

Právo EU - nová úprava přeshraničního přístupu k elektronickým důkazům v trestních věcech a upevnění justiční spolupráce mezi členskými státy

EU Law - New Regulation of Cross-border Access to Electronic Evidence in Criminal Matters and Strengthening judicial Cooperation between Member States

MARTIN JANKŮ¹

Abstrakt

S tím, jak se "kybernetické" aspekty stále více stávají součástí trestné činnosti, nabývají na významu elektronické důkazy a možnost širokého přístupu k nim. Uchovávání těchto důkazů mimo jurisdikci státu vyšetřujícího orgánu přimělo orgány činné v trestním řízení aktivně zkoumat možnosti spolupráce se soukromými poskytovateli služeb na dobrovolné bázi. Legislativa EU tento typ spolupráce nedávno formalizovala přijetím nařízení (EU) 2023/1543 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení spolu se směrnicí (EU) 2023/1544. V příspěvku autor objasňuje klíčová ustanovení tohoto nařízení, následně pak kriticky reflektuje garance pro ochranu základních lidských práv s ohledem na privatizaci postupů v oblasti vymáhání práva.

Klíčová slova

elektronické důkazy; evropský vydávací příkaz (EVP); evropský uchovávací příkaz (EUP); poskytovatelé služeb; zásada vzájemného uznávání

Abstract

As cyber-related aspects are increasingly become part of criminal activity, electronic evidence and the possibility of wide access to it are gaining more importance. The storage of this evidence outside the investigating jurisdiction prompted law enforcement authorities to actively explore avenues for collaboration with private service providers on a voluntary basis. This has resulted in the establishment of an informal channel of cooperation, running parallel to those established through mutual legal assistance and the principle of mutual recognition. The EU legislation has recently formalised this type of cooperation by adopting Regulation (EU) 2023/1543 on the European Extradition Order and the European Preservation Order for electronic evidence in criminal proceedings together with Directive (EU) 2023/1544. In this paper, the author explains the key provisions of this Regulation, and then critically reflects the guarantees for the protection of fundamental rights with regard to the privatisation of law enforcement procedures.

1 doc. JUDr. Martin Janků, CSc., Provozně ekonomická fakulta ČZU v Praze

Key words

electronic evidence (e-evidence), European Production Order, European Preservation Order, service providers, principle of mutual recognition

DOI

<http://dx.doi.org/10.37355/fvpk-2025/1-05>

1 Úvod

Rozsáhlé využívání online služeb k dosažení cíle trestných útoků, které často přesahují rámec páčání klasické počítačové kriminality či kyberkriminality (trestné činy při kterých je užito moderních informačních a komunikačních technologií²), zvyšuje význam modernizace a přizpůsobování souboru nástrojů, které policejní a soudní orgány používají k jejich odhalování na vnitrostátní i nadnárodní úrovni. Nedílnou součástí včasné prevence a účinného potírání soudobé trestné činnosti je zejména přístup k elektronickým datům (známým také jako digitální data, což je termín, který zahrnuje různé kategorie dat, jako jsou údaje o účastnících, údaje o provozu či údaje o obsahu v oblasti telekomunikací³). Lze je získat různými způsoby v závislosti na národním právu státu, v jehož jurisdikci jsou elektronické údaje uloženy, na existenci dvoustranných nebo mezinárodních dohod o přeshraničním přístupu k elektronickým údajům nebo důkazům obecně, ale také v důsledku dalších okolností, jako je například to, zda jsou dané údaje volně přístupné či nikoliv.

V praxi je přístup vyšetřujících orgánů k elektronickým údajům poměrně komplikovanou záležitostí. Hlavním důvodem je délka řízení předvídaného existujícími nástroji pro vzájemnou právní pomoc, které - přestože se zaměřují na boj proti kyberkriminalitě, a tedy zohledňují specifika příslušného trestního řízení - byly buď přijaty před rozšířením tzv. *cloud computingu* (poskytování služeb pomocí cloudů), jako např. Budapešťská úmluva o počítačové kriminalitě z roku 2001, nebo - přestože se zabývají přeshraničním přístupem k důkazům v trestním řízení - neobsahují specializovaně ustanovení týkající se elektronických dat vzhledem k jejich krátkému životnímu cyklu, jako např. Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech (dále jen "směrnice o evropském vyšetřovacím příkazu").⁴ Zatímco tedy směrnice o evropském vyšetřovacím příkazu byla přijata na základě zásady vzájemného uznávání rozsudků a soudních rozhodnutí⁵ a vybudovala kanály *spolupráce mezi příslušnými orgány členských států* za účelem provádění vyšetřovacích úkonů, přístup k elektronickým údajům je nakonec většinou zajišťován prostřednictvím *dobrovolné přímé spolupráce*

2 Srov. KOLOUCH, J. *Cyber Crime*. 2016, Praha: CZ.Nic, ISBN 978-80-88168-18-8; online na https://knihy.nic.cz/media/filer_public/46/a9/46a97e3e-4fc7-4598-a73e-a44b2cce5e57/cybercrime-ukazka.pdf

3 Přehled stávajícího právního rámce v členských státech EU viz Smuha, N.: *Towards the EU harmonization of access to cross-border e-evidence*: (2018) *European Criminal Law Review*, 83 a násl.

4 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

5 VAŠKE, V. *Uznání a výkon cizích rozhodnutí v České republice*. Praha: C.H. Beck, 2007. 491 s. ISBN 978-80-7179-614-5.

mezi zahraničními poskytovateli služeb a vnitrostátními vyšetřujícími a soudními orgány.⁶ Vzhledem k tomu, že tato alternativa je rychlejší a méně byrokratická, stala se ve srovnání s využíváním nástrojů vzájemné právní pomoci často využívanou formou spolupráce, i když v praxi ne vždy zaručuje úspěšný výsledek. Podle studie Europolu není zejména přímá spolupráce se zahraničními poskytovateli služeb ve většině členských států EU upravena (alespoň ne výslovně)⁷, což vede k rozdílnému zacházení s žádostmi o spolupráci podanými vnitrostátními orgány jednotlivých států v závislosti na místě usazení poskytovatele služeb. Podle téže studie navíc zůstává nejisté, zda budou údaje získané prostřednictvím dobrovolné spolupráce přípustné jako důkaz před příslušnými vnitrostátními trestními soudy.⁸ A ani spolupráci ze strany poskytovatelů služeb nelze považovat za samozřejmost. Existují různé důvody, jako jsou vzájemně si odporující vnitrostátní právní předpisy, které působí problémy co se týče legálnosti spolupráce se zahraničními policejními a soudními orgány, nedostatek prostředků pro řešení rostoucího počtu žádostí, jakož i či nedostatek vůle k vyhotovení protokolů o spolupráci pro tento účel.⁹

Proto se jako významný průlom jeví nové právní předpisy EU o přeshraničním přístupu k elektronickým důkazům v trestním řízení (dále též "e-důkazy"). Tyto byly přijaty v červenci 2023 po složitých a dlouhých jednáních probíhajících od zveřejnění návrhu Komise v dubnu 2018.¹⁰

Nová pravidla jsou obsažena v nařízení (EU) 2023/1543 (dále jen "nařízení") a směrnici (EU) 2023/1544¹¹ (dále jen "směrnice") a vstoupí v platnost v srpnu 2026.¹² Nařízení směřuje k usnadnění přímé spolupráce mezi příslušnými vnitrostátními orgány a zahraničními poskytovateli služeb působícími v EU bez ohledu na místo jejich usazení, a tedy i jejich přímého zapojení do vymáhání práva. Směrnice potom zajišťuje, aby poskytovatelé služeb, kteří nabízejí služby v EU, aniž by měli stálou pobočku na území EU, jmenovali právního zmocněnce alespoň v jednom členském státě EU za účelem uchovávání a předkládání elektronických důkazů v trestním řízení.

V tomto příspěvku hodláme objasnit některá klíčová ustanovení nařízení. Zaměříme se nejprve na analýzu ustanovení, jež určují pravidla pro přímou spolupráci s poskytovateli

6 Dok. Evropské komise 'Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward' (2017) <https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf>

7 Viz Europol, 'SIRIUS EU Electronic Evidence Situation Report' (2023). Dostupné online <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2023>

8 Tamtéž, s. 42.

9 Tamtéž, s. 16.

10 Evropská komise, Návrh nařízení Evropského parlamentu a Rady o evropských vydávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, COM/2018/225 final - 2018/0108.

11 Směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení.

12 Ucelený přehled klíčových ustanovení obou právních nástrojů viz Juszczak A., Sason, E.: *The use of electronic evidence in the European Area of Freedom, Security and Justice. An introduction to the new EU package on e-evidence* (2023) EUCRIM 2, 182 a násl.

služeb, znamenající posun v privatizaci činností při vymáhání práva. Dále konfrontujeme cíl nařízení upřednostňovat rychlost a účinnost trestní represe s možnými konflikty s národní úpravou práva na obhajobu a ochrany základních lidských práv. V závěru se zmíníme o budoucích problémech, které vyplývají nejen z provádění nové legislativy EU, ale také z rychlého technologického vývoje, umožňujícího mj. přímé získávání důkazů z informačních systémů.

2 Nařízení (EU) 2023/1543 a jeho stěžejní ustanovení

2.1 Předmět a oblast působnosti

Nové nařízení o přeshraničním přístupu k elektronickým důkazům bylo přijato s dvojitým cílem:

- 1) zvýšit efektivitu policejního vyšetřování trestných činů a posílit důvěru v jednotný digitální trh zlepšením bezpečnosti a snížením pocitu beztrestnosti za trestné činy spáchané v online prostředí a
- 2) zajistit přitom ochranu základních práv osob, kterých se takové přeshraniční vyšetřování týká.

Proto nové nástroje, jimiž jsou evropský vydávací příkaz (dále jen "EVP") a evropský uchovávací příkaz (dále jen "EUP"), mohou být vydány nejen z podnětu příslušného orgánu členského státu, ale také na žádost samotné podezřelé nebo obviněné osoby nebo advokáta jednajícího jejím jménem v rámci platného práva na obhajobu a v souladu s vnitrostátním trestním právem procesním. EVP a EUP lze vydat pouze v rámci probíhajícího trestního řízení a pro výkon trestu odnětí svobody nebo ochranného opatření spojeného s odnětím osobní svobody v délce nejméně čtyř měsíců po skončení trestního řízení, který musel být uložen rozhodnutím, jež nebylo vydáno *in absentia* (vzhledem k rozdílným vnitrostátním právním přístupům k této otázce), v případech, kdy odsouzená osoba uniká před spravedlností. Dále je vzhledem k neexistenci harmonizovaného přístupu k trestání právnických osob za trestné činy napříč členskými státy EU vyjasněno, že EVP i EUP mohou být vydány v řízení týkajícím se trestného činu, za který by mohla ve vydávajícím státě nést odpovědnost nebo být potrestána právní osoba. A konečně se nařízení nepoužije na řízení zahájená v rámci vzájemné právní pomoci jinému členskému státu nebo třetí straně.

2.2 Poskytovatelé služeb a e-důkazy: definice a hlavní rozdíly

Poskytovatelé služeb, s nimiž mohou přímo spolupracovat příslušné orgány vydávajícího státu, jsou definováni jako fyzické nebo právní osoby poskytující služby elektronické komunikace, internetových domén a číslování adres internetového protokolu a další služby informační společnosti, které umožňují jejich uživatelům mezi sebou navzájem komunikovat, uchovávat nebo jiné zpracování údajů jménem uživatele. Spojovacím článkem mezi poskytovatelem služeb a vykonávajícím státem není místo uložení údajů určených k vydání nebo uchování, ale místo poskytování služeb v

Unii. To znamená, že EVP a EUP nevycházejí z principu teritoriality, a to především s ohledem na složité uplatňování této zásady v oblasti přístupu k elektronickým údajům a jejich proměnlivé lokalizace. Takové řešení je možné najít i v národní legislativě.¹³ Proto nařízení vyžaduje, aby výše uvedené služby poskytovatele mohly využívat i fyzické nebo právnické osoby v členském státě a aby existovalo podstatné spojení s tímto členským státem. Takové spojení existuje, má-li poskytovatel služeb provozovnu v členském státě, nebo, v případě neexistence takové provozovny, má-li tento poskytovatel významný počet uživatelů/klientů v jednom nebo více členských státech nebo zaměřuje-li svou činnost na jeden nebo více členských států.

Neméně důležité je vymezení elektronických důkazů (e-důkazů) a zejména rozlišení mezi různými kategoriemi údajů, které do této definice spadají. Nařízení se drží tradičního rozlišování mezi:

- a) údaje o účastníkovi,
- b) údaje o provozu a
- c) údaje o obsahu.

Klade přitom důraz na oblast telekomunikací.

Do první kategorie (údaje o účastníkovi) patří údaje, které má poskytovatel služeb a které souvisejí s předplatným jeho služeb, konkrétně údaje, které se týkají totožnosti účastníka nebo zákazníka, typu služby a doby jejího trvání, jakož i údaje související s ověřováním využívání služby (s výjimkou prostředků ověřování totožnosti uživatele, jako jsou hesla). Údaje o provozu souvisejí s poskytováním služby nabízené provozovatelem a poskytují k ní kontext nebo dodatečné informace (např. polohu zařízení, datum, čas, dobu trvání atd.). Údaje o obsahu jsou definovány jako jakákoliv digitální data (např. text, hlasové video), jež nespadají do výše uvedených dvou kategorií.

Nařízení definuje dva různé režimy: první (považovaný za méně rušivý) nabízí větší flexibilitu pro údaje o účastnících a zahrnuje údaje požadované výhradně za účelem identifikace účastníka v rámci konkrétního vyšetřování, jako jsou IP adresy a případně zdrojové porty a časová razítka; druhý (přísnější a více rušivý) režim zahrnující údaje o pohybu, které nejsou požadovány výhradně pro účely identifikace uživatele, a údaje o obsahu.

2.3 Požadavky na vydávání, oznamování a vymáhání EVP a EUP

Výše uvedené rozlišování mezi různými kategoriemi údajů má plošný dopad na několik oblastí úpravy. Za prvé, kategorie údajů, které mají být poskytnuty, určuje, který orgán je oprávněn vydat takový příkaz. EVP k získání údajů o účastníkovi nebo údajů požadovaných výhradně za účelem identifikace uživatele i EUP bude vydávat soudce, vyšetřující soudce nebo státní zástupce či jakýkoli jiný příslušný orgán, který v daném případě jedná jako vyšetřující orgán v trestním řízení s pravomocí nařídit shromažďování důkazů.

¹³ Např. belgický trestní řád spojuje povinnost poskytovatele služeb umožnit přístup k elektronickým datům nikoliv s místem jeho sídla nebo místem uložení dat, ale s faktory, jako je jazyk poskytovaných služeb či doména nejvyšší úrovně (viz Smuha N., op. cit. v pozn. 2).

V druhém případě bude EVP resp. EUP potvrzen soudcem, vyšetřujícím soudcem nebo státním zástupcem. Ale v případech, kdy jsou k předložení požadovány údaje o provozu (s výjimkou údajů požadovaných výhradně za účelem identifikace uživatele) nebo údaje o obsahu, není již uveden jako možný vydávající orgán státní zástupce.

Dále nařízení obsahuje další omezení, neboť EVP k získání údajů o provozu (které nejsou požadovány výhradně pro účely identifikace uživatele) nebo údajů o obsahu může být vydán pouze pro:

- trestné činy, za které lze ve vydávajícím státě uložit trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky;
- bez ohledu na trestní rámec - podvody a padělání bezhotovostních platebních prostředků, pohlavní zneužívání a pohlavní vykořisťování dětí a dětskou pornografii a útoky proti informačním systémům, *pokud jsou zcela nebo zčásti spáchány prostřednictvím informačního systému;*
- trestné činy terorismu, *bez ohledu na způsob jejich spáchání,* a pro výkon trestu odnětí svobody nebo ochranného opatření spojeného s odnětím svobody v trvání nejméně čtyř měsíců uloženého na základě trestního řízení rozhodnutím, které nebylo vydáno *in absentia*.

Nařízení obecně stanoví pro vydání EVP přísnější podmínky než pro vydání EUP. EVP zejména musí být nezbytný a přiměřený vzhledem k vyšetřovanému případu a "může být vydán pouze tehdy, pokud by podobný příkaz mohl být vydán za stejných podmínek v obdobném vnitrostátním případě." (čl. 5 odst. 2 nařízení). Naopak v případě EUP je požadavek přiměřenosti posuzován pouze s ohledem na "účel zabránit odstranění, smazání nebo změně údajů, a bylo tak možné podat následnou žádost o vydání těchto údajů", ať už prostřednictvím vzájemné právní pomoci nebo prostřednictvím EVP (čl. 6 odst. 2 nařízení).

Kromě toho nařízení stanoví další podmínky pro vydání EVP k získání údajů o provozu (s výjimkou údajů požadovaných výhradně za účelem identifikace uživatele) nebo údajů o obsahu v následujících případech:

- údaje chráněné profesní mlčenlivostí podle práva vydávajícího státu, kdy lze EVP vydat pouze tehdy, jestliže osoba vázaná profesní mlčenlivostí má bydliště ve vydávajícím státě, oslovení osoby by mohlo ohrozit vyšetřování nebo pokud byla tato osoba právoplatně zbavena své profesní mlčenlivosti;
- údaje chráněné imunitami nebo výsadami udělenými podle práva vykonávajícího státu nebo se na tyto údaje vztahují v tomto státě pravidla pro určení a omezení trestní odpovědnosti týkající se svobody tisku a svobody projevu v jiných sdělovacích prostředcích, což je případ, kdy si vydávající stát může před vydáním příslušného EVP vyžádat objasnění statusu těchto údajů nebo od něj upustit, pokud riskuje, že dotyčné údaje patří do této zvláštní kategorie.

Tato alternativa souvisí se snahou co nejvíce chránit základní lidská práva osob, které se mohou stát předmětem vyšetřování z důvodu své politické, profesní či dokonce

dobrovolné činnosti (např. členové politických stran, investigativní novináři, členové nevládních organizací atd.)

V dalším kroku jsou EVP či EUP vydávány ve formě certifikátů (v nařízení označovány jako „EPOC“¹⁴), které jsou zpravidla adresovány určené provozovně nebo zástupci dotčeného poskytovatele služeb, výjimečně pak též vykonávajícímu orgánu. Co se posledně uvedeného týče, oznámení vykonávajícímu orgánu se zasílá pouze v případě EVP vydaných za účelem získání údajů o provozu (s výjimkou údajů požadovaných výhradně za účelem identifikace uživatele) nebo údajů o obsahu. Zároveň však nařízení zavádí důležitou výjimku pro oznámení vykonávajícímu orgánu v případech, kdy má vydávající orgán důvodné podezření, že daný trestný čin byl, je nebo pravděpodobně bude spáchán ve vydávajícím státě a dotčená osoba v něm má bydliště.

Oznámení (nebo jeho neučinění) má dopad na časový rámec provedení EPOC. Obecně platí, že poskytovatel služeb předá požadované údaje nejpozději do 10 dnů nebo - v naléhavých případech do 8 hodin po obdržení EPOC. Tyto lhůty se prodlužují v případech, kdy je vyžadováno oznámení vykonávajícímu orgánu, a v závislosti na tom, zda tento orgán uplatnil některý z důvodů pro odmítnutí příkazu (viz dále), nebo potvrdil, že tak učinit nehodlá. Důvody pro odmítnutí EVP zahrnují následující:

- 1) požadované údaje jsou chráněny imunitami nebo výsadami podle práva vykonávajícího státu, které brání provedení nebo výkonu příkazu, nebo se na požadované údaje vztahují pravidla pro určení nebo omezení trestní odpovědnosti, která se týkají svobody tisku nebo svobody projevu v jiných sdělovacích prostředcích;
- 2) provedení EPOC by znamenalo zjevné porušení některého ze základních práv uvedeného v čl. 12 odst. 1 písm. a). 6 Smlouvy o Evropské unii (SEU) a v Listině základních práv EU (LZPS);
- 3) provedení EPOC by bylo v rozporu se zásadou *ne bis in idem*; a
- 4) vyšetřovaný čin nenaplnuje skutkovou podstatu trestného činu podle práva vykonávajícího státu¹⁵, ledaže se jedná o některý z trestných činů uvedených v příloze nařízení, který je ve vydávajícím státě „trestán odnětím svobody nebo ochranným opatřením spojeným se zbavením osobní svobody s horní hranicí trestní sazby v délce nejméně tří let“ (čl. 12 odst. 1 písm. d).

Dále čl. 16 nařízení stanoví postup výkon EVP a EUP v případě, že poskytovatel služeb nevyhoví příslušnému EPOC, aniž by uvedl důvody přijatelné pro vydávající orgán, popř. pokud vykonávající orgán neuvedl žádný z výše uvedených důvodů pro odmítnutí. V tomto případě se EVP stává "klasickým" nástrojem vzájemné právní pomoci a jeho výkon lze odepřít z důvodů vyjmenovaných v nařízení, zejména:

- EVP nebyl vydán pro některý z trestných činů uvedených v nařízení;

¹⁴ Angl. *European Production Order Certificate*.

¹⁵ Tzv. *kritérium dvojího ohrožení (double jeopardy)*.

- je dána faktická nemožnost splnění z důvodu okolností, které poskytovatel služby nemůže ovlivnit, nebo příkaz obsahuje zjevné chyby,
- požadované údaje jsou nedostupné, příp. chráněné imunitami nebo výsadami udělenými podle práva vykonávajícího státu nebo se na ně vztahují pravidla pro určení nebo omezení trestní odpovědnosti, která se týkají svobody tisku nebo svobody projevu v jiných sdělovacích prostředcích;
- výkon EVP by za konkrétních okolností v dané věci vedl ke zjevnému porušení příslušného základního práva dle SEU a LZPS.

Důvody odmítnutí výkonu EUP jsou obdobné.

A konečně nutno uvést, že v případě nesplnění povinností podle uznaného EVP nebo EUP, jehož vykonatelnost potvrdil vykonávající orgán, uloží tento orgán peněžitou sankci ve výši "až 2 % celkového celosvětového ročního obratu poskytovatele služeb dosaženého za předchozí finanční rok" (čl, 15 odst. 1).

2.4 Ochrana základních práv dotčených osob

Nařízení napomáhá vytvoření právního rámce pro přístup k údajům, který se týká jedné z nejintimnějších oblastí soukromí v digitálním věku: obsahu a kontextu telekomunikačních služeb. Tento právní rámec, který klade důraz na rychlost a efektivitu, může vytvářet problémy v souvislosti se zajištěním základních lidských práv. Kompromisní řešení dosažená jako výsledek dlouhotrvajících jednání o obsahu nařízení v rámci unijního dialogu byla přijata s cílem umožnit dotčenému jedinci zasahovat do probíhajících procedur. Je tomu tak například v případě dodržování zásady *ne bis in idem* či požadavku trestnosti jednání podle práva obou států, jehož neexistence představuje důvod pro odmítnutí výkonu EVP, jakož i v případech, kdy vykonávající stát může zasáhnout a uvést tyto důvody pro odmítnutí výkonu EVP či EUP, a to i v případech, kdy mu oznámení nedošlo (viz výše). Tyto kroky mají význam proto, že zapojují do celé procedury vykonávající stát a umožňují mu v rámci jeho jurisdikce zasáhnout a chránit práva dotčených osob.

Neméně důležité je informování osoby, jejíž údaje jsou požadovány (nařízení ji označuje jako „uživatele“). Vydávající orgán bez zbytečného odkladu informuje tuto osobu o poskytnutí údajů na základě EVP. Uvedené informování může být odloženo nebo omezeno, nebo dokonce odepřeno, pokud by byla ohrožena prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkon trestů, a dále aby byla chráněna veřejná, resp. národní bezpečnost, jakož i práva a svobody třetích osob. V takovém případě vydávající orgán uvede ve spisu důvody pro odložení informování, jeho omezení nebo upuštění od něj (včetně stručného odůvodnění).

A konečně nařízení stanoví právo dotčené osoby (podezřelého, obviněného nebo třetí osoby) na účinné prostředky nápravy EVP (nikoli u EUP), přičemž toto právo lze uplatnit pouze u soudů vydávajícího státu.

3 Přímá spolupráce státních orgánů s poskytovateli služeb jako zintenzivnění procedury vymáhání práva

Rozhodnutí EU formalizovat dříve dobrovolnou přímou spolupráci mezi národními vyšetřujícími orgány a poskytovateli služeb v jiných členských státech je reakcí na kritiku malé účinnosti existujících nástrojů vzájemné právní pomoci a zejména evropského vyšetřovacího příkazu. Nicméně je důležité zdůraznit, že směrnice o evropském vyšetřovacím příkazu (č. 2014/41/EU) není implementována v Dánsku a Irsku. Jak známo, oba státy se justiční spolupráce v trestních věcech tradičně účastní pouze v omezené míře, přičemž zejména rozhodnutí Irska o opt-out značně ovlivnilo oblast pohybu e-důkazů, vzhledem k tomu, že v irské jurisdikci sídlí řada evropských poboček nejvýznamnějších technologických společností (např. Meta, Microsoft, Google).¹⁶

Model přímé spolupráce představuje podstatné omezení národní suverenity vykonávajícího státu, tj. státu, v němž má poskytovatel služeb provozovnu. Toto omezení, pokud vyplývá z mezinárodní smlouvy, může být uplatňováno na základě zásady mezinárodního práva, podle níž suverenní státy mohou jednat jakýmkoli způsobem, pokud tím neporušují výslovný zákaz.¹⁷ V oblasti přeshraniční justiční spolupráce v trestních věcech na úrovni EU i Rady Evropy se ovšem jedná o široké sebeomezení států.¹⁸ Za zmínku zejména stojí, že použití nařízení EU jako legislativního nástroje významně omezuje diskreci národního zákonodárce v oblasti justiční spolupráce, a to na základě čl. 82 odst. 1 SFEU, který představuje základní ustanovení primárního práva EU týkající se justiční spolupráce mezi členskými státy v trestních věcech a právní základ pro vytvoření kanálů přímé spolupráce vyšetřujících orgánů s poskytovateli služeb...

Podle čl. 82 odst. 1 SFEU představuje základ justiční spolupráce v trestních věcech na úrovni EU zásada vzájemného uznávání. Ačkoli toto ustanovení nepřisuzuje pojmu vzájemné uznávání konkrétní význam ani neuvádí, že se nezbytně musí týkat spolupráce mezi vnitrostátními orgány veřejné moci, zcela nepochybně se týká *justiční* spolupráce, což je pojem, nezahnující soukromé subjekty.¹⁹ Zásada vzájemného uznávání si bere za vzor jiný unijní právní rámec, a sice *evropské hospodářské právo*. Je proto často argumentováno, že by měla být vykládána flexibilním způsobem a že v této souvislosti existuje prostor pro zohlednění nejnovějšího technologického vývoje, mj. zejména rostoucího významu přeshraničního přístupu k elektronickým důkazům.²⁰ Přijetí takového názoru však nebere v úvahu odlišné politické souvislosti *evropského trestního práva* ve srovnání s evropským hospodářským právem, neboť v případě toho druhého uplatňování zásady vzájemného uznávání umožňuje volný pohyb osob, zboží a služeb, zatímco v případě trestního práva se

¹⁶ V takovém případě se nadále použije Evropská úmluva o vzájemné pomoci v trestních věcech z roku 1959.

¹⁷ Zásada je odvozována z rozhodnutí PCIJ v případě *Lotus* (1929) – blíže viz Hertogen A. Letting *Lotus Bloom*, *European Journal of International Law*, Volume 26, Issue 4, November 2015, s. 901–926, <https://doi.org/10.1093/ejil/chv072>

¹⁸ TOSZA, S. *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?* (2023) *EDPL* 2, s. 165.

¹⁹ *Tamtéž*, s. 169.

²⁰ Gless, S. *Zum Prinzip der gegenseitigen Anerkennung* (2004) *ZStW* 116 (2), s. 353 ad.

dotýkáme omezení základních svobod jako ústavního základu národních právních řádů.²¹ Kromě toho je tato omezující funkce uplatňována v kontextu, který neznamená sbližování vnitrostátních právních úprav v procesních otázkách jako celku, a tedy zahrnujících např. též ochranu práva na obhajobu, neboť směrnice přijaté na základě Usnesení Evropské rady ze dne 30. listopadu 2009 o „cestovní mapě pro posílení procesních práv podezřelých nebo obviněných osob v trestním řízení“ se tímto regulačním aspektem blíže nezabývaly.²² V každém případě je třeba poznamenat, že již před přijetím návrhu Komise EU na zlepšení přeshraničního přístupu k elektronickým důkazům byly právní přístupy jednotlivých členských států dosti rozdílné, nejen pokud jde o otázky související s nezbytnou vazbou na národní právní řády při činění vyšetřovacích úkonů s přeshraničními účinky, ale také s ohledem na procesní záruky, které jsou poskytovány osobám, jichž se tyto vyšetřovací úkony dotýkají. Vzhledem k tomu existovaly v národních úpravách značné diskrepance mezi postupným rozšiřováním postupů při činění vyšetřovacích úkonů a ochranou práv podezřelých nebo obviněných osob. Nařízení se touto otázkou nezabývá, neboť se nezabývá výkonem práva na obhajobu dotčených osob, s výjimkou toho, že samotnému podezřelému nebo obviněnému přiznává právo požádat o vydání EVP nebo EUP v rámci platné národní úpravy práva na obhajobu.

Je však pravda, že spolupráce se soukromými subjekty, zakotvená v nařízení, není první unijní úpravou v této oblasti. Právní rámec EU pro boj proti praní špinavých peněz je zřejmě nejreprezentativnějším příkladem norem, jimiž je soukromým osobám, nazývaným zde jako povinné subjekty, uložena řada povinností v oblasti náležité péče. Vyvolává to otázky ohledně vhodnosti decentralizace rozhodování týkajícího se trestního soudnictví, jež má dopad na jeho výkon.²³

Připomenout můžeme ještě některé další příklady, jako je existence mechanismů *whistleblowingu* v soukromém i veřejném sektoru, fungování programů resp. útvarů pro trestněprávní *compliance* v soukromých firmách či tzv. interní investigace.²⁴ Nově přijatý unijní předpis o přeshraničním přístupu k elektronickým důkazům však posunuje rozsah zapojení soukromých subjektů do výkonu veřejného práva na novou úroveň, která překračuje rámec pouhé samoregulace a zasahuje do oblasti výkonu veřejných povinností, včetně posuzování zákonnosti, přiměřenosti či ochrany základních lidských práv. Návrh nařízení o přeshraničním přístupu k elektronickým důkazům, předložený Komisí, poprvé vyslovil myšlenku privatizace vzájemné právní pomoci, včetně právních norem ukládajících poskytovatelům služeb dokonce i povinnost zkoumat, zda příslušný EVP zjevně neporušuje základní lidská práva nebo není zjevně zneužitelný, a přitom na druhé straně obsahuje hrozbu sankcí, které mohou být uloženy v případě nedodržení

²¹ Tamtéž, s. 358.

²² Srov. doc. 2009/C 295/01, online na [https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009G1204\(01\)](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009G1204(01))

²³ Blíže viz VAVOULA, N. *The evolving EU anti-money laundering regime. Challenges for fundamental rights and the rule of law* Maastricht Journal of European and Comparative Law. 2016, no. 2, s. 261 a násl.

²⁴ NÁHLOVSKÁ, E. Význam etického kodexu pro trestněprávní compliance. Advokátní deník. 16. 1. 2016 Dostupné online: <https://advokatnidenik.cz/2020/01/16/vyznam-etického-kodexu-pro-trestnepravni-compliance/>

povinností po obdržení vykonatelného příkazu.²⁵ V této podobě však návrh nebyl do konečné verze nařízení zahrnut. Nařízení nakonec stanoví pouze oznámení EVP k získání dat o provozu (s výjimkou údajů určených výhradně k identifikaci uživatele) nebo dat o obsahu vykonávajícímu orgánu, které může vést k uplatnění některého z důvodů k jeho odmítnutí (viz výše), mezi nimiž je i zjevné porušení příslušného základního práva uvedeného v čl. 6 Smlouvy o EU či v LZPS. Z toho tedy nutně vyplývá, že ve všech *ostatních případech* je to poskytovatel služeb, od něhož se očekává, že bude fungovat jako jakýsi „detektor“ porušení základních práv a při jeho zjištění odmítne vykonat příslušný EVP či EUP, čímž spustí mechanismus podle čl. 16 nařízení („Výkon příkazu“). Pokud však vykonávající orgán dospěje k opačnému závěru, tedy že k porušení základních práv vydáním EVP nedochází a příkaz má být vykonán, poskytovatel služeb při odmítnutí stále čelí riziku uložení sankce podle čl. 15 nařízení. To znamená, že poskytovatel služeb je postaven před dilema „splnění nebo potrestání“, dilema, které může být mj. ovlivněno i nedostatkem potřebných odborných znalostí (pokud jde o posouzení, v jakých případech může být vydání příkazu k poskytnutí nebo uchování dat v rozporu se základními právy), krátkými lhůtami k provedení a velkým počtem příkazů, které musí vykonat. Současné ale mohou být výše zmíněné „ostatní případy“, tj. situace, za nichž vykonávající stát nemá žádnou či skoro žádnou možnost zasáhnout z důvodu chybějícího oznámení, tvořeny žádostmi pocházejícími z vydávajícího státu, který se snaží identifikovat zranitelné osoby, jako jsou kupř. novináři, kteří mohou vyšetřovat skandál kolem politické korupce v tom samém státu.²⁶

Tento regulační rámec je komplikován skutečností, že poskytovatelé služeb jsou soukromými subjekty, které se řídí především korporátními zájmy. Soukromé společnosti sice často vyvíjejí iniciativy ve prospěch veřejných zájmů (např. v oblasti firemního etického kodexu a odpovědnosti firmy), ale zejména tehdy, pokud to zároveň (nebo především) slouží jejich veřejnému image nebo korporátní agendě.

To ale ještě neznamena, že jim může či měl by být svěřen výkon veřejné moci. Ta naopak vyžaduje nestrannost a nezávislost, což jsou kvality, které často nejsou vlastní soukromým společnostem, ani v souladu s jejich podnikatelskými zájmy. Při prosazování těchto zájmů může dokonce dojít k vykonání potenciálně zneužívajícího EVP či EUP, jen aby tyto subjekty zamezily uvalení sankcí. Je tomu tak zejména proto, že peněžité sankce mají nepříznivý dopad nejen na podnikový rozpočet, ale znamenají také poškození pověsti a další možné finanční ztráty, pokud je například odmítnutí splnit určitý EVP veřejností vnímáno jako krytí vyšetřovaného protiprávního jednání. Kromě toho jsou hodnotové soudy, které patří do veřejné sféry, spojeny s veřejnoprávními pravidly přijímání (politické) zodpovědnosti, zatímco zaměstnanci soukromé firmy se zodpovídají akcionářům a vlastníkům společnosti. Navíc může být s přenesením výkonu veřejné moci do soukromého sektoru spojeno i riziko zneužití moci či její výkon pod vlivem korupce.

25 MITSILEGAS, V. *Privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*. *Maastricht Journal of European and Comparative Law*, 2018, No. 25, s. 263 et sd.

26 Viz EDRI, „e-Evidence“ trilogues: what's left of fundamental rights safeguards' (2022) online <https://edri.org/our-work/e-evidence-trilogues-whats-left-of-fundamental-rights-safeguards/>

4 Závěr a vývoj *de lege ferenda*

Iniciativa unijního normotvůrce upravit přeshraniční přístup k elektronickým důkazům v trestním řízení ukazuje rostoucí význam tzv. druhé generace forenzních důkazů, která zahrnuje mimo jiné i digitální data.²⁷ Jejich používání znamená nutnost zajistit, aby se občané seznámili s vlastnostmi těchto důkazů, a aby byla vytvořena správná infrastruktura pro jejich zpracování, včetně poskytnutí potřebných procesních záruk v trestním řízení, zahrnujícím využití elektronických důkazů získaných prostřednictvím EVP.

V tomto ohledu jsou formulace přijaté ve finální verzi nařízení a z nich vyplývající normativní důsledky problematické na více úrovních. Kladou totiž zvýšený důraz na trestní represi a efektivitu vymáhání práva, a to i za cenu oslabení ochrany základních lidských práv. Z této obecné tendence je jasnou výjimkou pouze výslovné uznání práva podezřelého nebo obviněné osoby požádat (ve prospěch jejího práva na obhajobu) o vydání EVP nebo EUP.

Nedostatek harmonizovaných pravidel pro přípustnost elektronických důkazů však představuje problém, který se stane ještě naléhavější vzhledem k rodící se třetí generaci forenzních důkazů, které budou generovány *přímo* informačními systémy.²⁸ Zatímco elektronické důkazy zahrnují mimo jiné údaje o obsahu, které mohou být vyměňovány prostřednictvím aplikace pro výměnu rychlých zpráv (*instant messaging*), důkazy generované umělou inteligencí (AI) budou zahrnovat například výstupy detektoru falzifikátů (*deepfake*), který zkoumá pravost výše uvedených údajů o obsahu (např. hlasová pošta) s pomocí AI. Prozatím jen málo národních zákonodárců podniklo kroky k regulaci používání důkazů generovaných AI. Snahy EU samotné vyvrcholily přijetím *AI Act* (2024), nařízení, kterým se stanoví harmonizovaná pravidla pro využití umělé inteligence.²⁹ To může mít nepřímý dopad na používání AI v oblasti trestního soudnictví, ale rozhodně se nezaměřuje na otázky, které se týkají trestního řízení a provádění důkazů. To znamená, že v oblasti trestního soudnictví, které se stále ještě přizpůsobuje digitálnímu prostředí, bude brzy postaveno před nutnost kategorizace nové generace důkazů, jejichž dekodování bude z větší či menší části v rukou soukromého sektoru, což před něj postaví další problémy související s tím, jak zajistit ochranu základních práv.

Literatura

DASKAL, J. Unpacking the CLOUD Act' (2018) *EUcrim* 4, s. 220 ad.

27 K nové „druhé generaci“ forenzních důkazů, které se vyznačují vysokou mírou průkaznosti, viz např. Murphy E.: *Inferences, Arguments, and Second Generation Forensic Evidence*, (2008) 59 *Hastings L.J.* 1047. Online na https://repository.uclawsf.edu/hastings_law_journal/vol59/iss5/4

28 See GLESS, S. *AI in the courtroom: a comparative analysis of machine evidence in criminal trials* (2020) *Georgetown Journal of International Law* 51, s. 195 a násl.

29 COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). Plný text online <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html>

EDRI. “e-Evidence” trilogues: what’s left of fundamental rights safeguards’ (2022). Dostupné z: <https://edri.org/our-work/e-evidence-trilogues-whats-left-of-fundamental-rights-safeguards/>>

EU. doc. 2009/C 295/01. Dostupné z: [https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009G1204\(01\)](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009G1204(01))

EU. Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward (2017) Online. Dostupné z: https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf

EUROPOL. SIRIUS EU Electronic Evidence Situation Report (2023). Online. Dostupné z: <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2023>

GLESS, S. Zum Prinzip der gegenseitigen Anerkennung. (2004) *ZStW* 116 (2), s. 353 a násl.

HERTOGEN, A. Letting Lotus Bloom, *European Journal of International Law*, Volume 26, Issue 4, November 2015, s. 901–926, Dostupné z: <https://doi.org/10.1093/ejil/chv072>

JUSZCZAK, A. and E. SASON. The use of electronic evidence in the European Area of Freedom, Security and Justice. An introduction to the new EU package on e-evidence (2023) *EUcrim* 2, 182 a násl.

KOLOUCH, J. Cyber Crime. 2016, Praha: CZ.Nic. Online. Dostupné z: https://knihy.nic.cz/media/filer_public/46/a9/46a97e3e-4fc7-4598-a73e-a44b2cce5e57. ISBN 978-80-88168-18-8.

MITSOLEGAS, V. Privatisation of mutual trust in Europe’s area of criminal justice: The case of e-evidence. *Maastricht Journal of European and Comparative Law*, 2018, No. 25, s. 263 a násl.

MURPHY, E. Inferences, Arguments, and Second Generation Forensic Evidence, (2008) 59 *Hastings L.J.* 1047. Online. Dostupné z: https://repository.uclawsf.edu/hastings_law_journal/vol59/iss5/4

NÁHLOVSKÁ, E. Význam etického kodexu pro trestněprávní compliance. *Advokátní deník*. 16. 1. 2016. Online. Dostupné z: <https://advokatnidenik.cz/2020/01/16/vyznam-etickeho-kodexu-pro-trestnepravni-compliance/>

PASTRANA, A. The Proposal on Electronic Evidence in the European Union’ (2021). *Global Affairs* 7, 777 (s. 785 ad.).

SMUHA, N. Towards the EU harmonization of access to cross-border e-evidence. (2018). *European Criminal Law Review*, 83 a násl.

TOSZA, S. The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One? (2023). *EDPL* 2, s. 165.

VAŠKE, V. Uznání a výkon cizích rozhodnutí v České republice. Praha: C.H. Beck, 2007. 491 s. ISBN 978-80-7179-614-5.

VAVOULA, N. The evolving EU anti-money laundering regime. Challenges for fundamental rights and the rule of law. *Maastricht Journal of European and Comparative Law*. 2016, no. 2, s. 261 a násl.

WIECZOREK, I. The emerging role of the EU as a primary normative actor in the EU Area of Criminal Justice’ (2021). *European Law Journal* 27, s. 349 a násl.