôrazňuje podporu spoločnostiam FinTech prostredníctvom jej inovačného centra Hub alebo regulačného prostredia (testovacie prostredie, v ktorom môžu inovatívne spoločnosti testovať svoje obchodné modely bez splnenia regulačných požiadaviek - zníženie nákladov na zavedenie inovatívnych nápadov, jednoduchší prístup k financiam, možnosť uvedenia inovatívnejšieho testovania a produktov na trh, spolupráca regulátora s inovátorom a zabezpečenie ochrany zákazníkov. Mnohé centrálné banky robia experimenty s technickými riešeniami na základe blockchainu (Hilleman a Rauch, 2017) 82% centrálnych bánk plánuje zaviesť vlastnú digitálnu menu centrálnej (národnej) banky a 52% centrálnych bánk plánuje použiť blockchain na platby, ktorých činnosť by mala byť koordinovaná s MMF s cieľom vytvoriť riešenia na jednotnom právnom základe. Lídrami v oblasti FinTech v strednej Európe sú Česká Republika spolu s Poľskom. Zisk vygenerovaný FinTech spoločnosťami v Čechách v roku 2017 sa odhaduje v rozmedzí 400 - 800 mld. českých korún, pričom jeho potenciálny zisk v budúcnosti môže dosahovať 5 - 15 mld. českých korún. Dopyt po FinTech rapídne stúpa, pretože pre spotrebiteľov predstavuje rýchlejšie a lacnejšie finančné služby bez zbytočnej administratívy. Medzi najväčšie FinTech trendy patria napríklad: Distributed Ledger, Blockchain, Kryptomeny, API (Application Programming Interface), AI (Artificial intelligence), Machine learning, Robo-Advisors, Big data, IoT (Internet of thing) a Biometrics.

Európsky kontinent je heterogénny, zjednotený len svojou spoločnou geografiou. To vedie k zložitému a zdĺhavému rozhodovaniu. Nové technológie môžu pomôcť nájsť spoločné riadenie a správu. Európska únia má obrovské perspektívy na začlenenie blockchain technológie do svojich

nariadení, praxe, hospodárstva, hoci čelí zvládnutiu hlavných problémov, ako je migračná kríza, finančná stabilita v ohrozených bankových systémoch. Prístup Švajčiarska k blockchainu je z pohľadu štátnych orgánov najinšpiratívnejším a hodným nasledovania. Je to reakcia štátu, ktorý dávno v minulosti rozpoznal moc peňazí, a teraz pokračuje vo svojej ceste k realizácii technologických novín skôr, ako iné krajiny získajú konkurenčnú výhodu. Je potrebné podporiť možnosti blockchain technológií zo strany štátu, namiesto dohľadu a potláčania a zákazov, je potrebné zriadiť konzorcia odborníkov, ktorí zabezpečia technickú základňu a predpisy zahŕňajúce všetky zainteresované strany založené na modeli rozdelenia moci podľa Montesquieu“ „nikto neverí nikomu, ale všetci sú informovaní“. To je odpoveď pre EÚ a konzervatívny svet, otvoriť sa vývoju, ale čo najrýchlejšie spracovať spoločné základy pre reguláciu blockchain technológie.

Appendix

Obrázok 1: Hlavné technológie formujúce finančné služby

Technológie		Finančné služby				
Základ	Inovácie	Platiť	Šetriť	Pôžičať si	Riadiť rizika	Radiť
Umelá inteligencia Big Data	Učiť sa pracovať s, obsluhovať stroje, technológiou/u Predikčná analýza		Investičné poradenstvo (roboty)			
				Rozhodnutia o úvere		
		Regtech, detekcia podvodov				
			Obchodovanie s aktívami			
Distributed computing	Distributed ledger Blockchain	Úhrady				
		B2B				
		Záložná kancelária				
		Digitálna mena				
Kryptografia	Chytré zmluvy Biometrika	Automatické transakcie				
		Bezpečnosť				
		Ochrana identity				
Prístup cez mobil Internet	APIs Digitálne peňaženky	Ľahko použiteľné digitálne peňaženky, finančný panel, P2P				
			Crowd-funding			
		Vnútorňa operatívnosť a expandovateľnosť				

Zdroj: IMF Staff

2.5 Digitálny humanizmus ako aktuálna výzva pre ďalší rozvoj a smerovanie Európskej únie

V súvislosti s digitálnym humanizmom je možné nájsť množstvo úvah o premene sveta okolo nás, sveta práce, ktorá z ľudí „sníme“ bremeno najťažších manuálnych úkonov a iných únavných činností, čím spoločnosť dospeje k zmenám v hodnotách. Vychádza nám z toho, že peniaze za prácu nebudú zohrávať až takú významnú úlohu, prvoradou bude zmysluplnosť činnosti v prospech priaznivého ľudského pokroku a vyššej kvality života. Predpokladá sa však, že aktuálne digitálne technológie ako napríklad umelá inteligencia, sa stanú novým motorom ekonomického rastu a posilňovania konkurencieschopnosti. Je problematické odhadnúť, aké kompetencie budú potrebné napr. v roku 2025. Ako mimoriadne dôležitá sa aktuálne javí flexibilita edukačného systému a výrobných podnikov pre adekvátnu reakciu v okamihu, až bude jasné, aké znalosti a kompetencie budú naozaj potrebné, konštatujú Barnová – Krásna (2018 a,b,c).

Stratégia digitálnej transformácie Slovenska v kontexte digitálneho humanizmu

Stratégia digitálnej transformácie Slovenska (2018) je stratégiou pre správny vstup do jednotného digitálneho trhu a transformáciu Slovenska na úspešnú digitálnu krajinu, sformulovaná stratégia je prostriedkom pre úspešnú digitálnu transformáciu Slovenska. Stratégia digitálnej transformácie Slovenska je rámcovou vládnu stratégiou, ktorá definuje politiku a konkrétne priority v oblasti digitálnej agendy. Daná stratégia vychádza z priorit a aktuálnej agendy jednotného digitálneho trhu EÚ. Na národnej úrovni je cieľom akcelerovať naštartované procesy v rámci budovania digitálneho trhu a realizovať nové opatrenia a politiky, ktoré vychádzajú z najaktuálnejších priorit EÚ. Stratégia obsahuje akčný plán opatrení v krátkodobom (júl 2019 – jún 2022) a dlhodobom horizonte (júl 2022 – december 2030). Aby Slovensko výrazne pokročilo v implementácii jednotného digitálneho trhu, je nutné správne nastavenie legislatívnych, regulačných ako aj nelegislatívnych opatrení, ktoré odstránia bariéry v súčasnom zložitom prístupe na jednotný digitálny trh a akcelerujú tak rozvoj digitálnej ekonomiky s priamym vplyvom na občanov a podnikateľské prostredie.

Úrad podpredsedu vlády SR pre investície a informatizáciu (ÚPPVII) ako ústredný orgán štátnej správy pre oblasť informatizácie spoločnosti je z hľadiska tematickej a koncepcnej náplne svojich aktivít hlavným koordinátor tejto stratégie. ÚPPVII zodpovedá za prípravu, stanovenie priorit ako aj realizáciu stratégie v koordinácii a spolupráci s ďalšími ústrednými úradmi štátnej správy. Stratégia digitálnej transformácie Slovenska tak predstavuje nadrezortnú stratégiu pre pokračovanie a akcelerovanie už naštartovaných procesov formovania jednotného digitálneho trhu na Slovensku, ako aj pre identifikáciu nových opatrení a politík, ktoré vychádzajú z najaktuálnejších priorit Európskej únie a rovnako aj zo špecifických priorit a potrieb Slovenska. Cieľovou entitou tejto stratégie je občan a cieľovým účelom tejto stratégie je zlepšenie a zjednodušenie každodenného života všetkých občanov, obyvateľov a návštevníkov krajiny.

Okrem aktuálnych trendov v Európskej únii, sa stratégia inšpiruje globálnymi trendmi v digitálnej transformácii a prioritami kľúčového dokumentu Organizácie spojených národov

Agendy 2030 pre udržateľný rozvoj (2030 Agenda for the Sustainable Development). Stratégia tak dáva prvoradý dôraz na aktuálne digitálne technológie ako napríklad umelá inteligencia, ktoré sa stanú novým motorom ekonomického rastu a posilňovania konkurencieschopnosti. Zároveň sa stratégia inšpirovala digitálnymi stratégiami vyspelých krajín ako Francúzsko, Fínsko, Veľká Británia a Singapur.

Stratégia tiež analyzuje aktuálny východiskový stav na Slovensku. Vychádza z aktuálnej situácie, špecifických priorít a najdôležitejších potrieb digitálnej transformácie na Slovensku. Na tomto základe stratégia analyzuje aktuálny východiskový stav na Slovensku, z ktorého vyplynuli prioritné oblasti a opatrenia úspešnej digitálnej transformácie, ktorá by mala priniesť významnú pozitívnu zmenu pre občanov Slovenskej republiky, píše sa v Stratégii digitálnej transformácie Slovenska (2018). Aby bolo možné uskutočniť digitálnu transformáciu, je nevyhnutné správne identifikovať predpoklady, ktoré digitálnu transformáciu podmieňujú a určujú. Ako predpoklady („enablers“) úspešnej digitálnej transformácie autori Stratégie digitálnej transformácie Slovenska (2018) vnímajú vo všetkých oblastiach:

- ✓ Ľudský kapitál – digitálnu transformáciu dokáže realizovať a využiť len vzdelaná pracovná sila;
- ✓ Infraštruktúra – potrebné technológie, riešenia a systémy a
- ✓ Regulačný rámec, ktorý definuje pravidlá a spôsob fungovania.

Zámerom stratégie je vytvoriť priaznivé prostredie pre zavádzanie digitálnych inovácií do praxe v určených prioritných oblastiach. Stratégia preto stanovuje tri základné oblasti, kde štát potrebuje a dokáže mať výrazný úspech v krátkom čase a ktoré sa stali ťažiskovým základom *Akčného plánu digitálnej stratégie Slovenska 2019-2022*:

- ✓ Zlepšenie vzdelávania a zabezpečenie zamestnanosti a digitálnych zručností pre modernú dobu,
- ✓ vytvorenie základov pre moderné dátové a digitálne hospodárstvo,
- ✓ zlepšenie schopností verejnej správy využívať údaje a inovácie.

Zlepšenie vzdelávania a zabezpečenie digitálnych zručností a zamestnanosti pre modernú dobu

V rámci oblasti podpory vzdelávania a posilnenia digitálnych zručností stratégia definuje nasledovné opatrenia:

Vzdelávanie a digitálne zručnosti:

- ✓ Vypracujeme Analýzu stavu digitálnych zručností na Slovensku s návrhom konkrétnych opatrení,
- ✓ vytvoríme Národný štandard digitálnej gramotnosti pre občanov,
- ✓ vypracujeme Stratégiu a Akčný plán nasadenia smart vzdelávania a digitálnych zručností pre všetkých,
- ✓ zavedieme výučbu programovania a dátovej vedy už od základných škôl,
- ✓ podporíme digitalizáciu služieb vysokých škôl a univerzít,

- ✓ zvýšime podiel žien v IT a digitálnom sektore a odstránime rodové stereotypy,
- ✓ zriadime efektívny mechanizmus na boj proti dezinformáciám,
- ✓ otestujeme viaceré prístupy k efektívnemu šíreniu výukového materiálu pre rekvalifikáciu a digitálne zručnosti zamestnancov formou pilotných štúdií („trials“),
- ✓ zapojíme sa do celoeurópskeho vzdelávacieho a rekvalifikačného programu zamestnancov v digitálnej ekonomike,
- ✓ v základných a stredných škôl odskúšame účinnosť rôznych pilotných projektov na zlepšenie vzdelávania a jeho prispôsobenie digitálnej dobe (napr. adaptívne vzdelávanie),
- ✓ zavedieme pilotné projekty pre mentorovanie a rekvalifikáciu učiteľov základných a stredných škôl,
- ✓ odskúšame účinnosť inteligentných testovacích nástrojov a príbuzných projektov pre zlepšenie digitálnych zručností občanov.

Zamestnanosť:

- ✓ Zatraktívňime podmienky zamestnávania IKT špecialistov a iných odborníkov a mladých talentov do verejnej správy,
- ✓ výrazne zjednodušíme procesy pre zamestnávanie najlepších expertov zo zahraničia.

Jedným z cieľov Európskej únie je elektronická (digitálna) inklúzia (e-Inclusion) ako súčasť sociálnej inklúzie, ktorá sa dotýka aj edukácie všetkých vekových kategórií. Nakoľko vzdelávanie prostredníctvom digitálnych technológií nie je obmedzené priestorom, časom ani metódami a môže byť plne prispôbené jednotlivcom, vďaka nemu získavajú prístup k vzdelaniu rôzne skupiny obyvateľstva, ktorým doteraz špecifické okolnosti vzdelávanie sťažovali alebo neumožňovali vôbec, napr. z dôvodu veku, zdravotného znevýhodnenia, vzdelania, sociálnej situácie alebo geografickej polohy. Otvorené technológie všetkým jedincom umožňujú, aby sa vzdelávali, a to kdekoľvek, kedykoľvek, prostredníctvom akéhokoľvek zariadenia a s podporou kohokoľvek (EUR-lex, 2013).

Digitálny humanizmus ako aktuálna výzva pre ďalší rozvoj a smerovanie Európskej únie

Petty (2015) považuje za centrum záujmu digitálneho humanizmu človeka, použitie technológií takým spôsobom, aby ľudia mali možnosť dosahovať svoje ciele novými spôsobmi a realizovať to, čo doposiaľ nebolo možné. Skutočnú hodnotu digitálnych technológií vidí v tom, že pomáhajú užívateľom šetriť čas, ktorý by strávili triviálnymi, rutinnými alebo málo efektívnymi úlohami. Veľkou prednosťou digitálnych technológií je, že umožňujú rýchlo a efektívne vyhľadávať, analyzovať, tvoriť, komunikovať a využívať informácie v digitálnom priestore. Je potrebné zdôrazniť, že digitálny humanizmus je protipólom k snahám o mechanizáciu, automatizáciu procesov, smerujúcich k ich fungovaniu bez prítomnosti človeka. Ústrednou myšlienkou automatizácie je, že človek je nahraditeľný strojmi.

Efektívne využívanie digitálnych technológií v súlade s definíciou digitálneho humanizmu má potenciál zjednodušiť aj procesy v rámci vzdelávania. Jeho hlavnou výhodou je, že poskytuje príležitosť (často bezplatne) získavať rôzne informácie zo širokého spektra nezávislých zdrojov, a

to rýchlo a efektívne, čím sa znižuje informačná závislosť učiacich sa na učiteľovi. Digitálny priestor aj učiteľom umožňuje jednoducho celosvetovo komunikovať, zdieľať svoje skúsenosti s kolegami a ľahko vytvárať obsah vzdelávania. Súčasné trendy naznačujú, že budúcnosť a aj vzdelávanie v budúcnosti budú digitálne. Bolo by nezodpovedné používať digitálne technológie bez jasne stanovených pravidiel. Preto je potrebné už teraz vymedziť princípy digitálnej humanistickej pedagogiky, predstavujúcej prienik medzi digitálnym humanizmom a digitálnou pedagogikou. Bykov a Leshchenko (2016) definujú digitálnu humanistickú pedagogiku ako vedu o zákonitostiach tvorby pozitívnej integrovanej vzdelávacej reality, považujú ju za novú pedagogickú disciplínu, ktorá prepája „-bio“ a „-techno“ a zaoberá sa tým, ako organizovať vyučovací proces, ak je realizovaný súčasne v reálnom i virtuálnom svete. Práve v tejto oblasti možno badať značné rezervy a tak vzniká potreba orientovať výskumnú činnosť na digitalizáciu v školstve.

Shrnutí

Podstatou digitálneho humanizmu ako aktuálnej výzvy pre ďalší rozvoj a smerovanie Európskej únie je orientovať digitalizáciu na záujmy ľudí a ich hodnoty. Digitálny humanizmus upozorňuje na to, že kým cieľom technického pokroku je zdokonaľovať technológie, v prípade digitálneho humanizmu ide o zdokonaľovanie človeka, o pozitívnu interakciu človeka a stroja (robota). Myslíme si, že digitálny humanizmus by mal zaujať jedno z kľúčových postavení v každom záväznom dokumente, ktorý sa bude zaoberať digitalizáciou akejkoľvek zložky nášho sveta a života ľudí v ňom, ako píšeme napr. Barnová – Krásna (2018a,b,c).

2.6 Ekonomika 4.0 a digitálna konkurencieschopnosť

Digitálna ekonomika

Internet prispel k sformovaniu nového dynamického sektora – digitálnej ekonomiky, v ktorej informačné a komunikačné technológie vytvárajú globálnu platformu, umožňujúcu realizovať podnikateľské zámery, komunikovať, kolaborovať a hľadať informácie (Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020).

Megatrendy ako mobilné technológie, cloudy, biznis inteligencia a sociálne siete nielen uvoľňujú inovačný potenciál v podnikoch a verejnej správe, ale podporujú aj tlak spotrebiteľov na:

- ✓ cenu služieb,
- ✓ kvalitu služieb,
- ✓ parametre,
- ✓ dostupnosť.

Priemysel a celé hospodárstvo prechádzajú v dôsledku zavádzania vyspelých informačných a komunikačných technológií a umelej inteligencie jednak do výroby, ale i služieb a všetkých sektorov hospodárstva, radikálnymi zmenami. Vplyv týchto zmien je natoľko dôležitý, že sa označujú ako nové hnutie nazývané 4. priemyselná revolúcia. Industry 4.0 je revolúcia založená na digitalizácii, na zmene výrobných procesov, na zmene obchodných modelov s cieľom urýchliť výrobu a zefektívniť ju, ako aj na prepojení systémov od požiadaviek zákazníkov až po finálny produkt prostredníctvom digitalizácie.

Digitalizácia má silný vplyv na národné hospodárstva; Združenia hodnôt sa môžu presúvať v rámci priemyslu a naprieč odvetviami a súčasní ekonomickí lídri môžu byť nahradení. Vlády musia prijať opatrenia na zabezpečenie toho, aby začínajúce a etablované spoločnosti mohli vytvárať nové obchodné modely a digitalizovať svoje existujúce operácie. Verejný sektor vrátane vzdelávacieho systému môže zohrávať dôležitú úlohu ako v oblasti rozvoja ľudského kapitálu, tak i v podpore inovačných sietí.

Podobne ako revolúcie, ktoré jej predchádzali, štvrtá priemyselná revolúcia má potenciál k zvýšeniu hladiny svetových príjmov a zlepšeniu kvality života obyvateľstva po celom svete. Nové technológie a pokrok priniesli pre mnohé krajiny zásadné zmeny, napr. za posledných 30 rokov sa v Indii počet obyvateľov žijúcich v chudobe znížil zo 60% na 22%, v Číne sa za to isté obdobie dostalo z chudoby 600 miliónov obyvateľov (<http://industry4.sk>).

K dnešnému dňu tí, ktorí získali najviac z prístupu k digitálnemu svetu boli spotrebiteľia. Technológia umožnila nové výrobky a služby, ktoré zvyšujú efektivitu a potešenie z našich osobných životov. Objednanie taxi, rezervácie letov, nákup tovaru, vykonanie platby, počúvanie hudby, sledovanie filmov alebo hranie hier, ale napríklad aj distribúciu e-receptov do lekární je už možné realizovať na diaľku. V budúcnosti tieto technologické inovácie povedú k zázračným zmenám v ponuke, s dlhodobými ziskami v náraste efektivity a produktivity.

Predpoklady a pripravenosť štátov na digitalizáciu ekonomík v celosvetovom porovnaní hodnotí Networked Readiness Index (publikovaný Svetovým ekonomickým fórom v Správe o globálnych informačných technológiách). Slovensko sa v roku 2016 umiestnilo na 47. mieste (139 hodnotených krajín), čo ho radí na chvost skupiny vyspelých a vysokopříjmových ekonomík.

Index je založený na kombinácii mäkkých a tvrdých ukazovateľov. Slovensko zaostáva najmä v kvalite tých faktorov, ktoré sa vzťahujú na fungovanie verejného sektora – kvalita legislatívneho prostredia, kvalita vzdelávacieho systému, postavenie a podpora informatizácie vládou, zdaňovanie zisku. Na druhej strane možno vidieť pozitívne hodnotenie takých faktorov, ako sú napr. nízka miera softvérového pirátstva, intenzita lokálnej konkurencie, pokrytie mobilnými sieťami, vybavenosť domácností počítačmi a internetom a využívanie IKT podnikateľským sektorom (Jeck, 2017).

Trendy rozvoja

Informačné technológie budú v budúcnosti utvárať podobu spoločnosti ešte výraznejšie ako doteraz. Úspešná verejná správa musí flexibilne využiť trendy spôsobom, ktorý umožní efektívne sledovanie cieľov a realizácie politík. Za najzásadnejšie trendy, ktoré definujú rozvoj a ovplyvňujú spôsob fungovania spoločnosti, súkromného a verejného sektora, je možné považovať:

- ✓ Využívanie analytických nástrojov na podporu rozhodovania („big data“);
- ✓ Poskytovanie čohokoľvek formou služieb;
- ✓ Transformácia zdravotníctva a vzdelávania;
- ✓ Nárast používania mobilného internetu;
- ✓ Prepojovanie fyzickej reality s digitálnou.

Digitalizácia verejnej správy

Inštitúcie verejnej správy zvyčajne komunikujú s veľkým počtom zákazníkov na základe vysoko regulovaných a štandardizovaných procesov. Práve digitalizácia tu ponúka obrovské príležitosti na zlepšenie skúseností so službami zákazníkom a uvoľnenie zdrojov spojených s opakovanými úlohami. Verejné orgány tiež zbierajú a uchovávajú údaje o údajoch. Využitie tohto pokladu môže viesť k inteligentnejším rozhodnutiam v každodenných činnostiach štátnych orgánov a vlády.

Už Národná koncepcia informatizácie verejnej správy ukazovala cestu pre modernizáciu verejných služieb a predstavuje základ pre budovanie „inovatívneho štátu“ a „štátu fungujúceho na základe využívania znalostí.“

NKÚ (2018) deklaruje, že jedným z kľúčových cieľov rozvoja slovenskej spoločnosti je pokrok v oblasti informatizácie verejnej správy a poskytovania kvalitných elektronických služieb občanom. V podmienkach Slovenskej republiky sa tento cieľ realizuje s využitím európskej finančnej pomoci ako aj z domácich zdrojov. K záveru roku 2017 bolo v dvoch operačných programoch pre rozvoj IT schválených 43 reformných zámerov v celkovej výške takmer 700 miliónov EUR. (OP efektívna verejná správa 161,4 mil. EUR a OP integrovaná infraštruktúra

534,3 mil. EUR). Z pohľadu občana je otázka poskytovania elektronických služieb kľúčová, avšak pre inštitúcie, ktoré prevádzkujú tieto systémy je dôležité tiež poznať, ako bude financovaná modernizácia existujúcej infraštruktúry. To je totiž cesta k tomu, aby mohli byť e-služby poskytované bezproblémovo a na úrovni dnešných moderných technologických možností.

Závažným nedostatkom je podľa NKÚ (2018) aj poddimenzovanosť a fluktuácia v oblasti ľudských zdrojov. Je evidentný problém nájsť odborníkov v oblasti IT, ktorí sú ochotní pracovať v štátnej správe, najmä v dôsledku nedostatočného platového ohodnotenia. Predpokladaná efektívnosť pracovných skupín, ktoré sa podieľali na vypracovávaní vykonávacích dokumentov, bola tiež poznačená absenciou systematickosti a rozdelenia práce, a v neposlednom rade aj chýbajúcimi minimálnymi požiadavkami na profesionálnu špecializáciu ich členov. To spôsobuje oneskorené schvaľovanie dôležitých dokumentov a tiež detailných akčných plánov. Národná kontrolná autorita upozorňuje, že táto situácia môže mať následne negatívny vplyv na efektívne a hospodárne využitie nielen národných, ale aj európskych zdrojov.

Riadenie projektov IT a ich kvalita závisí aj od odbornosti ľudí, ktorí sú priamo do tohto procesu zapojení. Bez vysoko kvalifikovaných zamestnancov štátnej správy nie je možné realizovať strategické verejné politiky zamerané na kvalitné a bezbariérové služby pre občanov. Je teda nevyhnutné zvážiť úpravu kvalifikačných požiadaviek a mzdového ohodnotenia ľudí na vysoko špecializovaných pracovných pozíciách, medzi ktoré bezpochyby patrí oblasť informatizácie.

Zlepšovanie verejných služieb

Informatizácia nevyhnutným faktorom pre zlepšenie služieb verejnej správy, služieb vo verejnom záujme ako i verejných služieb, pre optimalizáciu verejnej správy a pre zvýšenie jej dôveryhodnosti a transparentnosti. Je to kontinuálny proces, v ktorom sa využívajú nové možnosti, ktoré IKT v danom okamihu poskytujú. Potenciál na zlepšenie skúseností občanov a spoločností v oblasti služieb prostredníctvom digitalizácie je obrovský. Ak by sa z najbežnejších servisných transakcií odstránila administratíva, nemeckí občania by mohli ročne získať 84 miliónov hodín voľného času. Spoločnosti by ušetrili 1 miliardu EUR na administratívnych nákladoch ročne. A tento potenciál je len teoretický. Krajiny ako Estónsko sú na čele. Len tri druhy služieb stále vyžadujú, aby Estónci komunikovali s úradníkom tvárou v tvár: svadby, rozvody a transakcie s nehnuteľnosťami. Všetko ostatné je digitalizované.

Je pravda, že digitalizácia interakcií verejnej služby je zložitou výzvou, ktorá si vyžaduje koordináciu medzi rôznymi úrovňami verejnej správy. Najúspešnejšie jednotlivé agentúry sa zameriavajú na potreby zákazníkov a implementujú tie isté agilné testovacie a učebné postupy, ktoré používajú súkromní online giganti.

Nestačí však zmeniť spôsob práce vo verejných agentúrach a postoje verejných činiteľov. Agentúry a obce závisia od národnej vlády, aby im poskytli správne podmienky na to, aby uspeli. Náš výskum a globálne skúsenosti s digitálnymi transformáciami vo verejnom sektore naznačujú, že existuje päť hlavných úloh, ktoré môžu národné vlády vykonávať na uľahčenie spustenia a prijatia digitálnych verejných služieb:

- ✓ Nastaviť zastrešujúcu digitálnu stratégiu a definovať ciele,

- ✓ poskytovať spoločné IT platformy,
- ✓ definujte technické normy,
- ✓ uľahčiť zmenu prostredníctvom právnych predpisov
- ✓ podpíšte a podporte pilotné projekty, ktoré pomôžu verejným orgánom vybudovať kľúčové digitálne zručnosti.

Stratégia Digitálneho jednotného trhu (DSM)

Je vybudovaná na troch pilieroch:

1. Lepší prístup spotrebiteľov a podnikov k online tovarom a službám v celej Európe – vyžaduje si to rýchle odstránenie kľúčových rozdielov medzi online a off-line svetmi, aby zmizli prekážky cezhraničných online činností.
2. Vytváranie priaznivých podmienok pre rozmach digitálnych sietí a služieb – vyžaduje si to rozvoj vysokorýchlostných, bezpečných a dôveryhodných infraštruktúr a služieb týkajúcich sa obsahu, podporený správnymi regulačnými podmienkami pre inovácie, investície, spravodlivou hospodárskou súťažou a rovnakými podmienkami pre všetky podniky.
3. Maximalizácia rastového potenciálu nášho európskeho digitálneho hospodárstva – vyžaduje si to investície do infraštruktúry a technológií IKT, ako sú napríklad cloud computing a big data, a výskum a inovácie na podporu priemyselnej konkurencieschopnosti, ako aj lepšie verejné služby, inkluzívnosť a zručnosti.

Digitálna ekonomika prispieva k:

- ✓ Ekonomickému rastu a tvorbe HDP;
- ✓ vytváraniu vysokokvalifikovaných pracovných miest;
- ✓ **konkurencieschopnosti krajiny** - Digitálna ekonomika je základom vedomostnej spoločnosti, pretože prispieva k rozvoju komunikačných technológií spájajúcich ľudí a k efektívnej výmene informácií, produktov a služieb. Zavádzanie IKT technológií má tiež vysoký potenciál zvyšovania produktivity práce v privátnom aj verejnom sektore a tým pádom aj zlepšovania konkurencieschopnosti.

Zmeny na trhu práce

Digitalizácia výroby materiálnych produktov už začala a očakáva sa, do akej miery budú digitalizované úkony v administratíve. Zároveň sa vyskytujú obavy, že digitalizácia nesúci pokrok a rad nových príležitostí, bude mať aj svoje sociálne dopady, pretože ide o úplne novú filozofiu výroby spätú s celospoločenskými zmenami (Kronig, 2015), ktoré sa prejaví predovšetkým na trhu práce, kde bude vytváraný nedostatočný počet pracovných miest pre potenciálnych pracovnú silu.

Informačné technológie už v ostatných dvoch desaťročiach významne prispeli k zmenám v oblasti riadenia ľudských zdrojov. Majú taktiež významný vplyv na premeny trhu práce. Jednoznačne prispeli k zmene jeho štruktúry, pracovných metód a pracovných postupov. Zrýchlili jeho dynamiku a fungovanie. (Glatz, 2014) Trend je jasne nastavený a trh práce sa vyvíja tak dynamicky, že zmeny je možné sledovať v štvrťročných intervaloch. Podiel on-line segmentov na všetkých transakciách trhu práce rastie (Kocianová, 2012).

V dôsledku zmeny technológií možno taktiež už niekoľko desaťročí pozorovať fragmentáciu práce v priestore a čase. Kotýnková (2016) upozorňuje, že bol trh práce vystavený flexibilizácii, na ktorej je však možné nazerať diferencovane, a to z nasledujúcich dvoch protichodných stránok:

- ✓ Flexibilizácia práce vedie k veľkému zneisteniu dotknutých osôb a sťažuje im v živote plánovať. Život jednotlivca stráca jasnú časovú štruktúru. Fragmentácia pracovných pomerov môže viesť až k erózii sociálnej súdržnosti, pokiaľ sa spoločnosť bude aj naďalej opierať o stálu prácu, ako tomu bolo vo "spoločnostiach práce" od 19. storočia až dodnes.
- ✓ Flexibilné charakter pracovných pomerov však zároveň so sebou nesie možnosť prepojenia zárobkovej činnosti spolu s ďalšími aktivitami, predovšetkým prepojenie práce a ďalšieho vzdelávania, pracovného a rodinného života, práce a voľného času.

Konkurencieschopnosť

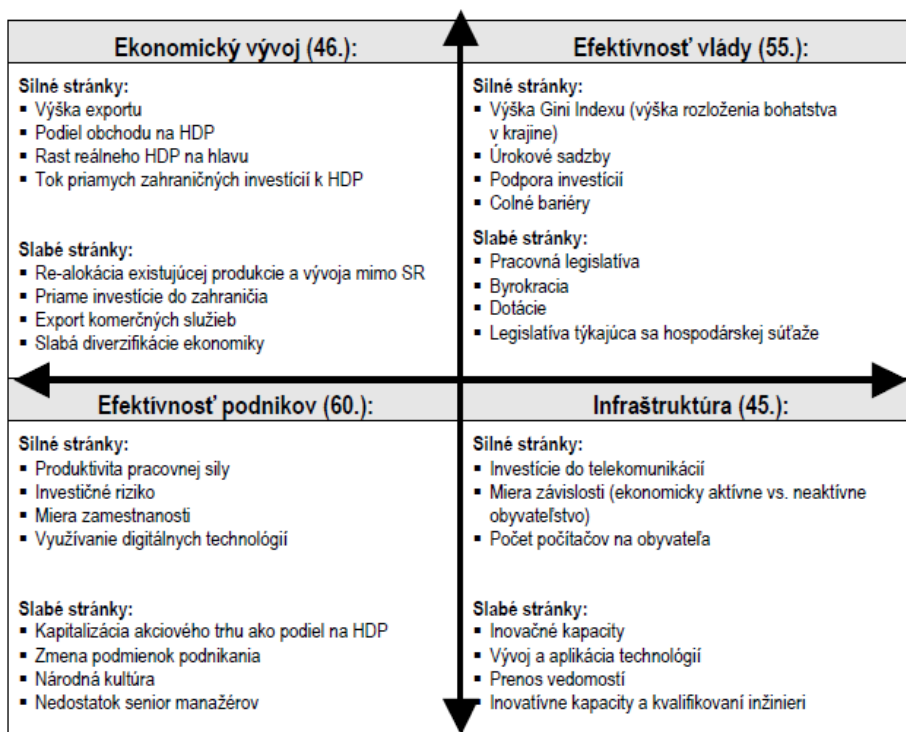
Z pohľadu kľúčových rebríčkov konkurencieschopnosti začalo Slovensko po viacročnej stagnácii strácať svoju pozíciu. V niektorých ukazovateľoch patrí medzi najhoršie krajiny EÚ. Z dlhodobého hľadiska to môže mať negatívny vplyv na hospodársky vývoj na Slovensku.

Konkurencieschopnosť Slovenska ťahá nadol hlavne **kvalita a efektívnosť verejných inštitúcií**. Svetové ekonomické fórum (WEF 2017) slabo hodnotí aj **efektívnosť trhu práce a oblasť vedy, výskumu a inovácií**. Najproblematickejšími faktormi na Slovensku sú podľa neho **korupcia, daňové zaťaženie a neefektívna vládna administratíva**. **Prepad v kvalite podnikateľského prostredia** hodnotenej Inštitútom pre rozvoj manažmentu (IMD 2017) súvisel so:

- ✓ slabou diverzifikáciou hospodárstva,
- ✓ zvýšením daňovej záťaže a regulácie podnikania,
- ✓ vyššou vnímanou korupciou,
- ✓ nedostatočnou pružnosťou trhu práce,
- ✓ nedostatkom pracovníkov v niektorých odvetviach a zároveň vysokou nezamestnanosťou mladých,
- ✓ ale aj často sa meniacimi podmienkami podnikania.

Index konkurencieschopnosti ekonomík

Najlepšie a najhoršie hodnotenými kritériami v prípade Slovenska boli v štyroch hodnotených oblastiach nasledovné (Svetová ročenka konkurencieschopnosti 2018):



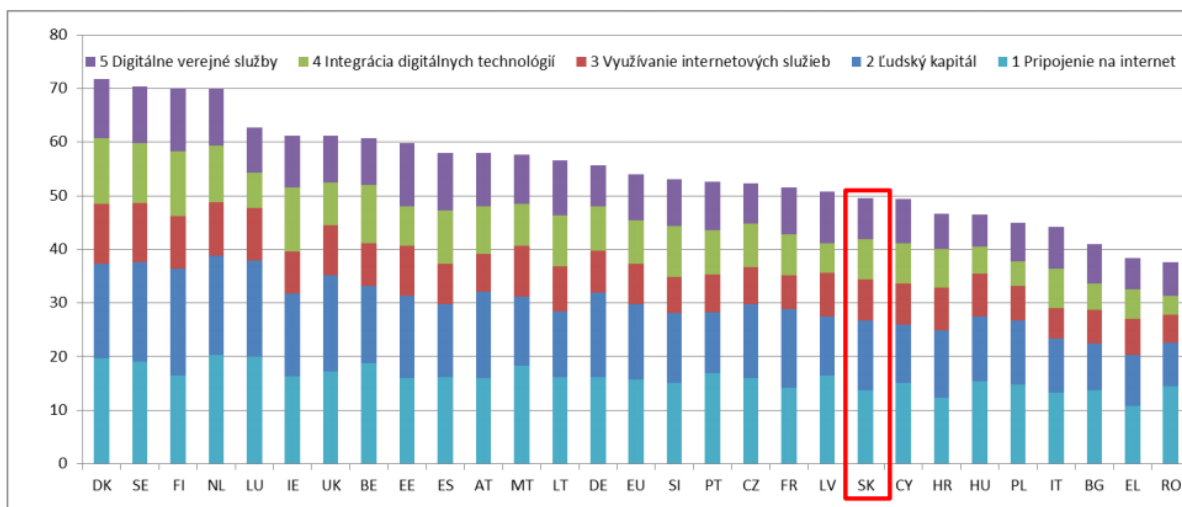
Zdroj: Svetová ročenka konkurencieschopnosti 2018

Slovenská republika sa tento rok umiestnila na 55. mieste spomedzi 63 hodnotených krajín. V medziročnom porovnaní sa postavenie Slovenska zhoršilo o 4 miesta.

Index digitálnej ekonomiky a spoločnosti (DESI) 2018

Slovensko v indexe digitálnej ekonomiky a spoločnosti (DESI, 2018) Európskej komisie za rok 2018 obsadilo 20. miesto spomedzi 28 členských štátov EÚ, čím dosiahlo pokrok. Zatiaľ čo sa jeho umiestnenie v rebríčku v porovnaní s rokom 2017 nezmenilo, jeho skóre sa zvýšilo vďaka zlepšenému výkonu vo všetkých rozmeroch meraných podľa indexu DESI. Slovenskí občania sú priemernými používateľmi internetu a náležite využívali rôzne online služby. Dostupnosť služieb pevného širokopásmového pripojenia a služieb 4G nie je rozšírená v takej miere, ako by bolo potrebné, avšak ultrarýchle širokopásmové pokrytie výrazne presahuje priemer EÚ. Pokiaľ ide o ľudský kapitál, napriek rastúcemu dopytu na trhu práce sa ponuka odborníkov v oblasti IKT naďalej nachádza pod priemerom EÚ.

V oblasti elektronickej verejnej správy Slovensko úspešne napreduje a v súčasnosti sa nachádza na 20. mieste. Počet používateľov elektronickej verejnej správy je však nižší ako priemer EÚ.



Zdroj: Index digitálnej ekonomiky a spoločnosti (DESI) 2018

Oblasť elektronizácie služieb verejnej správy (eGovernment) je pravdepodobne najviditeľnejšou formou presahu štvrtej priemyselnej revolúcie do spoločnosti. Na Slovensku je už niekoľko rokov normatívnou súčasťou (a prioritou najmä v proklamatívnej rovine) hospodárskej politiky.

Umiestnenie štátov v celosvetovom rebríčku (v oblasti eGovernment)

	2008	2016
Estónsko	13.	13.
Poľsko	33.	36.
Chorvátsko	47.	37.
Grécko	44.	43.
Maďarsko	30.	46.
Česko	25.	50.
Bulharsko	43.	52.
Slovensko	38.	67.

Zdroj: E-Government Development Index (OSN)

Výzvy pre rast konkurencieschopnosti

Žiaľ v prostredí priaznivého vývoja nezamestnanosti a zlepšujúcej sa kondície podnikov na Slovensku dochádza k relatívnemu zhoršovaniu domácich podmienok pre podnikanie. Tento negatívny signál sa môže postupne prejaviť v nižšej investičnej aktivite. Po odznení súčasného pozitívneho efektu už rozbehnutého rozšírenia výrobných kapacít v automobilovom priemysle

môže zhoršenie kvality podnikateľského prostredia a konkurencieschopnosti Slovenska negatívne ovplyvniť domáci hospodársky rast a dobíhanie vyspelejších krajín EÚ.

Najväčšími výzvami pre rast konkurenčnej schopnosti v najbližších rokoch sú pre Slovensko podľa Svetovej ročenky konkurencieschopnosti najmä:

- ✓ Nedostatok kvalifikovaných zamestnancov
- ✓ Vysoké administratívne zaťaženie podnikov
- ✓ Výzva v podobe nadchádzajúcej digitalizácie podnikov na Slovensku
- ✓ Vysoké náklady na prijímanie a prepúšťanie zamestnancov
- ✓ Absencia reforiem vo vzdelávaní a verejných službách.

Profesijne orientované študijné programy vysokoškolského vzdelávania - cesta k naplneniu cieľov?

Priemysel v skutočnosti nepotrebuje toľko „univerzitných absolventov“, orientovaných na vedeckú kariéru. Teda nie všetci absolventi prvého stupňa potrebujú vedomosti s hlbokými teoretickými základmi, ale mali by získať poznatky a zručnosti pre potreby praxe. Prax potrebuje nielen univerzitných inžinierov/magistrov, ale tiež profesijných bakalárov, ktorých naše školy nevychovávali. Vláda na základe viacerých analýz vie, koľko absolventov VŠ potrebujú jednotlivé odvetvia priemyslu v súčasnosti a koľko ich budú potrebovať v budúcnosti. Súčasný systém financovania však „finančne motivuje“ aj samotné školy, aby čo najviac bakalárov pokračovalo v druhom stupni štúdia, pretože tam za nich získame viac finančných prostriedkov.

Faktom ostáva, že s titulom bakalár sa na Slovensku uspokojia len tri percentá populácie, zatiaľ čo v krajinách OECD je to priemerne 16 percent. Toto mizivé percento ukončených bakalárov, ktorí nepokračujú na druhom stupni štúdia, je pre prax aj tak väčšinou nepoužiteľné, pretože nemajú požadované praktické vedomosti vo svojom odbore.

Až 57 % vysokoškolsky vzdelaných ľudí pracuje v úplne inom odbore ako vyštudovali. A 35 % vysokoškolákov (Ing. / Mgr.) sa po ukončení štúdia musí uspokojiť s pracovnou pozíciou vhodnou pre stredoškolačka. Inak povedané, magistri a inžinieri potom pracujú na pozíciách, kde by stačil aj nižší stupeň vzdelania. Tento trend majú práve zvrátiť nové profesijné odbory, ktoré by mali pripraviť zamestnancov pre automobilový či strojársky sektor, ale aj pre lesníctvo, poľnohospodárstvo a zdravotníctvo, či pri adekvátne prispôbenej legislatíve i pre verejný sektor a konkrétne oblasť informatizácie. Bežný prvý stupeň univerzitného štúdia sa zameriava na teoretické aj praktické poznatky. „Profesijne orientované bakalárske študijné programy sa zameriavajú na zvládnutie použitia týchto poznatkov pri výkone povolania (MŠ VVŠ SR).

Zhrnutie

Digitálna revolúcia sa datuje niekedy od polovice minulého storočia a je charakterizovaná zlúčením technológií, ktoré stierajú hranice medzi fyzickými, digitálnymi a biologickými sférami. Prináša zmeny, ktorých šírka a hĺbka ohlasujú transformáciu celých systémov výroby a riadenia. Miliardy ľudí spojených mobilnými zariadeniami, s nebývalým výpočtovým výkonom, prakticky

neobmedzenými dátovými kapacitami a prístupom k znalostiam, prináša takmer neobmedzené možnosti.

Dokážeme sa však takejto miere, rozsahu a komplexnosti transformácie pre ľudstvo tak zásadnej, ako žiadna iná technologická zmena z minulosti, o ktorej v tomto momente nevieme, ako sa ako sa bude vyvíjať, adekvátne postaviť a primerane, integrovane a komplexne reagovať? Tak, aby boli zahrnuté všetky zúčastnené strany na globálnom základe od verejného do súkromného sektora, do akademickej obce, či do občianskej spoločnosti?

2.7 Stane se základní nepodmíněný příjem nástrojem přerozdělování v nadcházející éře digitalizace a robotizace?

Základní nepodmíněný příjem (dále jen: „ZNP“) se stal v současné době předmětem diskusí v souvislosti s nadcházející érou digitalizace a robotizace. Možnost implementace ZNP jako nástroje budoucího řešení příjmové redistribuce si získává v posledních letech stále více pozornosti, i když se jedná o řešení kontroverzní. Vyjdeme-li však ze skutečnosti, že lidstvo stojí na prahu další etapy industriálního vývoje, která přinese změny ve způsobu vytváření bohatství a následně v oslabení propojení kapitálu a práce, pak nastává otázka, jakou podobu bude mít redistribuce vytvořeného bohatství.

Kyberneticko-fyzikální systémy a umělá inteligence v budoucnu vyřadí člověka z procesu tvorby hodnot, tak jak tomu dnes. K tomu, aby bylo vytvářeno bohatství, již nebude potřeba klasického spojení lidské práce a kapitálu, neboť se očekává, že v řadě profesí bude lidská práce nahrazena moderními technologiemi, a to jak v profesích manuálních, tak i v profesích administrativních a kontrolních. Nelze sice pochybovat o tom, že vzniknou nová odvětví, ve kterých budou vytvářena nová pracovní místa, o nichž v současné době nemáme přesnou představu, ale i přesto lze predikovat, že část populace v produktivním věku práci buď nenajde, protože pracovních míst nebude dostatek, nebo se nebude schopna přizpůsobit novým standardům a požadavkům trhu práce.

Lidé se vždy snažili ulehčit si práci a najít cestu, jak se věnovat více svým zálibám, než rutinní práci. Zdá se, že tento čas již přichází, lze však sledovat, že přináší nejen nadšení z pokroku, ale také řadu otázek, jejichž řešení bude složité. Prostředky na uspokojování svých životních potřeb získávají lidé dosud prací, za kterou jsou finančně ohodnoceni, avšak éra digitalizace a robotizace se přibližuje a spolu s tím se vynořuje otázka, jak redistribuovat bohatství i těm, kteří nenajdou uplatnění na trhu práce. V této nově vzniklé situaci představuje koncept ZNP jednu z možností, jak se vypořádat se složitou otázkou redistribuce bohatství. Většina diskusí se prozatím neopírá o pevná fakta, ale o odhady, které vyplývají z rozmanitých pokusů zavést ZNP v různých částech světa a v různých formách, z nichž nelze prozatím vyvodit jednoznačné výsledky (BIEN, 2017). Kapitola vychází z porovnání různých názorů na budoucnost práce a otvírá otázku ZNP jako jednoho z nástrojů řešení příjmové redistribuce.

Definice ZNP

Jednou z nejvýznamnějších institucí zabývajících se problematikou základního nepodmíněného příjmu je světová síť pracovišť, výzkumníků a vědců *Basic Income Earth Network* (dále: „BIEN“), která usiluje o rozšíření co největšího povědomí o ZNP a podporuje jeho zavedení. Definice základního nepodmíněného příjmu dle BIEN: „*Základní nepodmíněný příjem je periodická, nepodmíněná, individuální platba všem členům společnosti bez potřeby dokládání prostředků, nebo vykonávání jakékoli práce*“ (BIEN, 2019).

V odborné literatuře lze najít celou řadu dalších definic, více jednoznačnou definici uvádí např. Daniel Raventós⁴: „Základní příjem je takový příjem, který stát vyplácí každému plnoprávnímu členu společnosti nebo v ní trvale usazenému jednotlivci, a to i tehdy, pokud nechce vykonávat placenou práci, přičemž se nebere v úvahu, zda jde o bohatého či chudého, nebo – jinak řečeno – nezávisle na tom, jaké jsou jeho další případné zdroje příjmu, a bez ohledu na to, s kým žije ve společné domácnosti“ (Raventós, 2015).

Z definic ZNP vyplývá, že mezi odborníky panuje shoda v tom, že ZNP musí splňovat pět základních zásad:

- ✓ individualita ve výplatě (příjem je přiznán všem občanům daného státu včetně rezidentům, a to individuálně a bez ohledu na to, s kým žijí v domácnosti),
- ✓ univerzalita poskytování (příjem je poskytován plošně, tzn. bez doložení na nároku na příjem),
- ✓ nepodmíněnost (příjem není vázán na žádnou protihodnotu ani odvedený výkon),
- ✓ periodicita (příjem je poskytován opakovaně)
- ✓ peněžní plnění (příjmem je peněžní platba).

Vrátíme-li se zpět do historie, nalezneme řadu myslitelů, kteří navrhovali způsoby, jak zajistit všem členům společnosti základní životní potřeby. I když se zdá, že koncept ZNP začal být předmětem diskusí až s nástupem průmyslové revoluce, opak je pravdou. Již se zrodem renesance se začaly objevovat názory, že zajištění základních životních podmínek by nemělo být výhradou pouze dobročinnost a charity, ale že o nejchudší by se měly postarat municipality (obce), a to z veřejné podpory. Jedním z takových myslitelů byl i humanista Thomas More⁵, který již v roce 1516 publikoval dílo *Utopia* (Thomas More, 1963), v němž navrhuje, aby lidem bylo zajištěno základní živobytí zamezující, aby byli vystaveni takové tísní, která ohrožuje jejich přežití.

Od myšlenek k realitě se pokusil přejít následovník Thomase More, a to Johaness Ludovic Vives⁶, který ve svém dopise z roku 1526 navrhuje starostovi belgického města Bruggy, aby municipalita převzala odpovědnost za zajištění živobytí pro své občany. Nejednalo se o ZNP, jak jej chápeme dnes, ale spíše o garantovaný minimální příjem za práci nebo za prokázanou ochotu pracovat. Tento myslitel ještě nepřipouštěl, že by finanční prostředky byly poskytovány již před tím, než vznikne jejich potřeba. Na rozdíl od základního nepodmíněného příjmu, jak ho chápeme dnes, by nárok na pomoc měli lidé až ve chvíli, kdy se stanou chudými, zatímco dnešní koncept ZNP je chápán jako pojistka před vlastním pádem do chudoby (Vives, 1526).

Prvotní myšlenky, které se objevily již v průběhu 16. století, byly v průběhu dalších století dále rozvíjeny a to jak v Evropě, tak v USA, přičemž hlavním záměrem zavedení ZNP bylo snížit příjmovou nerovnost a chudobu. ZNP se stal v průběhu staletí předmětem výzkumu ekonomů a politiků a to jak z pravého, tak z levého křídla politického spektra. Zatímco levicově orientovaní odborníci zdůrazňovali výhody ZNP jako nástroje, který zajistí ve společnosti vyšší rovnost

⁴ Daniel Raventós, španělský ekonom a univerzitní profesor na katedře teoretické sociologie Ekonomické fakulty Barcelonské univerzity.

⁵ Thomas More (1478 - 1535), anglický myslitel, spisovatel a právník.

⁶ Johaness Ludovic Vives (1493 – 1540), španělský humanista a filosof

redistribucí příjmů a tím sociální smír a stabilitu, odborníci z pravé strany politického spektra zdůrazňovali snížení moci byrokratů, jednoduchost redistribuce a tím i pokles administrativních nákladů. Významným představitelem pravicově orientovaných ekonomů byl např. americký liberální ekonom Milton Friedman⁷, nositel Nobelovy ceny, který rozpracoval myšlenku negativní příjmové daně, svojí podstatou velmi blízkou konceptu ZNP (Friedman, 1982).

Od 16. století byl základní nepodmíněný příjem diskutován hlavně jako nástroj boje s chudobou obyvatelstva. S nástupem průmyslové revoluce v druhé polovině 19. století se diskuse zaměřily navíc na nutnost přetrnout bludný kruh chudoby, neboť nízké příjmy obyvatelstva nevytvářely prostor, aby lidé část svých příjmů odkládali, čímž se nevytvářel dostatek kapitálu pro investice, kterých bylo zapotřebí pro ekonomickou expanzi.

S nástupem digitalizace a robotizace se diskuse zavedení ZNP posunula, ZNP začíná být zvažován jako nástroj umožňující redistribuci zisků vytvořenými moderními technologiemi. Vychází se z úvahy, že při tvorbě hodnot již nebude potřeba lidské práce. Hlavní argumentace pro implementaci ZNP vychází z obav, že nabídka práce převáží poptávku po práci. ZNP by v tomto novém kontextu přestal být pouze nástrojem boje proti chudobě, ale hlavně nástrojem umožňujícím důstojný život ve společnosti, kde lidská práce již nebude patřit mezi hlavní výrobní faktory.

ZNP by se mohl stát vhodným nástrojem pro redistribuci zisků plynoucích z vlny automatizace a globalizace pro svoji transparentnost, jak uvádí ekonom Ugo Colombino⁸. Mezi pozitiva ZNP řadí velkou míru transparentnosti a nízké administrativní náklady. Kromě pozitivních faktorů upozorňuje ale i na faktory negativní, jako např.: vysoká finanční náročnost spojená s nutností zvýšeného výběru daní, problém zásluhovosti systému a též potenciální negativní dopady na úsilí, motivaci a autonomii lidí a dokonce i možné, až nežádoucí snížení nabídky práce jako důsledek vyšších příjmů a zvýšených daní (Ugo Colombino, 2015)⁹.

Změny na trhu práce

Z výše uvedeného pojednání o ZNP je zřejmé, že i když se jedná o téma kontroverzní, je mu v posledních letech věnováno stále více pozornosti a to v souvislosti s proměnou industriální společnosti, ke které začalo docházet již od konce 20. století.

Nahlédneme-li zpět do 70. let minulého století, dostáváme se do období nástupu pracovně úsporných technologií (postupného zavádění numericky řízených strojů, počítačů apod.), čímž se oslabil vztah mezi ekonomickým růstem a tvorbou nových pracovních míst¹⁰. Byl-li pro předcházející vývoj industriální éry typický vztah vzájemné závislosti mezi ekonomickým růstem

⁷ Milton Friedman (1912 – 2006), americký liberální ekonom 2. poloviny 20. století, nositel Nobelovy ceny za ekonomii, který významně přispěl k rozvoji neoklasické ekonomie.

⁸ Ugo Colombino, profesor na Universitě v Turíně

⁹ Za zmínku též stojí, že ZNP značně zpopularizoval Elon Musk, když ve svých četných prohlášeních vyslovil, že v nedaleké budoucnosti roboti zcela nahradí lidskou práci a rozdávat peníze „*zdarma*“ bude nevyhnutelné. Elon Musk je úspěšný americký podnikatel, filantrop a vizionář. Založil internetový systém PayPal, kosmickou společnost SpaceX a vede automobilku Tesla Inc.

¹⁰ Mezinárodní organizace práce dokládá, že 1% ekonomický růst vyvolá růst nových pracovních míst o 0,3 %, přičemž tento vztah se nadále oslabuje (ILO, 2013).

a objemem a kvalitou pracovní síly, pak od 70. let tato závislost přestává platit. Sociolog Zygmunt Bauman¹¹ označil novou etapu vývoje společnosti jako etapu post-moderní, v níž se faktor práce stává ve vztahu k ekonomickému růstu marginálním (Bauman, 1998). To, že se vztah mezi ekonomickým růstem a prací rozpojil, lze doložit tím, že ekonomický růst začal být od konce 20. století dosahován i při stagnaci počtu pracovních míst, případně při jejich velmi pozvolném nárůstu (OECD, 2018).

Jestliže od druhé poloviny 19. století a téměř po celé 20. století dominovala „společnost práce“, neboli přesněji společnost, v níž výkon práce v placeném zaměstnání tvořil základní strukturu společnosti, v současné době se faktor práce v hospodářské činnosti postupně oslabuje. Profese, které svého času garantovaly materiální jistoty, již dnes nelze spojit s trvalým sociálním statusem, kariéry jsou nevypočitatelné a povýšení stále více nepřehledné (Bogedan, Schildman, 2015). Jestliže práce měla sílu příjmově a sociálně stratifikovat společnost, tak v posledních dekádách 20. století tato síla značně zeslábla a to v souvislosti s proměnami hospodářské činnosti, kde došlo k nasazení pracovně úsporných technologií s následným dopadem na trh práce.

Nastupující etapa digitalizace a robotizace přinese - stejně jako předcházející etapy - změny ve způsobu vytváření bohatství. První etapa industriální éry byla založena na využití páry, druhá etapa na elektrifikaci a zavedení montážních linek, třetí pak na rozvoji IT technologií a pracovně úsporných technologií. Hybatelem čtvrté etapy industriálního vývoje je Internet, který stojí v centru propojení *virtuálně-kybernetického světa se světem fyzické reality*, což bude mít své sociální dopady. Vladimír Mařík charakterizuje budoucí vývoj společnosti následovně: „V jádru 4. průmyslové etapy (revoluce) stojí spojení virtuálně-kybernetického světa se světem fyzické reality. To s sebou přináší významné interakce těchto systémů *s celou společností, tedy se světem sociálním*“.(Mařík a kol., 2016). Do centra naší pozornosti se tedy dostávají kyberneticko-fyzikálně-sociální systémy.

Odhaduje se, že pracovní síla bude vytlačena z hospodářských činností, tak je dnes známe. Bezpochyby dojde ke změnám kvalifikačních potřeb trhu práce, přičemž je nutné zvažovat i sociální aspekty těchto změn. I když se očekává, že se budou postupně vytvářet nová odvětví, ve kterých lidská práce najde uplatnění a o jejichž existenci dnes nemáme tušení, je potřeba přiznat, že pravděpodobně určitá část populace zaměstnání nenajde, protože tvorba pracovních míst nebude dostatečná, nebo se určitá skupina obyvatel nebude schopna přizpůsobit novým standardům a požadavkům.

V roce 2013 předložili studii zabývající se dopady digitalizace a robotizace na trh práce američtí výzkumníci Carl B. Frey a Michael A. Osborne (Frey, Osborne, 2013), kteří vytvořili model pravděpodobnosti komputelizace profesí (model nahrazení profesí počítačem). Profese rozdělili do čtyř skupin, které jsou charakterizovány typem pracovních úkolů: skupiny profesí manuálních vs. kognitivních a rutinních vs. nerutinních. Došli k závěru, že ohroženy jsou především profese rutinní a to jak manuální, tak i kognitivní, neboť probíhají na zaběhnutých schématech, která lze algoritmizovat. Předpovídají však, že díky umění analyzovat tzv. big data a vytvářet z nich vzorce, budou později ohroženy i kognitivní profese nerutinního charakteru.

¹¹ Zygmunt Bauman (1926 – 2017), polský sociolog a filosof žijící od roku 1971 ve Velké Británii.

Automatizace manuálních nerutinních profesí bude umožněna zejména rozvojem robotizace a tzv. machine learning.

Carl B. Frey a Michael A. Osborne vyslovili předpoklad, že komputerizace proběhne ve dvou vlnách. V první vlně budou zasaženy rutinní profese ve výrobě a ve stavebnictví, v odvětví dopravy a logistiky, v obchodě a rutinní administrativní pozice, přičemž podíl těchto pracovních pozic činí v USA 47 % na celkové zaměstnanosti. S odstupem času dojde k technologickému překonání bariér u nerutinních profesí ať již manuálních, tak kognitivních a komputerizace se za pomoci umělé inteligence a samoučících se systémů dotkne i nejvíce kvalifikovaných profesí zahrnující rozhodovací proces. Většina nerutinních profesí je ale založena na vykonávání více typů pracovních úkonů a jejich kombinaci a proto lze předpokládat, že většina těchto profesí nezanikne zcela, ale dojde k nahrazení některých úkonů stroji, čímž se změní náplň práce těchto profesí.

Metodu amerických autorů do prostředí českého trhu práce aplikoval Aleš Chmelař (Chmelař, 2015). Z této studie je patrné, že z hlediska rozložení počtu zaměstnanců na českém trhu práce je vysoká koncentrace zaměstnanců v profesích s vysokým stupněm ohrožení komputerizací. Mezi nejohroženější profese se na českém trhu práce řadí obslužné profese ve výrobě, úřednické a administrativní profese, dále profese řidičů, pokladních apod., tedy profese založené na rutinních schématických úkonech, které lze nahradit relativně jednoduchou digitalizací využívající IT technologie. Na rozdíl od vyspělých ekonomik, např. ekonomiky USA, kterou analyzoval Freyem a Osborn, chybí v české ekonomice vysoké zastoupení skupiny profesí, jejichž ohrožení digitalizací je nízké (IT specialisté, profese ve vědě a výzkumu, apod.), z čehož vyplývá, že pouze malá část profesí zastoupených v české ekonomice nebude digitalizací ohrožena vůbec.

Míra ohrožení pracovních míst je hodnocena také ve studii OECD Employment Outlook 2017, ze které vyplývá, že Česká republika je hned po Slovensku druhou, digitalizací nejvíce ohroženou zemí, v důsledku vysoké koncentrace zaměstnanců v profesích lehce nahraditelných stroji a roboty, neboť je zde vysoký podíl zaměstnanosti v průmyslu a z toho ve zpracovatelském sektoru (OECD, 2017). Ze studie vyplývá, že během následujících 20 let bude automatizací vysoce ohroženo 10 % pracovních míst a u dalších 36 % dojde k podstatné změně náplně práce. Vyjádřeno počty zaměstnaných v české ekonomice ve 4. čtvrtletí 2018 to znamená, že 533 tis. pracovních míst je vysoce ohrožených a u 1,92 mil. pozic dojde k podstatné změně v prováděných činnostech.

Ačkoli se odhady liší, převládá názor, že budoucí úbytek pracovních míst bude vyšší než přírůstek nových pracovních míst. Důsledkem kvalifikačního nesouladu mezi nabídkou a poptávkou po práci budou růst skupiny lidí, které se nebudou schopny přizpůsobovat rychle se měnícím podmínkám trhu práce a hrozí, že budou zůstávat dlouhodobě mimo trh práce (MPSV, 2016). V současné době je společnost založena na principu, že člověk v produktivním věku získává prostředky na své potřeby za vykonanou práci. Vychází však problém, jak naložit s těmi, kteří zůstanou dlouhodobě mimo trh práce. Snižovat nezaměstnanost již nebude možné hospodářským růstem, neboť ten naráží na hranici environmentální udržitelnosti a dosažitelnosti zdrojů. Bude-li produkce obstarávána v éře digitalizace a robotizace tzv. bezobslužně, pak je pravděpodobné, že by došlo pouze k rozšíření výroby s využitím nových kyberneticko-fyzikálních systémů. Možnost boje s nezaměstnaností hospodářským růstem je, zdá se, vyčerpána.

Financování ZNP

Veškeré kritiky směřující ke konceptu ZNP poukazují na to, že distribuce ZNP ve výši, která by zajistila občanům důstojné živobytí, si vyžádá značné finanční zdroje a vyvstává otázka, jak tyto zdroje vytvořit. Je však třeba hned úvodem k této otázce zdůraznit, že digitalizace a robotizace přinese velký nárůst produktivity práce díky využití nových technologií (digitální systémy, umělá inteligence) stejně, jako došlo k nebývalému nárůstu produktivity práce vždy s využitím nově nastupujících, té doby neznámých technologií (pára, elektřina, montážní linky, mikročipy, numericky řízené stroje a počítače).

Rozhodnutí o tom, v jaké výši bude důstojný život zajištěn prostřednictvím ZNP, musí provést každá společnost sama v rámci demokratického rozhodovacího procesu a přijmout tím i důsledky tohoto rozhodnutí. Společnost může upřednostnit nižší ZNP a nižší daně, nebo může být ochotna za vyšší ZNP odvádět vyšší daně (Straubhaar, 2017). Důležitým rozhodnutím však bude, jaké nástroje využít k tvorbě zdrojů na financování ZNP. Většina návrhů směřuje do oblasti (1) daní a (2) úspor ze zjednodušeného sociálního zabezpečení.

V oblasti daňové reformy se zvažuje jak zvýšení současných daní, tak zavedení nových daní, především daně z robotizace a automatizace, ale i daně z finančních transakcí nebo navýšení progresu u solidární daně. Zvažováno je rovněž zrušení rozmanitých slev z daňového základu nebo slev ze samotné daně. Zdrojem financování ZNP se také stanou současné výdaje ze systému sociálního zabezpečení, neboť ZNP v plné míře nahradí sociální dávky, čímž dojde též ke zjednodušení sociálního systému a snížení administrativních nákladů¹².

Výsledky diskuse

Pokud se podíváme na problematiku ZNP z hlediska jeho využití v éře digitalizace a robotizace, což zapříčiní zánik, případně snížení řady pracovních míst, pak ZNP představuje možné řešení. ZNP se v této souvislosti stane nástrojem motivace těch, kteří nebudou mít naději uspět na pracovním trhu, k rezignaci na zaměstnání, neboli umožní, aby se práce vzdali. Pokles v nabídce práce by se tím vyrovnal očekávanému snížení poptávky po práci a trh práce by měl tendenci k rovnováze.

Na pracovní místa je nutné nahlížet jako na specifický zdroj, s nímž disponuje celá společnost, avšak v éře digitalizace a robotizace nebudou mít všichni možnost tento zdroj čerpat a proto koncept ZNP představuje jednu z možností, jak se s nově vzniklou situací vypořádat. Neboli, nebude-li trh práce jako specifický zdroj celé společnosti v budoucnu dostupný všem jejím členům, pak by se nárůst placené pracovní neaktivity mohl jevit jako přijatelný.

ZNP se může stát nástrojem, který umožní všem lidem ve společnosti žít důstojný život, neboť zaručí těm, kterým se nepodaří vstoupit na trh práce, aby se neocitli na nízkých dávkách v hmotné nouzi a v sociálním vyloučení. Implementace ZNP by měla též podnítit snížení rozsahu

¹² K financování ZNP je též možno použít výnosy z kolektivního vlastnictví přírodních zdrojů (na příkladu Aljašky je uváděna výplata tzv. částečného ZNP, který je vyplácen z výnosů fondu, do kterého směřují poplatky za těžbu ropy, čímž všichni obyvatelé Aljašky dostávají dividendu za využívání jejího přírodního bohatství (Alaska 2018).

pracujících chudých, kteří nyní pracují na méně kvalitních pracovních místech, kde čelí nízkým platům a často také špatným pracovním podmínkám. ZNP by dal každému možnost, rozhodnout se zda vykonávat špatně placenou práci či nikoliv, aniž by byl následně ohrožen chudobou a sociálním vyloučením. Neochota pracujících vykonávat tyto práce by měla vyvolat tlak na zaměstnavatele, aby u těchto pracovních pozic zlepšili pracovní podmínky, čímž by mělo dojít ke kultivaci pracovního prostředí.

Výše ZNP by měla být taková, aby tento příjem umožnil život na takové ekonomické, sociální a kulturní úrovni, která je v dané společnosti vnímána jako uspokojivá. Stejně jako současné dávky v hmotné nouzi, které chrání jejich příjemce před propadem do chudoby a sociálního vyloučení, i ZNP by měl ochránit všechny občany a rezidenty před propadem do chudoby a sociálního vyloučení, ale nově by měl oslabovat motivaci k práci, aby se ti, pro které nebude trh práce dostupný, práce vzdali s tím, že budou mít *nepodmíněně* zajištěn životní standart, který je společností vnímán jako přijatelný. ZNP by měl poskytnout každému jednotlivci pevný materiální základ, na němž mohou dále stavět a určovat směr svého života, přičemž těm, kteří uspějí na trhu práce, nebude ZNP krácen. Zavedení ZNP by tím navíc přispělo k tomu, aby se práce, které jsou v současné době neplacené, nebo nedostatečně placené, např. výchova dětí a péče o přestarlé rodiče, staly formou ZNP prací placenou.

Zatímco u současných dávek v hmotné nouzi se při stanovení jejich výše vyžaduje, aby jejich příjemcům dávky zabránily v propadu do chudoby a sociálního vyloučení a zároveň neoslabovaly motivaci k práci, posláním ZNP v éře digitalizace a robotizace by byla nově motivace k resignaci na placené zaměstnání. Dávka, která motivuje k resignaci na zaměstnání není v našem sociálním systému zcela neznámá. Jedná se o předčasný důchod, který je vyplácen těm, kteří neplní podmínky pro odchod z trhu práce do řádného starobního důchodu. Starší pracovní síle, která nemá šanci uspět na trhu práce je tím dána možnost rezignovat na práci a odejít do (předčasného) starobního důchodu a to až o 5 let dříve, je-li důchodový věk nezaměstnaného 63 let a více, nebo o 3 roky dříve, je-li jeho důchodový věk nižší než 63 let.

V souvislosti s možností implementace ZNP se upozorňuje na nutnost zpřísnění imigrační politiky, neboť se zvažuje riziko přílivu imigrantů do země, která poskytuje v rámci svého sociálního systému nepodmíněné zajištění životní standartu. Řešením je definování oprávněných příjemců na základě občanství, avšak i toto řešení v rámci volného pohybu pracovní síly obyvatel v EU může vyvolat konflikt, a to mezi občany daného státu a imigranty bez občanství. Řešením by pak bylo zavedení ZNP na úrovni celé Evropské unie, avšak to je již řešení další složité otázky jednotného ZNP pro země s různou příjmovou úrovní a s příjmovými nerovnostmi.

Shrnutí

Ohlédneme-li se zpět do historie, pak po celou dobu své existence se lidé vždy snažili ulehčit si práci. Usilovali o to, aby si usnadnili práci a mohli se věnovat svým zálibám. Zdá se, že ten čas nyní přichází, avšak nepřináší s sebou pouze uspokojení z tohoto pokroku, ale také řadu otázek, jejichž řešení může být složité. Jednou z nejsložitějších otázek je právě redistribuce bohatství vytvořeného s přispěním digitalizace a robotizace.

Vhodným nástrojem redistribuce bohatství by se mohl stát v budoucnu ZNP. Jestliže nahlédneme na trh práce jako na specifický zdroj společnosti, na který v éře digitalizace a robotizace nebudou mít všichni přístup a tím možnost z něho čerpat, jeví se koncept ZNP jako jedna z možností, jak se s nově vzniklou situací vypořádat. Neboli, nebude-li trh práce dostupný všem jejím členům, pak by se nárůst placené pracovní neaktivity mohl jevit jako přijatelný.

Výše ZNP by měla být taková, aby tento příjem umožnil život na takové ekonomické, sociální a kulturní úrovni, která je v dané společnosti vnímána jako uspokojivá. Stejně tak jako současné dávky v hmotné nouzi, které chrání jejich příjemce před propadem do chudoby a sociálního vyloučení, i ZNP by měl ochránit všechny občany a rezidenty před propadem do chudoby a sociálního vyloučení, ale nově by měl oslabovat motivaci k práci, aby se ti, pro které nebude trh práce dostupný, práce vzdali s tím, že budou mít *nepodmíněně* zajištěn životní standart. ZNP by měl poskytnout každému jednotlivci pevný materiální základ, na němž mohou dále stavět a určovat směr svého života.

Obhájci ZNP tvrdí, že jeho zavedení by vedlo k výraznému zlepšení kvality života ve společnosti, neboť by umožnil jeho příjemců soustředit se pouze na tu práci, která je bude uspokojovat a nevykonávat práci, která je pro ně pouze zdrojem získání příjmu. Navíc by došlo i k tomu, že práce, které jsou v současné době neplacené, nebo nedostatečně placené, mezi které patří především výchova dětí a péče o přestárle rodiče, by se staly prací placenou. Další oblastí, u které se předpokládá její navýšení díky ZNP je celá oblast dobrovolnictví, a to např. v takových žádoucích oblastech jako je komplexní péče o životní prostředí.

Hlavní kritika směřující ke konceptu ZNP poukazuje na to, že distribuce ZNP ve výši, která by zajistila občanům důstojné život, si vyžádá značné finanční zdroje a vyvstává proto otázka, jak tyto zdroje vytvořit. Při hledání odpovědi na tuto otázku je nutné zdůraznit, že digitalizace a robotizace přinese velký nárůst produktivity práce využitím nových technologií (digitální systémy, umělá inteligence) stejně, jako k tomu došlo v minulosti vždy při využití nově nastupujících, do té doby neznámých technologií (pára, elektřina, montážní linky, mikročipy, numericky řízené stroje a počítače). Důležitým rozhodnutím bude, jaké nástroje budou využity k tvorbě zdrojů na financování ZNP, neboli jak bude upravena fiskální a sociální politika. Většina návrhů na tvorbu dostatečných zdrojů pro financování ZNP směřuje do oblasti úpravy daní a úspor ze zjednodušeného sociálního zabezpečení.

Na základní nepodmíněný příjem můžeme nahlížet i z jiného pohledu než jen ekonomického, neboť se nejedná pouze o změnu, která se dotkne jenom redistribuce příjmů, ale ovlivní i vnímání člověka jako člena společnosti. Lidé přestanou být vnímáni jenom jako pracovní síla na straně nabídky na trhu práce, ale budou-li mít základní materiální základnu, budou svobodnější ve svém rozhodování a tím také odolnější vůči vnějšímu ovlivňování nebo manipulaci.

Česká republika má vysoké zastoupení profesí, které budou ohroženy digitalizací a robotizací. A naopak těch, které jsou méně ohrožené, má v mezinárodním měřítku podprůměrně. Odhaduje se, že v České republice bude během 20 let vysoce ohroženo automatizací téměř 540 tisíc pracovních míst a u téměř 2 milionů se zásadně změní náplň práce. Vzniknou zcela určitě nová pracovní místa, nicméně poměr nově vzniklých k zaniklým pracovním místům je odhadován na 2:5. Z tohoto pohledu je proto velmi důležité hledat možné způsoby, jak se vypořádat se situací, kdy

určitá část obyvatel nebude mít možnost získat placené zaměstnání. Základní nepodmíněný příjem může být i v České republice jednou z cest. Vhodné nástroje pro redistribuci bohatství vytvořeného digitalizací a robotizací v rámci sociální a fiskální politiky je potřebné začít postupně promýšlet s cílem zajistit, aby očekávané změny ve společnosti proběhly plynule a za únosných sociálně-ekonomických podmínek.

Zpracováno v rámci Interní grantové agentury VŠE IGS F5/12/2018.

Literatura

- [1] ALASKA, (2018). *Permanent Fund Divided Division* [online]. Alaska : Alaska government web, Department of Revenue Alaska [cit. 2019-03-01]. Dostupné z WWW <<https://pfd.alaska.gov/>>
- [2] ALI, R., BARRDEAR, J., CLEWS, R., SOUTHGATE, J., (2014). *The Economics of Digital Currencies*. Bank of England Quarterly Bulletin.
- [3] ANDRAŠKO, J., GÁBRIŠ, T., HOCHMAN, J., OLEJÁR, D., (2018). *Zákon o kybernetickej bezpečnosti Komentár*. Bratislava: Wolters Kluwer, 544 s. ISBN 978-80-8168-905-5
- [4] BANQUE DE FRANCE, (2013). *Les dangers liés au développement des monnaies virtuelles l'exemple du bitcoin*. [cit. 2019-15-02]. Dostupné z WWW: <<https://publications.banque-france.fr/les-dangers-lies-au-developpement-des-monnaies-virtuelles-l'exemple-du-bitcoin>>
- [5] BARIVIERA, A. F., BASGALL, M. J, HASPERUÉ, W., NAIOUF, M., (2017). Some stylized facts of the Bitcoin market. *Physica A: Statistical Mechanics and Its Applications*, s. 484, 82-90. doi:10.1016/j.physa.2017.04.159
- [6] BARNOVÁ, S., KRÁSNA, S., (2018a). Digitálny humanizmus a digitálna pedagogika v kontexte hodnôt Európskej únie v 21. Storočí. In: *Evropské hodnoty - tradice a jejich proměny v 21. Století*. Bílý, J. (ed). České Budějovice: Vysoká škola evropských a regionálních studií, 2018. ISBN 978-80-7556-028-5. s. 82-87.
- [7] BARNOVÁ, S., KRÁSNA, S., (2018b). Virtuálna generácia a aplikácia digitálnych technológií vo vyučovaní. In: *Duševné zdravie a wellbeing virtuálnej generácie*, 21.11.2018, Slovensko. Zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava: IPčko, 2018. ISBN 978-80-971933-7-9, s. 205-212.
- [8] BARNOVÁ, S., KRÁSNA, S., (2018c). Digitálne pracoviská v kontexte digitálneho humanizmu. Aktuálne problémy podnikovej sféry 2018 : International scientific conference 16th-17th May 2018, Bratislava. In: Kintler, J. , Uhliar, M. (eds). *Aktuálne problémy podnikovej sféry 2018: zborník vedeckých prác*. Bratislava: Bratislava Ekonom, 2018. ISBN (online) 978-80-225-4536-5, s. 57-62.

- [9] BAUMAN, Z., (1998). *Work, Consumerism and The New Poor*. Oxford : Oxford University Press. 183 s.
- [10] BECH, M., GARRATT R., (2017). *Central Bank Cryptocurrencies*, Bank for International Settlement. [cit. 2018-10-09]. Dostupné z WWW: <http://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.
- [11] BENDA, M., (2016). *Perspektivy sdílené ekonomiky*. Dokumentační bulletin MF 6/2016 [online]. Praha 2016, s. 8 [cit. 2018-12-30]. Dostupné z WWW: <http://www.mfcr.cz/assets/cs/media/Bulletin-knihovny-MF_2016-c-06_Financni-a-ekonomicke-informace-62016.pdf >
- [12] BÉREŠOVÁ, G., (2013). *Európska únia a jej orgány*. Bratislava, Univerzita Komenského v Bratislave, s. 163. ISBN 978-80-223-3380-1.
- [13] BIEN, (2018). *About Basic Income, What is Basic Income?* [online]. Basic Income Earth Network. [cit. 2019-03-03]. Dostupné z WWW: <<https://basicincome.org/basic-income/>
- [14] BIEN, (2018). *Overview of Current Basic Income Related Experiments* [online]. Basic Income Earth Network. [cit. 2019-03-03]. Dostupné z WWW: <<http://basicincome.org/news/2017/10/overview-of-current-basic-income-related-experiments-october-2017/#ontario>
- [15] BOGEDAN, C., SCHILDMAN, CH., (2015) Co znamená „strana pracujících“ v 21. století?, In: *Eseje o práci*. Praha : Friedrich-Ebert-Stiftung, pp. 18-21. ISBN 978-80-877-24-4
- [16] BOTSMAN, R., (2015) *Defining the sharing economy what is collaborative consumption and what isnt* [online]. 2015 [cit. 2018-12-21]. Dostupné z WWW: <<http://www.fastcoexist.com/3046119/defining-the-sharing-economy-what-is-collaborative-consumption-and-what-isnt> >
- [17] BOTSMAN, R., ROO, R., (2010). *What's mine is yours: The rise of collaborative consumption*. New York: HarperCollins Publishers, 2010. ISBN 978-0-06-204645-1
- [18] BRIÈRE, M., OOSTERLINCK, K., SZAFARZ, A., (2015). *Virtual currency, tangible return: Portfolio diversification with bitcoin*. J. Asset Management. 16, 365–373.

- [19] BYKOV, V.U., LESHCHENKO, M.P., (2016). Digital humanistic pedagogy: Relevant problems of scientific research in the field of using ICT in education. In: *Information Technologies and Learning Tools*, 53(3), 1-17. ISSN 2076-8184.
- [20] CAGANOV, D., BAWA, M., SZILVA, I., & SPIRKOVA, D., (2016). Importance of internet of things and big data in building smart city and what would be its challenges. In *Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 605–616). Berlin, Switzerland: Springer.
- [21] CECH TAXIKÁTOV, (2018). Činnosť taxislužby [online]. 2018 [cit. 2019-1-21]. Dostupné z WWW <<http://cechtaxi.sk/o-nas/>>
- [22] CIRÁK, J. a kol., (2008). *Občianske právo všeobecná časť*. Bratislava: Heuréka, 2008. 359 s. ISBN 978-80-89122-51-6.
- [23] Coinatmradar.com., (2017).[cit.2019-15-02]. Dostupné z WWW: <<https://coinatmradar.com/>>
- [24] Coinmarketcap. (2017). [cit.2019-15-02]. Dostupné z WWW: <<https://coinmarketcap.com/>>
- [25] COLOMBINO, U., (2015). *Is unconditional basic income a variable alternative to other social welfare measures?* [online]. Itálie : University of Torino. [cit. 2019-01-17]. Dostupné z WWW: <<https://wol.iza.org/uploads/articles/128/pdfs/is-unconditional-basic-income-viable-alternative-to-other-social-welfare-measures.pdf>>.
- [26] Cryptocoincharts.com, (2017). [cit.2019-15-02]. Dostupné z WWW: <<https://cryptocoincharts.info/markets/info>>
- [27] DAVENPORT, K., (2013). How Internet of Things Will Change Industry. CISCO. Dostupné na: <<http://www.industrial-ip.org/en/industrial-ip/internet-of-things/howthe-internet-of-everything-will-transform-industries>>.
- [28] DELLOITTE, (2018). *FinTech in Czech Republic and in the world*. [cit. 2019-15-02]. Dostupné z <<https://www2.deloitte.com/cz/cs/pages/financial-services/articles/fintech-v-cr-i-ve-svete.html>>
- [29] *Digitálny marketing*. [online]. Bratislava: Portál Podnikateľský manažment, 2014, 06. 11. 2014 [cit. 2019-03-31]. Dostupné z WWW: <<http://epodnikanie.euin.org/node/170>>

- [30] DORNER, W., LEMBERGER, M., (2013). Südostbayern – Vom Armenhaus zur Technologieregion? *Standort*, vol. 37, no. 3, pp. 166–171. DOI: 10.1007/s00548-013-0274-0
- [31] DRAGHI, M., CONSTÂNCIO, V., (2017). ECB press conference. [cit. 2019-10-01]. Dostupné z WWW: <<https://www.ecb.europa.eu/press/pressconf/2017/html/ecb.is170907.en.html>>
- [32] DWYER, G. P., (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81-91. doi:10.1016/j.jfs.2014.11.006
- [33] EBA. EUROPEAN BANKING AUTHORITY, (2014). *Opinion on 'virtual currencies'*. [cit. 2019-15-02]. Dostupné z WWW: <<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-014-08+Opinion+on+Virtual+Currencies.pdf> . pp. 21, 38-39.
- [34] EICHHORST, W., (2013). The European Labour Market Succes through flexibility and mobility. Success via reform: The German Jobs miracle. Konrad-AdenauerStiftung. CES. Dostupné na: <http://www.kas.de/wf/doc/kas_34465-544-2-30.pdf?140218161147>.
- [35] EP, (2018), *Virtual Currencies*, Monetary Dialogue July 2018, [cit. 2019-15-02]. Dostupné z: WWW: <http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf
- [36] Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia., (2006). *PSIB SR '06* [online]. [cit. 2007-09-11]. Dostupné z WWW: <<http://www.dsm.tate.cz/cz/psib-sr-2006/>>.
- [37] Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia., (2008). *PSIB SR '08* [online]. [cit. 2009-05-06]. Dostupné z WWW: <<http://www.dsm.tate.cz/cz/psib-sr-2008/>>. ISBN 978-80-969747-1-9>
- [38] EUR-lex, (2013). Otváranie systémov vzdelávania: nové technológie a otvorené vzdelávacie zdroje ako prostriedky inovačného vyučovania a vzdelávania pre všetkých. [online]. [cit. 2019-03-29]. Dostupné z WWW: <<http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52013DC0654>
- [39] EUROPEAN CENTRAL BANK, (2018). *The role of euro banknotes as legal tender*, Speech by Yves Mersch, Member of the Executive Board of the ECB, at the 4th Bargeldsymposium

of the Deutsche Bundesbank, Frankfurt am Main, [cit. 2019-15-02]. Dostupné z WWW: <<https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180214.en.html>

- [40] EURÓPSKA KOMISIA, (2016). Oznámenie Európskej komisie Európskemu parlamentu, Rade, Hospodárskemu a sociálnemu výboru a Výboru regiónov. *Európska agenda pre kolaboratívne hospodárstvo*. Brusel 2. 6. 2016. COM 2016 (356 Final)
- [41] Európska únia, (2010). *Stratégia Európa 2020*. [online]. [cit. 2019-2-2]. Dostupné z WWW: <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_sk cit. 2.2.2019>.
- [42] Európska únia, (2010). *Stratégia Európa 2020*. [online]. [cit. 2019-2-2]. Dostupné z WWW: <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_sk cit. 2.2.2019>.
- [43] Európska únia, (2010). Zmluva o fungovaní Európskej únie. Ú.v. EÚ C 83. 30.3.2010.
- [44] Európska únia, (2010). Zmluva o založení Európskeho spoločenstva pre atómovú energiu.
- [45] Európska únia, (2012). Odporúčania pre vnútroštátne súdy pri podávaní návrhov na začatie prejudiciálnych konaní. Ú.v. C 338, 6.11.2012, s. 1–6.
- [46] Európska únia, (2016). 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) (Text s významom pre EHP) Ú.v. L 119, 4.5.2016, s. 1–88.
- [47] EURÓPSKA ÚNIA, (2010). Zmluva o fungovaní Európskej únie, Ú.v. EÚ C 83.30.3.2010.
- [48] EVANS, D., (2011). The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. CISCO. White Paper. Dostupné na: <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>.
- [49] EYAL, N., (2014). Hooked: Wie Sie Produkte erschaffen, die süchtig machen. München: Redline Verlag.

- [50] FATF, FINANCIAL ACTION TASK FORCE, (2014). *Virtual Currencies, Key Definitions and Potential KYC/CFT Risks*, FATF Report. [cit. 2019-15-02]. Dostupné z <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>>
- [51] FCA FINANCIAL CONDUCT AUTHORITY, (2017). *Our Mission 2017, How we regulate financial services*. [cit. 2019-15-02]. Dostupné z WWW: <<https://www.fca.org.uk/publication/corporate/our-mission-2017.pdf>>.
- [52] FCA FINANCIAL CONDUCT AUTHORITY., (2016). *Call for Input on Supporting the Development and Adopters of RegTech*, Feedback statement. [cit. 2019-15-02]. Dostupné z WWW: <<https://www.fca.org.uk/publication/feedback/fs-16-04.pdf>>.
- [53] FELSON, M.; SPAETH, JOE L., (1978) *Community Structure and Collaborative Consumption: A routine activity approach*. American Behavioral Scientist [online]. 1978, 21 (March-April), s. 614-624. DOI 10.1177/00027642802100411
- [54] FINANČNÁ SPRÁVA SR, (2018). *Oznámenie pre poskytovateľov služieb prepravy a ubytovania sprostredkovaných prostredníctvom digitálnej platformy* [online]. Banská Bystrica [cit. 2019-01-09]. Dostupné z WWW: <<https://www.financnasprava.sk/sk/podnikatelia/dane/digitalne-platformy>>
- [55] FREY, C. B., OSBORNE M. O., (2013). *The Future of Employment: How Susceptible are Jobs to Computerisation?* Oxford: Oxford Martin School.
- [56] FRIEDMAN, M., FRIEDMAN, R.D., (1982). *Capitalism and freedom*. Chicago : University of Chicago Press, 1982. ISBN 0-226-26401-7. CMELAŘ, A., (2015). *Dopady digitalizace na trh práce v ČR a EU* [online]. Praha : Úřad vlády České republiky, [cit. 2019-03-25] Dostupné z WWW: <<https://www.vlada.cz/assets/evropske-zalezitosti/analyzy-EU/Dopady-digitalizace-na-trh-prace-CR-a-EU.pdf>>
- [57] GÁBRIŠ, T., (2014) *Cyber law*. Bratislava: Univerzita Komenského v Bratislave, 249 s. ISBN 978-80-7160-384-9.
- [58] GAWER, A., (2011). *Platforms, Markets and Innovation*. Edward Elgar Publishing Inc, 2011. 416 s. ISBN 978-1-84844-789-9.

- [59] GLASER, F., ZIMMERMANN, K., HAFERKORN, M., WEBER, M.C., SIERING, M., (2014). Bitcoin—asset or currency? Revealing users' hidden intentions. In: *Twenty-Second European Conference on Information Systems (ECIS)*, Tel Aviv
- [60] GREGUŠOVÁ, D. a kol., (2005). *Právo informačných a komunikačných technológií*. Bratislava: Vydavateľstvo STU, 2005. 184 s. ISBN 80-227-2195-6
- [61] GREGUŠOVÁ, D., HALÁSZOVÁ, Z., (2018). *Zákon o E-Governmente Komentár*, Bratislava: EUROKODEX, 237 s. ISBN 978-80-8155-080-5
- [62] GREGUŠOVÁ, D., PERÁČEK, T., CAPANDOVÁ, P. et al., (2016). Execution of the public authorities' competencies electronically in the Slovak republic. *Proceedings of SGEM 2016: International Multidisciplinary Conference on Social Sciences and Arts [3rd]*. Albena, Bulgaria. ISBN 978-619-7105-51-3, pp. 611-618
- [63] HALABURDA, H., GANDAL, N., (2014). Competition in the Cryptocurrency Market. *SSRN Electronic Journal*. doi:10.2139/ssrn.2506463
- [64] HATINA, T. a kol., (2006). *Terminologický slovník bezpečnosti a ochrany zdravia pri práci*. VÚ č..2310. Inštitút pre výskum práce a rodiny, Bratislava.
- [65] HENDRICKSON, J. R., LUTHER, W. J., (2017). Banning Bitcoin. *SSRN Electronic Journal*. doi:10.2139/ssrn.2850730
- [66] HENG, S. 2014. Industry 4.0: Upgrading of Germany's Industrial Capabilities on the Horizon. Available via SSRN.. <https://ssrn.com/abstract=2656608>. Accessed Dec 2016.
- [67] HILEMAN, G., RAUCHS, M., (2017). *Global Blockchain Benchmarking Study*. University of Cambridge, Centre for Alternative Finance. [cit. 2019-10-01]. Dostupné z WWW: <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-blockchain-benchmarking-study.pdf>
- [68] HYATTE, M., (2012). *Platform: Get Noticed in a Noisy World*. Nashville, Tennessee: Thomas Nelson, Inc., 2012.261 s. ISBN 978-1-59555-503-8.
- [69] Icowatchlist.com, (2017). [cit.2019-15-02]. Dostupné z WWW: <<https://icowatchlist.com/>>
- [70] ILO, (2013): *World of work*, Ženeva: ILO

- [71] INTERNATIONAL BUSINESS MACHINES, (2017). *IBM Leading the Pack in Blockchain Banking*, Institute for Business Values. [cit. 2019-15-02]. Dostupné z WWW: <<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN>
- [72] JANSÁ, L., OTEVŘEL, L., (2011). *Softwarové právo v IT*. Bratislava: Vydavateľstvo: Computer Press, 2011. 340 s. ISBN 978-80-251-3458-0.
- [73] JECK, T., (2017). Slovenská ekonomika a štvrtá priemyselná revolúcia: faktory a predpoklady. Ekonomický ústav SAV, Bratislava 2017. ISSN 1337-5598.
- [74] KLUČKA, J., MAZÁK, J., (2004). *Základy európskeho práva*, s. 132.
- [75] KOCIANOVÁ, R., (2012). *Personalni řízení: východiska a vyvoj*. 2. preprac. a rozš. vyd. Praha: Grada. ISBN 978-80-247-3269-5.
- [76] KOČIŠOVÁ, L. et al., (2018) *Securitization of liabilities in Slovak business law*. In International business information management association conference [31], Norristown: International business information management association, Milan. 2018. s. 5061-5069. ISBN 978-0-9998551-0-2
- [77] KOTÝNKOVÁ, M., (2016) *Průmysl 4.0: dopad digitalizace hospodářské činnosti na trh práce* In Paradigmy zmien v 21. storočí. Ekonomický ústav SAV Bratislava 2016. ISBN 978-80-7144-265-3
- [78] KOUBEK, J., (2015). *Řízení lidských zdrojů*. Praha: Management Press. 400 s. ISBN 9788072612888.
- [79] KRÁLIK, J., KRÁLIKOVÁ, K., (2016) *Polícia (v slovenskej spoločnosti)*. Brno: Tribun EU, 248 s. ISBN 978 – 80 – 263-1050-1
- [80] KRÁSNA, S., (2015). *Pracovná spokojnosť zamestnancov na trhu práce v podmienkach SR*. Dubnica nad Váhom: DTI, 2015. ISBN 978-80-89732-59-3.
- [81] KRONIG, R., (2015). *Total Digital – Rationalisierung unter dem Deckmantel einer Revolution*. [Online.] [Cit. 12. marca 2019] Dostupné na: <<http://www.gegenblende.de/++co++31958504-0dbc-11e4-8028-52540066f352>>.

- [82] KÚTIK, J., JAKUBČINOVÁ, M., KRÁLIKOVÁ, K., (2018) *Dejiny verejnej správy na území Slovenska: vybrané časti a kapitoly*. Bratislava: VEDA, 246 s. ISBN 978-80-224-1640-5.
- [83] LACKO, Ľ., (2012). *Osobní cloud*. Bratislava: Computer press, 2012. 270 s. ISBN 978-80-251-3744-4.
- [84] LAGARDE, CH., (2017), Central Banking and Fintech—A Brave New World? [cit. 2019-10-02]. Dostupné z WWW: <<https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>>
- [85] LI, X., WANG, C. A., (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems*, 95, 49-60. doi:10.1016/j.dss.2016.12.001
- [86] LOYDLOVÁ, M., (2013). *Reklama*. Bratislava: Ekonóm, 91 s. ISBN 978-80-225-3798-8
- [87] MADAR, Z. a kol., (1995). *Slovník českého práva. Zv. 1*. Praha: Linde Praha a.s., 716 s., ISBN 80-85647-62-1
- [88] MAISNER, M. a kol., (2011). *Základy softwarového práva*. Praha: Wolters Kluwer, 2011. 356 s. ISBN 978-80-7357-638-7.
- [89] MARIK, V., (2016). *Průmysl 4.0: Vyzva pro Českou Republiku*. Praha: Management Press.
- [90] MAŘÍK, V., a kol. (2019). *Průmysl 4.0: Výzva pro Českou republiku*. Praha: Management press. ISBN: 978-80-7261-440-0
- [91] MAŠTALKA, J., (2008). *Osobní údaje, právo a my*. Praha: Vydavatelství C.H.Beck. s. 14-15.
- [92] MATES, P., (2002). *Ochrana osobních údajů* . Praha: Vydavatelství Karolinum. s. 38.
- [93] MATES, P., MATOUŠKOVÁ, M., (1997). *Evidence, informace, systémy – právní úprava*. Praha: Codex Bohemia, 263 s. ISBN 80-85963-27-2.
- [94] MATKOVČÍKOVÁ, N., (2017). Budovanie značky zamestnávateľa ako efektívne riešenie prilákania a udržania si kvalitnej pracovnej sily v podniku. In *Ekonomické- sociálne nástroje*

ako faktor tvorby pracovných miest v podnikoch: zborník vedeckých statí : VEGA č. 1/0662/15. Bratislava :Vydavateľstvo EKONÓM, 2017. s. 23-28. ISBN 978-80-225-4471-9.

- [95] MATOFSKA, B., (2016). *What is the Sharing Economy?* 1. 9. 2016 [online]. [cit. 2019-1-09]. Dostupné z WWW: <<http://www.thepeoplewhoshare.com/blog/what-is-the-sharing-economy>>
- [96] MAY T.C., (1992), *The Crypto Anarchist Manifesto*. [cit. 2019-15-02]. Dostupné z WWW: <<http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>>
- [97] MILOŠOVIČOVÁ, P. et al., (2018). *The particularities of entrepreneurship according to the trade licensing act in the conditions of the Slovak Republic*. International business information management association conference [31], Norristown: International business information management association, Milan. 2018. s. 2736-2745. ISBN 978-0-9998551-0-2
- [98] MILOŠOVIČOVÁ, P., PAŠKTROVÁ, L., (2015). Rozvoj slovensko-nemeckých hospodárskych vzťahov. In: *Globalization and its socio-economic consequences : part 2. - Žilina: University of Žilina*, 2015. s. 505-514. ISBN 978-80-8154-145-2. Globalization and its socio-economic consequences: International scientific conference. 15th, Rajecké Teplice, 7.-8.10.2015.
- [99] MPSV, (2016). *Iniciativa Práce 4.0* [online]. Praha: Ministerstvo práce a sociálnych vecí. [cit. 2019-03-25] Dostupné z WWW: <https://portal.mpsv.cz/sz/politikazamest/prace_4_0/studie_iniciativa_prace_4.0.pdf>
- [100] Národná rada Slovenskej republiky, (1992). Zákon č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov.
- [101] Národná rada Slovenskej republiky, (2018). Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Dôvodová správa k návrhu zákona.
- [102] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY, (1991). Zákon č. 531/1991Zb. Obchodný zákonník.
- [103] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY, (2017). Zákon č. 344/2017, ktorým sa mení a dopĺňa zákon č. 595/2003 Z. z. o dani z príjmov. Dôvodová správa k návrhu zákona.

- [104] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY, (2018). Zákon č. 56/2012 Z. z. o cestnej doprave v znení neskorších predpisov.
- [105] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Jednotný informačný systém kybernetickej bezpečnosti*. [citované 2018-11-3]. Dostupné z [www: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html>](http://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html).
- [106] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Kybernetická bezpečnosť*. [citované 2018-11-3]. Dostupné z [www: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html>](http://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html).
- [107] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Národná stratégia kybernetickej bezpečnosti*. [citované 2018-11-3]. Dostupné z [www: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html>](http://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html).
- [108] *Návrh Stratégie digitálnej transformácie Slovenska*. (2018). [online]. [cit. 2019-03-09]. Dostupné z WWW: <https://platforma.slovensko.digital/t/strategia-digitalnej-transformacie-slovenska-pre-roky-2019-2030/5974>
- [109] News BTC, (2017). Legolas Combines Decentralization and a Centralized Platform to Create an Ideal Exchange for Large Investors. [cit. 2019-15-02]. Dostupné z WWW: [<http://www.newsbtc.com/2017/09/02/legolas-decentralized-centralized-platform/>](http://www.newsbtc.com/2017/09/02/legolas-decentralized-centralized-platform/)
- [110] NOVOTNÝ, V., KLÍMA, K., KRÁLIKOVÁ, K., – DUDOR, L., (2017) *Veřejná správa v zemích Visegrádské čtyřky. (Česká republika, Maďarsko, Polská republika, Slovenská republika)*. Praha: Leges, 192 s. ISBN 978 – 80 – 7520 – 215 – 8.
- [111] OECD, (2017). Industrial production (indicator). doi:<https://doi.org/10.1787/39121c55-en>. Available via. <https://data.oecd.org/industry/industrial-production.htm>. Accessed May 2017.
7. PAC-IT (2013).
- [112] OECD, (2017). *Employment Outlook 2017* [online]. [cit. 2019-03-25] Dostupné z WWW: [<http://www.oecd.org/els/oecd-employment-outlook-19991266.htm](http://www.oecd.org/els/oecd-employment-outlook-19991266.htm)
- [113] OECD, (2018). *Employment Outlook 2018* [online]. [cit. 2019-03-25] Dostupné z WWW: [<http://www.oecd.org/els/oecd-employment-outlook-19991266.htm](http://www.oecd.org/els/oecd-employment-outlook-19991266.htm)

- [114] OKRESNÝ SÚD BRATISLAVA, (2018). Uznesenie Okresného súdu Bratislava I zo dňa 16. februára 2018) v konaní o návrhu na nariadenie neodkladného opatrenia v právnej veci žalobcu: Občianske združenie koncesovaných taxikárov, proti žalovanému: Uber B.V.
- [115] PERÁČEK, T., (2011). *Spravodlivosť a spravodlivý prístup k informáciám*. [Dizertačná práca]. Bratislava: Univerzita Komenského v Bratislave.
- [116] PERÁČEK, T., MUCHA, B., KOČIŠOVÁ, L., (2017). Importance of the e-government act and its impact on the management and economy of the enterprise in the Slovakia. *Proceedings of Management and economics in manufacturing: global scientific conference*. Zvolen, Slovakia. ISBN 978-80-228-2993-9, pp. 90-96
- [117] PETTEY, C., (2015). *Embracing Digital Humanism*. [online]. [cit. 2019-03-19]. Dostupné z WWW: <https://www.gartner.com/smarterwithgartner/embracing-digital-humanism/>.
- [118] PIETERS, G., VIVANCO, S., (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, 39, 1-14. doi:10.1016/j.infoecopol.2017.02.002
- [119] PODNIKAJTE.SK., (2013). *Povinnosti pri pracovných úrazoch*. In Podnikajte.sk ISSN 1338-2187. [citované 2018-11-3]. Dostupné z www: <<https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/povinnosti-pri-pracovnych-urazoch>>.
- [120] POHORELÁ, P., (2019). *GDPR po skončení pracovného pomeru*. In Podnikajte.sk ISSN 1338-2187. [citované 2018-11-3]. Dostupné z www: <<https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/povinnosti-pri-pracovnych-urazoch>>.
- [121] POLEDNÁKOVÁ, A., (2016). *Strategické plánovanie a rozvoj venkova*. In PÁNA, Lubomír. *Nástroje a aktuální problémy regionální politiky: studia (monografie)*. - České Budějovice: Vysoká škola evropských a regionálních studií, 2016. ISBN 978-80-87472-99-6, s. 9-13.
- [122] PORTER, M., (2003). The Economic Performance of Regions. *Regional Studies*, vol. 37, no. 6-7, pp. 545-546. DOI: 10.1080/0034340032000108688
- [123] Príručka na vykonávanie auditu informačných systémov, (2003). No: 331/2003-22, Bratislava: MF SR, 2003. 23 s.

- [124] RAVENTÓS, D., (2015). *Materiální podmínky svobody*. Praha : Rubato. ISBN: 978-80-87705-20-9
- [125] RBC. Royal Bank of Canada Capital Markets, (2018). *Crypto Currency & Blockchain Technology: A Decentralized Future*. [cit.2019-15-02]. Dostupné z WWW:<https://ca.rbcwealthmanagement.com/documents/77054/77074/Crypto+Currency+%26++Blockchain+Technology+-+A+Decentralized+Future+RBC+Capital+Markets+Jan+2018.pdf/594fcb18-1b28-48c1-920f-74938c59cc90>
- [126] RIES, E., (2012). *Lean Startup: Schnell, risikolos und erfolgreich Unternehmen gründen*. München: Redline Verlag.
- [127] ROWLEY J., (2018). Crunchbase, Oath Tech Network, *With at least \$1.3 billion invested globally in 2018*, VC funding for blockchain blows past 2017 totals. [cit. 2019-15-02]. Dostupné z WWW: <https://techcrunch.com/2018/05/20/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/?guccounter=1>
- [128] RUSSEV, S. a kol., (2002). *Metódy vývoja informačných systémov*. Bratislava: Vydateľstvo Ekonóm, 2002. ISBN 80-225-1542-6.
- [129] RUSSEV, S. a kol., (2003). *Automatizácia tvorby informačných systémov*. Bratislava: Vydateľstvo Ekonóm, 2003. ISBN 80-225-1602-3.
- [130] SCHAEFFER, E., (2017). *Industry X.0: Realizing digital value in industrial sectors*. Munchen: Redline Verlag.
- [131] SCHWEIZER, L., (2018). *Zle uchopená kybernetická bezpečnosť môže firmu stáť až 300 000 eur*. In *Právne noviny*. [citované 2018-11-3]. Dostupné z [www: <https://www.pravnenoviny.sk/zle-uchopena-kyberneticka-bezpecnost-moze-firmu-stat-az-300-000-eur>](http://www.pravnenoviny.sk/zle-uchopena-kyberneticka-bezpecnost-moze-firmu-stat-az-300-000-eur).
- [132] SLOV-LEX. Právny a informačný portál. *Zákon č.69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*. [citované 2018-11-3]. Dostupné z [www: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/#paragraf-20>](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/#paragraf-20).

- [133] SMEJKAL, V. a kol., (2004). *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha: C.H.Beck, 2004. 700 s. ISBN 80-7179-765-0.
- [134] STANEK, P., & PAUHOFOVA, I., (2016). *Adaptačné procesy a pulzujúca ekonomika v cykle paradigmy zmien v 21. storočí*. EU SAV, Bratislava.
- [135] STAUBHAAR, T., (2017). *On the Economics of a Universal Basic Income* [online]. Intereconomics 52/2017. [cit. 2018-04-30]. Dostupné z WWW: <<https://archive.intereconomics.eu/year/2017/2/on-the-economics-of-a-universal-basic-income/>>
- [136] STEPHANY, A., (2015). *The Business of Sharing: Making it in the New Sharing Economy*. 1. vyd. Houndmills, Basingstoke [u.a.]: Palgrave Macmillan. 2015. ISBN: 978-1-349-47762-3.
- [137] Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020)
- [138] Súdny dvor EÚ, (2015). Právna vec C-230/14, Weltimmo s.r.o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság, Rozhodnutie z 1. októbra 2015 ECLI:EU:C:2015:639. [online]. [cit. 2019-2-2]. Dostupné z WWW: <<http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=SK>>.
- [139] SÚDNY DVOR EÚ, (2017). Návrhy generálneho advokáta vo veci C-434/15. [online]. Luxemburg. [cit. 2018-12-30]. Dostupné z WWW: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-05/cp170050sk.pdf>>
- [140] SÚDNY DVOR EÚ, (2017). Rozhodnutie z 20. decembra 2017 vec C-434/15, Asociación Profesional Elite Taxi proti Uber Systems Spain SL [on-line]. Luxemburg. [cit. 2018-12-09]. Dostupné z WWW: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=198047&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=78824>>
- [141] SÚDNY DVOR EU: Tlačové komuniké č.117/15 z 6.10.2015 Luxemburg. Rozsudok vo veci C-362/14 Maximilian Schrems/Data Protection Commissioner. [online]. [cit. 2019-2-2]. Dostupné z WWW: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sk.pdf>>.

- [142] SÚDNY DVOR EU, (2016). Právna vec C-582/14 *Patrick Breyer proti Bundesrepublik Deutschland*. Rozhodnutie z 19. októbra 2016. ECLI:EU:C:2016:779. <http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=SK>.
- [143] SUNDARARAJAN, A., (2016). *The Sharing Economy: The End of Employment and the Rise of Crowd - Based Capitalism*. Cambridge, Massachusetts: The MIT Press, 2016. ISBN 978-0-262-03457-3.
- [144] SYSÁKOVÁ, V., ŠLAHOR, L., (2010). *Peniaze a bankovníctvo*. Bratislava : KARTPRINT, 2010. 14-16 s. ISBN 978-80-88870-89-0.
- [145] SZARKOVÁ, M. a kol., (2013). *Personálny marketing a personálny manažment*. Bratislava: Vydavateľstvo EKONÓM. ISBN 978-80-225-3594-6.
- [146] SZARKOVÁ, M. et al., (2014). *Personnel marketing and personnel management – functions and competences*. Bratislava: vydavateľstvo EKONÓM, 2014. 106 s. ISBN 978-80-225-3937-1.
- [147] ŠPIDLA, A. *Kybernetická a informačná bezpečnosť*. Český inštitút manažérov informačnej bezpečnosti. [citované 2018-11-3]. Dostupné z www: <<http://www.unievydavatel.cz/>>.
- [148] The Chicago Mercantile Exchange, (2017). [cit.2019-15-02]. Dostupné z <http://www.cmegroup.com/mediaroom/pressreleases/2017/10/31/cme_group_announceslaunchofbitcoinfutures.html/>
- [149] TOMEK, G., & VAVROVA, V., (2017). *Prumysl 4.0 aneb nikdo sam nevyhraje*. Pruhonice: Professional Publishing.
- [150] Úrad na ochranu osobných údajov SR, (2013): Metodické usmernenie 1/2013 k pojmu osobné údaje. Bratislava.
- [151] VALKOVÁ, Z., DUDÁŠ, J., PALÚŠ, J., (2013). *Zákon o ochrane osobných údajov. Komentár od autorov zákona*. 1. vyd. Mojmirovce: Kaštieľ Mojmirovce, s.r.o., 2013, s. 45.
- [152] VEBER, J.; KRAJČÍK, V.; HRUŠKA, L. a kol., (2016). *Sdílená ekonomika*. Praha: VŠPP. [online]. [cit. 2018-12-30]. Dostupné z WWW: <<https://www.vspp.cz/wp-content/uploads/2017/05/zprava.pdf>>

- [153] VIVES, J. L. *De Subventionem Pauperum, Sive de humanis necessitatibus*. [online]. Basic Income Earth Network. [cit. 2019-03-20] Dostupné z: <<http://basicincome.org/basic-income/history/>>
- [154] Výbor regiónov : Stanovisko Výboru regiónov „Stanovisko k balíku právnych predpisov o ochrane údajov“ *Ú.V, C 391, 18.12.2012, s. 127–133*.
- [155] WEF, (2015). *World Economic Forum Survey*. [cit.2019-15-02]. Dostupné z WWW: <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>.
- [156] ZÁVODNÝ, P. a kol., (2012). *Počítačové siete a distribuované spracovanie dát*. Bratislava: Sprint, 2012. 225 s. ISBN 978-80-88848-76-8.

Rejstřík

B

bezpečnost' IS/IT 14
blockchain 61, 63, 65, 66, 67, 71
BOZP 21, 22

C

cloudová zmluva 39

D

digitalizace a robotizace 86, 88, 89, 91, 92, 93
digitalizácia 77, 78, 80
digitálna ekonomika 77, 80
digitálne hospodárstvo 74
digitálny humanizmus 73, 75, 76, 95

F

FinTech 66, 68, 69, 71, 97

I

informácia 33, 35
informačné systémy 10
informačné technológie 78, 80
inominátny kontrakt 38

K

kapitál 74, 82
kolaboratívna ekonomika 47
komunikácia 27, 36

kryptomena 61
kybernetická bezpečnosť 10, 19

M

malé a stredné podniky 10, 20, 21, 22
manažment 97

O

ochrana osobných údajov 24, 28
online 22, 28, 32, 33, 34, 35, 36, 37, 52, 57, 63, 79, 80, 82,
osobné údaje 20, 21, 22, 24, 27, 28, 29, 30,

P

personálne 10, 12
Policajný zbor SR 32, 33, 34, 35, 37

R

redistribuce příjmů 93
regional development 53, 54, 56, 58, 59, 60
regulácia 46, 66, 69
rural development 52, 53, 55, 56, 57, 60

S

služba 33, 37, 40, 42, 43, 44, 46, 49
startups 52, 53, 54, 55, 56, 58, 60

Z

základní nepodmíněný příjem 86, 88, 93

Adresář

PaedDr. Silvia BARNOVÁ, PhD., Katedra školskej pedagogiky a psychológie, Vysoká škola DTI, Ul. Sládkovičova 533/20, 018 41 Dubnica nad Váhom, Slovenská republika, E-mail: barnova@dti.sk

Ing. Benita BELÁŇOVÁ, Ph.D., Katedra informačného manažmentu, Fakulta podnikového manažmentu, Ekonomická univerzita v Bratislave, Dolnozemská 1/b, 852 35 Bratislava, Slovenská republika, E-mail: benita.belanova@euba.sk

doc. Ing. Ivana BUTORACOVÁ ŠINDLERYOVÁ, PhD., Fakulta sociálnych vied Univerzita sv. Cyrila a Metoda Trnava, Bučianska 4/A, 917 01 Trnava, Slovenská republika, E-mail: ivana.butoracova@ucm.sk

doc. PhDr. Andrea ČAJKOVÁ, PhD., Fakulta sociálnych vied, Univerzita sv. Cyrila a Metoda Trnava, Bučianska 4/A, 917 01 Trnava, Slovenská republika, E-mail: andrea.cajkova@ucm.sk

prof. Dr. Wolfgang DORNER, Institute of Applied Informatics, Technologie Campus Freyung, Technische Hochschule Deggendorf, Grafenauer Str. 22, 94078 Freyung, Germany, E-mail: wolfgang.dorner@th-deg.de

Ing. Marcel ĎURIŠ, MBA., Katedra marketingu, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 05 Bratislava 25, Slovenská republika, E-mail: duris.marcel@gmail.com

Magdalena FALTER, M.A., Institute of Applied Informatics, Technologie Campus Freyung, Technische Hochschule Deggendorf, Grafenauer Str. 22, 94078 Freyung, Germany, E-mail: magdalena.falter@web.de

RNDr. Růžena FEREBAUEROVÁ, Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 6, 370 01 České Budějovice, E-mail: ferebauerova@vsers.cz

Mgr. Richard HELIGMAN, Katedra marketingu, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 05 Bratislava 25, Slovenská republika, E-mail: richard.heligman@fm.uniba.sk

JUDr. Ing. Eduard JENČO, MBA., Paneurópska vysoká škola, Fakulta práva, Ústav súkromného práva, Paneurópska vysoká škola n.o., Tomášikova 20, 820 09 Bratislava, Slovenská republika, E-mail: eduard@jenco.sk

doc. Ing. Magdalena KOTÝNKOVÁ, CSc., Katedra hospodářské a sociální politiky, Národohospodářská fakulta, Vysoká škola ekonomická v Praze, nám. W. Churchilla 4, 130 67 Praha, Česká republika, E-mail: kotynkov@vse.cz

PhDr. PaedDr. Slávka KRÁSNA, PhD., Katedra školskej pedagogiky a psychológie, Vysoká škola DTI, Ul. Sládkovičova 533/20, 018 41 Dubnica nad Váhom, Slovenská republika, E-mail: krasna@dti.sk

Mgr. Natália MATKOVČÍKOVÁ, PhD., Katedra manažmentu, Fakulta podnikového manažmentu, Ekonomická univerzita v Bratislave, Dolnozemska 1, 852 35 Bratislava, Slovenská republika, E-mail: natalia.matkovcikova@euba.sk

prof. JUDr. Daniela NOVÁČKOVÁ PhD., Katedra ekonómie a financií, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 06 Bratislava, Slovenská republika, E-mail: daniela.novackova@fm.uniba.sk

doc. Ing. Oldřich PEKÁREK, CSc., Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 6, 370 01 České Budějovice, E-mail: pekarek@vsers.cz

doc. RNDr. Darina SAXUNOVÁ, Ph.D., Katedra Ekonómie a financií, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 05 Bratislava 25, Slovenská republika, E-mail: darina.saxunova@fm.uniba.sk

doc. Ing. Iveta STANKOVIČOVÁ, Ph.D., Katedra informačných systémov, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 06 Bratislava, Slovenská republika, E-mail: iveta.stankovicova@fm.uniba.sk

doc. Ing. Mgr. Ľubomíra STRÁŽOVSKÁ PhD., Katedra marketingu, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 05 Bratislava 25, Slovenská republika, E-mail: lubomira.strazovska@fm.uniba.sk

doc. PhDr. Rozália SULÍKOVÁ, PhD., Katedra marketingu, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 05 Bratislava 25, Slovenská republika, E-mail: rozalia.sulikova@fm.uniba.sk

Ing. Jarmila WEFERSOVÁ, Ph.D., Katedra ekonómie a financií, Fakulta managementu, Univerzita Komenského v Bratislave, Odbojárov 10, 820 06 Bratislava, Slovenská republika, E-mail: jarmila.wefersova@fm.uniba.sk

Název: Digitální ekonomika a společnost
Autoři: RNDr. Růžena Ferebauerová, doc. Ing. Oldřich Pekárek, CSc. et al.
Rozsah: 113 s.
Náklad: 200 ks
Účel: Monografie
Rok vydání: 2019
Vydavatel: Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 6, 370 01 České Budějovice, ČR
Tisk: Tribun EU s.r.o.

ISBN 978-80-7556-048-3