Cezhraničné zaist'ovanie digitálnych dôkazov ako prostriedok boja proti závažnej trestnej činnosti¹

Cross-border Taking of Digital Evidence as a Means of Combating Serious Crime

LUCIA HRDLÍČKOVÁ²

Abstrakt

Príspevok sa vo svojom obsahu zameriava na problematiku cezhraničného zabezpečovania elektronických dôkazov, ktoré predstavuje prostriedok trestného práva procesného s nezastupiteľným významom v boji proti viacerým závažným druhom trestnej činnosti, akou je napríklad trestná činnosť spojená so zásahmi do života alebo zdravia jednotlivca, drogová trestná činnosť či korupčná trestná činnosť. Cieľom príspevku je identifikovať základný právny rámec cezhraničného poskytovania elektronických dôkazov predovšetkým s akcentom na odpočúvanie a záznam telekomunikačnej prevádzky a objektívne zhodnotiť možnosti zabezpečovania digitálnych dôkazov, a to tak v rámci USA, ako aj v rámci priestoru Európskej únie (ďalej len „EÚ“).

Kľúčové slová

elektronické dôkazy, odpočúvanie a záznam telekomunikačnej prevádzky, Dohovor o počítačovej kriminalite, európsky vyšetrovací príkaz, ochrana života a zdravia

Abstract

The content of the article focuses on the issue of cross-border provision of electronic evidence, which is a means of criminal procedural law of irreplaceable importance in the fight against several serious types of crime, such as crime related to interference with life or health of individuals, drug crime or corruption. criminal activity. The aim of the paper is to identify the basic legal framework for the cross-border provision of electronic evidence, especially with an emphasis on interception and recording of telecommunications traffic and to objectively evaluate the possibilities of securing digital evidence, both within the US and within the European Union (EU).

Key words

electronic evidence, interception and recording of telecommunications traffic, Convention on Cybercrime, European Investigation Order, protection of life and health

DOI

<http://dx.doi.org/10.37355/fvpk-2021/3-04>

¹ Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-16-0106. This work was supported by Slovak Research and Development Agency under the Contract No. APVV-16-0106.

² JUDr. Lucia Hrdličková, Právnická fakulta Trnavskej univerzity v Trnave, Katedra trestného práva a kriminológie, Okresná prokuratúra Senica

Úvod

Boj s kriminalitou, ktorý je súčasťou represívnej politiky štátu, má za primárny cieľ zabezpečiť ochranu jeho základných hodnôt, akými sú najmä život, zdravie, majetok občanov a bezpečnosť spoločnosti. K naplneniu tohto cieľa disponuje štát niekoľkými prostriedkami, ktorých použitie musí byť odôvodnené verejným záujmom. Problematiku zabezpečenia ochrany života a zdravia jedincov možno zaradiť medzi najvýznamnejšie a najdiskutovanejšie otázky v podmienkach trestného práva. Na potrebu garantovania dostatočnej ochrany života a zdravia ľudí je potrebné brať ohľad aj vo sfére celosvetovej spolupráce v trestných veciach, v rámci ktorej dochádza k aplikácii určitých právnych nástrojov priamo sa dotýkajúcich sféry života a zdravia. V uvedenom kontexte je z hľadiska trestného práva procesného potrebné upírať pozornosť predovšetkým na potrebu rýchleho a efektívneho zabezpečenia dôkazov, a to predovšetkým za účelom včasného odhalenia páchatelia trestného činu a ochrany spoločnosti.

V ostatnej postmodernej dobe, ktorá sa vyznačuje sústavným a relatívne neobmedzeným pohybom osôb za hranice štátu, sa možno čoraz častejšie stretnúť s páchaním trestnej činnosti, ktorá siaha až za hranice toho-ktorého štátu. Z pohľadu aplikačnej praxe možno v cezhraničnej trestnej činnosti v rámci justičnej spolupráce badať predovšetkým sofistikovanejšie a rafinovanejšie páchanie trestnej činnosti, napr. pri špecifických druhoch drogových trestných činov). Vzhľadom na všetky vyššie uvedené skutočnosti je potrebné, aby sa krajiny snažili nájsť nielen vnútroštátne, ale aj medzinárodné koncepcie, ktoré zodpovedajú súčasným požiadavkám spoločenskej reakcie na trestnú činnosť.

1 Elektronické dôkazy v medzinárodnom a európskom kontexte

Pojem elektronické, resp. digitálne dôkazy, sa vzťahuje nielen k odpočúvaniu, ale aj k oznámeniu údajov o telekomunikačnej prevádzke, a to aj v prípade, ak sú údaje prenášané prostredníctvom počítačového systému.³ Pod elektronickými dôkazmi je potrebné rozumieť akúkoľvek informáciu s určitou výpovednou, resp. dôkaznou hodnotou, ktorá je relevantná pre trestné konanie, bola získaná zákonným spôsobom a je prenášaná alebo uchovávaná v digitálnej podobe.⁴ Elektronickými dôkazmi teda budú akékoľvek dôkazy nachádzajúce sa v elektronickej forme, ako napr. údaje o telekomunikačnej prevádzke alebo údaje zo sociálnych sietí či rôznych komunikačných platforiem. Sú to dôkazy, ktoré sú uložené v elektronickej podobe podnikom poskytujúcim verejné služby alebo siete a zahŕňajú prevádzkové údaje, lokalizačné údaje, obsahové údaje, údaje o predplatiteľoch, o prístupe apod. Elektronické dôkazy sú v súčasnosti potrebné približne pri 85 % vyšetrovaných trestných činov a v dvoch tretinách je potrebné ich získať od poskytovateľov služieb so sídlom v zahraničí. V rozmedzí rokov 2013 až 2018 bol zaznamenaný výrazný

3 Primerane pozri § 115 ods. 11 a § 116 ods. 6 zákona č. 301/2005 Trestný poriadok v znení neskorších predpisov (ďalej len „Trestný poriadok“).

4 POLČÁK, R. a kol. Elektronické dôkazy v trestním řízení. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 91.

vzostup žiadostí o poskytnutie elektronických dôkazov poskytovateľom tzv. online služieb.⁵ Pokiaľ ide o delenie elektronických dôkazov, tieto možno rozdeliť podľa toho, či sú uložené na pevnom zariadení (napr. na mobilnom telefóne, počítači alebo tablete) alebo sa nachádzajú len v operačnej pamäti (software), na perzistentné a volatilné.⁶

1.1 Základný právny rámec poskytovania elektronických dôkazov

V súvislosti s cezhraničným zabezpečovaním digitálnych dôkazov je potrebné poukázať na právny rámec pozostávajúci z medzinárodných zmlúv, dohovorov a smerníc, vďaka ktorým možno na základe žiadosti o právnu pomoc dožadujúceho štátu adresovanej štátu dožadovanému predmetné dôkazy zabezpečiť. Uvedený právny rámec elektronických dôkazov pozostáva z:

- Dohovoru o počítačovej kriminalite (oznámenie FMZV č. 137/2008 Z. z.),
- Dohovoru Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním (oznámenie FMZV č. 164/2016 Z. z.),
- Európskeho dohovoru o vzájomnej pomoci v trestných veciach (oznámenie FMZV č. 550/1992 Zb.) a jeho dvomi dodatkovými protokolmi (oznámenie FMZV č. 12/1997 Z. z. a č. 165/2005 Z. z.),
- Dohovoru o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie a protokol k nemu (oznámenie FMZV č. 572/2006 Z. z.),⁷
- Smernice Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV,
- Smernice Európskeho parlamentu a Rady 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV (transpozícia do 31. 5. 2021),
- Smernice Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach (a s ňou súvisiaceho zákona č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach).

Pokiaľ ide o načrtnutú právnu úpravu týkajúcu sa zabezpečovania elektronických dôkazov, je potrebné uviesť, že neustále napredovanie a vývoj komunikačných a informačných technológií so sebou prináša okrem mnohých výhod tiež výzvy, a to predovšetkým v súvislosti s odhaľovaním a dokazovaním trestnej činnosti a prevenciou

5 *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, Brussels, 5. 2. 2019, COM(2019) 70 final.

6 *Data Recovery Specialists: What is volatile data? There are two types of data sources, persistent and volatile, but how does this effect an investigation?* [online] (cit. 18. 3. 2021). Dostupné na: <http://www.datarecoveryspecialists.co.uk/blog/what-is-volatile-data>

7 *V súvislosti s odpočúvaním je dôležité aj Odporúčanie Výboru ministrov Rady Európy Rec(85)10 z 28. júna 1985, a to predovšetkým pre stanovenie podmienok pre odmietnutie žiadosti o právnu pomoc a náležitosti žiadosti o právnu pomoc pri odpočúvaní a zázname telekomunikačnej prevádzky.*

kriminality. Napriek tomu, že stopy vo forme elektronických dôkazov sa zachovávajú v kybernetickom priestore a štáty majú k dispozícii pri ich cezhraničnom zabezpečovaní k dispozícii vyššie uvedený právny rámec, sú právomoci štátov v oblasti presadzovania práva a zabezpečovania elektronických dôkazov stále obmedzené a nedostatočné. V nadväznosti na uvedené tak možno vymedziť i pripravovanú právnu úpravu, a to:

- Druhý dodatkový protokol k Dohovoru Rady Európy o počítačovej kriminalite,⁸
- Dohoda medzi Európskou úniou a USA o zabezpečovaní elektronických dôkazov,⁹
- Tzv. legislatívny balík EÚ k elektronickým dôkazom,¹⁰ ktorý tvorí:
 - Návrh nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach, a

8 Bližšie pozri *Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185)*, Brussels, 5. 2. 2019, COM(2019) 71 final.

9 Bližšie pozri *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, Brussels, 5. 2. 2019, COM(2019) 70 final.

10 Predmetné príkazy majú za cieľ poskytnúť príslušným orgánom členského štátu možnosť faktického uchovávanía alebo predloženia elektronických údajov na účely trestného konania zo strany poskytovateľov služieb elektronickej komunikácie, ktorí majú sídlo alebo zastúpenie v inom členskom štáte. Európsky príkaz na predloženie elektronických dôkazov je v zmysle návrhu nariadenia definovaný ako záväzné rozhodnutie vydávajúceho orgánu jedného členského štátu, ktorým sa nariaďuje poskytovateľovi služieb predložiť elektronické dôkazy. Európsky príkaz na uchovanie údajov má však iba určitý preventívny charakter, nakoľko má umožniť zabránenie odstránenia, vymazania alebo zmeny relevantných údajov v prípadoch, kedy dosiahnutie predloženia uvedených údajov môže trvať dlhší čas. Po vydaní predmetného príkazu teda bude potrebné, aby nasledovalo vykonanie úkonu vzájomnej právnej pomoci, vydanie európskeho vyšetrovacieho príkazu alebo európskeho príkazu na predloženie dôkazov. Na to, aby bolo možné predmetné príkazy vydať, je potrebné, aby:

- a) sa jednalo o uložené údaje (poskytovatelia služieb nimi disponujú v čase prijatia osvedčenia o európskom príkaze),
- b) údaje spadali do jednej z kategórií predpokladaných nariadením (údaje o predplatiteľoch, údaje o prístupe, údaje o transakciách alebo obsahové údaje).

K základným výhodám, ktoré predmetné nariadenie priniesie, možno zaradiť predovšetkým určenie jurisdikcie, podľa ktorej budú predmetné príkazy na predloženie a uchovanie dôkazov adresované právnomu zástupcovi určenému poskytovateľom služieb na účel zhromažďovania dôkazov v trestnom konaní. V naznačenom kontexte nariadenie upravuje aj situáciu, ktorá spôsobuje v aplikačnej praxi jedny z najzásadnejších problémov, a to uchovávanie údajov o užívateľoch z Európy providermi so sídlom v USA. Inými slovami, dotknuté nariadenie sa bude vzťahovať bez rozdielu na všetkých providerov, ktoré poskytujú služby v rámci územia EÚ, bez ohľadu na to, v ktorej krajine bol ten-ktorý provider založený. V neposlednom rade je potrebné veľmi kladne hodnotiť predovšetkým stanovenie lehôt na získanie vyžadovaných údajov, ktoré je určené na 10 dní od prijatia žiadosti (pri nebezpečenstve hroziacom pre život alebo zdravie iných je lehota poskytnutia údajov stanovená na 6 hodín).; bližšie pozri *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, Strasbourg, 17. 4. 2018 COM(2018) 225 final, 2018/0108(COD) a *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, Strasbourg, 17. 4. 2018 COM(2018) 226 final, 2018/0107(COD).

- Návrh smernice Európskeho parlamentu a Rady, ktorou sa stanovujú harmonizované pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

2 Právna pomoc na základe Dohovoru o počítačovej kriminalite vo vzťahu k USA

Na základe Dohovoru o počítačovej kriminalite môže byť realizované tak cezhraničné poskytnutie elektronických dôkazov, ako aj realizácia cezhraničného odpočúvania telekomunikačnej prevádzky, a to predovšetkým s poukazom na to, že všetky telekomunikačné systémy fungujú v digitálnom priestore, pričom po splnení Dohovorom o počítačovej kriminalite stanovených podmienok môže jeden členský štát „vstúpiť“ aj za hranice svojho digitálneho priestoru do priestoru iného zvrchovaného štátu. Dohovor o počítačovej kriminalite bol otvorený na podpis dňa 23. novembra 2001 v Budapešti, pričom Národná rada Slovenskej republiky vyslovila súhlas s predmetným dohovorom uznesením č. 583 zo dňa 23. októbra 2007. Prezident Slovenskej republiky ratifikoval dohovor dňa 12. decembra 2007 a ratifikačná listina bola dňa 8. januára 2009 uložená u depozitára Dohovoru o počítačovej kriminalite – generálneho tajomníka Rady Európy. Dohovor o počítačovej kriminalite nadobudol pre Slovenskú republiku platnosť dňa 1. mája 2008 a je prijatý pod oznámením Ministerstva zahraničných vecí Slovenskej republiky č. 137/2008 Z. z.

Pokiaľ ide o rozsah Dohovoru o počítačovej kriminalite, tento je vymedzený jeho článkom 23 a článkom 25. Zmluvné strany¹¹ spolupracujú v súlade s príslušnými ustanoveniami Dohovoru o počítačovej kriminalite, za použitia vymedzených nástrojov na medzinárodnú spoluprácu v trestných veciach, a to na účely vyšetrovania trestných činov alebo konania o trestných činoch, ktoré súvisia s počítačovými systémami a údajmi, ako aj na účely zhromažďovania dôkazov o trestnom čine v elektronickej forme.¹² Dohovor o počítačovej kriminalite sa vzťahuje na počítačové trestné činy, trestné činy týkajúce sa detskej pornografie, ako aj trestné činy týkajúce sa porušenia autorských a príbuzných práv. V nadväznosti na problematiku odpočúvania je potrebné osobitne poukázať na čl. 3 predmetného dohovoru, ktorý zakotvuje pre zmluvné strany potrebu prijatia legislatívnych opatrení vo vzťahu k nezákonnému zachyteniu údajov. V rámci slovenského právneho poriadku možno nájsť vyjadrenie čl. 3 Dohovoru o počítačovej kriminalite v § 247c Trestného zákona s názvom trestný čin neoprávneného zachytávania počítačových údajov, ktorý postihuje porušenie práva na súkromie inej osoby pri komunikácii a platí pre každú formu elektronického prenosu údajov, a to prostredníctvom telefónu, e-mailu, faxu alebo prenosom súborov.¹³ Podľa čl. 25 ods. 1 Dohovoru o počítačovej kriminalite si

11 Ku dňu 12. marca 2021 ratifikovalo Dohovor o počítačovej kriminalite spolu 65 štátov, a to či už členských alebo nečlenských štátov Rady Európy; zoznam štátov je dostupný online na internetovej stránke: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>

12 Čl. 23 Dohovoru o počítačovej kriminalite.

13 KLIMEK, L., J. ZÁHORA a K. HOLCR. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, 2016, s. 176.

zmluvné strany na účely vyšetrovania trestných činov alebo konania o trestných činoch, ktoré súvisia s počítačovými systémami či údajmi a zhromažďovania dôkazov o trestných činoch v elektronickej forme, v čo najširšom rozsahu poskytujú pomoc. Naznačená možnosť právnej pomoci spočíva v oprávnení príslušných štátov, ktoré sú zmluvnými stranami Dohovoru o počítačovej kriminalite, zasielať iným zmluvným stranám tohto dohovoru žiadosti o právnu pomoc. Vybavenie právnej pomoci závisí od vnútroštátnym právnym poriadkom ustanovených podmienok dožiadanej strany alebo od podmienok ustanovených príslušnými použiteľnými zmluvami o právnej pomoci, vrátane dôvodov odmietnutia spolupráce.¹⁴

V nadväznosti na právnu úpravu Dohovoru o počítačovej kriminalite v podmienkach Slovenskej republiky je subjektom príslušným na zasielanie a prijímanie žiadostí Ministerstvo spravodlivosti Slovenskej republiky, ktoré je spolu s Generálnou prokuratúrou Slovenskej republiky aj ústredným orgánom. Kontaktným miestom je Prezídium Policajného zboru, Úrad medzinárodnej policajnej spolupráce, Národná ústredňa Interpol Bratislava a orgánom príslušným na prijatie žiadosti o predbežnú väzbu je príslušný prokurátor krajskej prokuratúry spolu s Ministerstvom spravodlivosti Slovenskej republiky. Pokiaľ ide o zaslanie žiadosti o predbežnú väzbu, oprávneným orgánom je Ministerstvo spravodlivosti Slovenskej republiky a súd príslušný na vydanie medzinárodného zatýkacieho rozkazu. Slovenská republika si vyhradila právo odmietnuť vykonanie žiadosti o uchovanie údajov vtedy, ak má dôvod sa domnievať, že v čase sprístupnenia nemožno splniť podmienku obojstrannej trestnosti skutku. Slovenská republika si taktiež vyhradila právo vyžadovať pre trestnosť konania spočívajúceho v zasahovaní do údajov podľa čl. 4 ods. 1 následok v podobe spôsobenia značnej škody.

V kontexte odpočúvania ďalej možno vymedziť opatrenia vzájomnej pomoci týkajúcej sa vyšetrovacích právomocí podľa čl. 33 a čl. 34 Dohovoru o počítačovej kriminalite, ktoré upravujú vzájomnú pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase a vzájomnú pomoc týkajúcu sa zachytenia obsahových údajov.

V súvislosti s cezhraničným zabezpečovaním elektronických dôkazov možno konštatovať, že jednou z najvyťaženejších krajín pri zasielaní žiadostí o právnu pomoc najviac spočívajúcu v poskytnutí predmetných dôkazov je práve USA, nakoľko na ich území sídlia najväčší poskytovatelia služieb.¹⁵ Na tomto mieste je potrebné uviesť, že EÚ a USA podpísali dňa 23. júna 2003 Dohodu o vzájomnej právnej pomoci s platnosťou odo dňa 1. februára 2010. Predmetná dohoda je kľúčovým a základným mechanizmom pre účinnú transatlantickú spoluprácu v oblasti trestného súdnictva, boja proti terorizmu či organizovanej trestnej činnosti.¹⁶ Pokiaľ ide o cezhraničné zabezpečovanie dôkazov na základe právnej pomoci medzi Slovenskou republikou (resp. všetkými štátmi, ktoré sú zmluvnými stranami) a USA,

¹⁴ Čl. 25 ods. 4 Dohovoru o počítačovej kriminalite.

¹⁵ Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 5. 2. 2019, COM(2019) 70 final.

¹⁶ Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 5. 2. 2019, COM(2019) 70 final.

táto je možná i na základe Dohovoru o počítačovej kriminalite, ktorý USA ratifikovali dňa 29. septembra 2009, pričom platnosť nadobudol dňa 1. januára 2007.

2.1 Kategórie elektronických dôkazov

V kontexte prístupu k elektronickým dôkazom v rámci USA je v prvom rade potrebné vymedziť kategórie, do ktorých USA digitálne dôkazy v zásade rozdeľujú. V zmysle prvej kategórie sa rozlišuje:

- a) získavanie uložených údajov, ktoré vznikli v minulosti,
- b) zachytávanie údajov (dát) priamo počas ich prenosu.

Do ďalšej samostatnej kategórie sa rozdeľujú aj:

- a) obsah,
- b) neobsahové údaje – prevádzkové údaje,
- c) neobsahové údaje – užívateľské a prístupové údaje.¹⁷

Pokiaľ ide o procesný postup pri žiadostiach Slovenskej republiky o právnu pomoc zasielaných do USA, je potrebné konštatovať, že žiadosti je potrebné zasielať čo najskôr, a to predovšetkým v dostatočnom časovom predstihu pred uplynutím maximálnej lehoty uchovávanía údajov, nakoľko po tejto lehote dochádza k ich automatickému vymazaniu. Pre úplnosť však možno uviesť, že v rámci žiadosti o právnu pomoc je možné žiadať aj o predĺženie lehoty uchovávanía. Žiadosť sa vyhotovuje v štruktúrovanej elektronickej forme, pričom jej obsah a rozsah je potrebné prispôbiť druhu údajov, resp. dôkazov, o ktoré sa žiada, ako aj druhu služby, s ktorou sa údaje spájajú. Pokiaľ ide o vybavovanie žiadostí o zabezpečenie elektronických dôkazov v USA, je potrebné uviesť, že približne 60 % žiadaných údajov tvoria užívateľské údaje.¹⁸

Ako sme uviedli vyššie, USA rozdeľuje kategórie údajov (ktoré u nás možno zahrnúť pod údaje, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahuje ochrana osobných údajov v zmysle § 116 Trestného poriadku) podľa miery a závažnosti zásahu do základných práv jednotlivca na užívateľské údaje, prevádzkové údaje a obsahové údaje.

2.1.1 Údaje o predplatiteľoch

Údaje o predplatiteľoch alebo užívateľoch sú údaje, ktoré opisujú kto je danou osobou a poskytujú základné informácie o používaní služby v určitom období (napr. časy prihlásenia

17 U.S. INTERNET SERVICE PROVIDER ASSOCIATION. *Electronic Evidence Compliance – A Guide for Internet Service Providers*. In: *Berkeley Technology Law Journal*. Volume 18, Issue 4. University of California, Berkeley School of Law, 2003.

18 BOHÁČIK, B. *Zabezpečovanie elektronických dôkazov najmä vo vzťahu k USA*. Seminár Justičnej akadémie Slovenskej republiky, Krpáčovo, 19. 5. 2016.

k účtu, doba používania služby atď.). Užívateľskými údajmi a záznamami o prístupe (tzv. access logs) sú meno a priezvisko, telefónne číslo, e-mailová adresa, e-mail použitý pri registrácii, a zahŕňajú dátum, čas a IP adresu každého prihlásenia jednotlivu. V naznačenom kontexte je ďalej potrebné uviesť právny režim, ktorým sa užívateľské údaje a prístupové záznamy spravujú, a ktorý je zakotvený v Electronic Communications Privacy Act (ECPA), Title 18, United States Code, Section 2703(c)(2). Najnižším právnym štandardom sa spravujú dôkazy, ktoré sú relevantné a súvisiace s prebiehajúcim vyšetrovaním.

2.1.2 Prevádzkové údaje

Prevádzkové údaje sú údaje, ktoré napomáhajú identifikácii osoby, s ktorou užívateľ komunikoval či webových stránok, ktoré navštívil. Predmetné údaje môžu byť dôležité napríklad pri vyšetrovaní detskej pornografie, nakoľko z nich možno zistiť informácie o odosielateľovi a príjimateľovi vrátane ich IP adries, dátumy a časy komunikácií, dĺžku a veľkosť komunikácie (napr. pri e-mailovej adrese možno zistiť osoby, ktoré a ktorým boli správy poslané, dátum odoslania alebo prijatia správy a veľkosť správy). Pre úplnosť je dôležité uviesť, že prevádzkové údaje síce zahŕňajú hlavičku e-mailu, avšak predmet e-mailovej správy už nie. Vo vzťahu k prevádzkovým údajom sa uplatňuje stredný štandard prístupu a na vydanie príkazu v USA je potrebné preukázať špecifické skutočnosti, ktoré odôvodňujú, že dané údaje sú relevantné a podstatné pre vyšetrovanie. Prevádzkové údaje sú upravené v Electronic Communications Privacy Act (ECPA), Title 18, United States Code, Section 2703(d) ako tzv. „d order“. Ak sú údaje zabezpečované cez právnu pomoc, dotknutá osoba sa neinformuje, avšak je potrebné žiadať o dôvernú (nesprístupnenie) žiadosť spolu s uvedením dôvodov.¹⁹ V prípade, že sa žiadosť o právnu pomoc realizuje po vznesení obvinenia konkrétnej osobe, je potrebné zdôvodniť žiadosť o dôvernú inými konkrétnymi skutočnosťami. Ďalej je potrebné uviesť, že americkí prokurátori musia súdu poskytnúť opis skutkových okolností spolu so zdôvodnením, ako požadované údaje prispievajú k dosiahnutiu účelu trestného konania a posunu vo vyšetrovaní.

Pokiaľ ide o neobsahové údaje, pre úplnosť je potrebné uviesť, že tieto môžu americkí poskytovatelia služieb poskytnúť dožadujúcemu štátu priamo a na dobrovoľnej báze, čo výrazne uľahčuje a zrýchľuje cezhraničnú spoluprácu. Uvedený postup priameho poskytnutia však nemožno uplatniť vo vzťahu k obsahovým údajom, a preto je dané dôkazy potrebné žiadať na základe právnej pomoci.

2.1.3 Obsahové údaje

Najprísnejší právny režim v USA sa uplatňuje vo vzťahu k obsahovým údajom. Pod obsahovými údajmi možno rozumieť informácie zaslané e-mailom či SMS medzi odosielateľom a príjmateľom, ktoré zahŕňajú písomné správy, texty, fotky, obrázky, odkazy

¹⁹ Uvedené sa uplatní v prípade, ak je známy páchateľ. Ak sa skutok týka neznámeho páchateľa nie je potrebné žiadať o nesprístupnenie žiadosti.

či pripojené súbory. Obsah správ vrátane predmetu e-mailu sa obdobne uplatňuje aj pri sociálnych sieťach a zahŕňa napríklad aj žiadosti o priateľstvo. Získanie obsahových dát na základe žiadosti o právnu pomoc z USA trvá v priemere až 10 mesiacov.²⁰ Tento čas sa však môže aj predĺžiť, a to napríklad v prípade, ak je žiadosť nedostatočná a je potrebné ju doplniť.²¹ Na to, aby USA poskytli obsahové údaje na základe žiadosti o právnu pomoc, je potrebné preukázať:

- tzv. *probable cause*, a
- skutočnosti odôvodňujúce, že údaje v žiadosti sú aktuálne.²²

Pojem „*probable cause*“ je odvodený zo Štvrtého dodatku americkej ústavy (The Fourth Amendment od the U. S. Constitution) na ochranu pred neodôvodnenou prehliadkou a zaistením, pričom má za cieľ garantovanie práva občanov na súkromie a slobodu pred nedôvodnými zásahmi zo strany vlády.²³ Pod pojmom prehliadka (search) podľa Štvrtého dodatku je okrem iného potrebné rozumieť aj elektronické sledovanie (electronic surveillance), ktoré zahŕňa odpočúvanie, obrazovo-zvukové záznamy, sledovanie geolokalizácie (napr. prostredníctvom RFID alebo GPS alebo údajov o bunkových lokalitách), tzv. data mining, sledovanie sociálnych médií monitorovanie údajov a prenosu informácií na internete.²⁴

Na zabezpečenie informácií, ktoré tvoria obsah telekomunikačnej prevádzky, ako aj na vydanie príkazu na odpočúvanie americkými justičnými orgánmi, je potrebné preukázať, že je splnená podmienka „*probable cause*“. Americké súdy zvyčajne považujú požiadavku „*probable cause*“ za splnenú vtedy, ak existuje dôvodná skutočnosť domnievať sa, že by mohol byť spáchaný trestný čin (za účelom zadržania, resp. zatknutia osoby) alebo (za účelom vykonania prehliadky, pod ktorú, ako sme už uviedli, spadajú aj odpočúvanie alebo oznámenie elektronických údajov tvoriacich obsah telekomunikačnej prevádzky) ak je daný dôvodný predpoklad, že na mieste, kde sa má vykonať prehliadka, sa nachádzajú dôkazy o vyšetřovanom trestnom čine a vykonanie požadovaného úkonu dopomôže k odhaleniu trestného činu.²⁵ V prípade vydania príkazu na prehliadku je potrebné písomné

20 *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, Brussels, 5. 2. 2019, COM(2019) 70 final.

21 Hlavnými dôvodmi, pre ktoré dochádza k odmietaniu dožiadaní iných štátov o zabezpečenie elektronických dôkazov zo strany USA v súčasnosti je nepreukázanie podmienky „*probable cause*“ zo strany dožadujúceho štátu, ďalej zásada proporcionality (rule de minimis) a sloboda prejavu European Parliament: 4th Working Document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) –Relation with third country law. Dostupné na: <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-636.343&format=PDF&language=EN&secondRef=01>

22 Seminár Justičnej akadémie Slovenskej republiky s názvom „Počítačová kriminalita a elektronické dôkazy“ – ONLINE, 1. 10. 2020–2. 10. 2020, lektor: JUDr. Branislav Boháčik.

23 Bližšie pozri napr. KIM, J. Fourth Amendment. In: *Legal Information Institute*. Cornell Law School, 2017. [online] (cit. 1. 4. 2021). Dostupné na: https://www.law.cornell.edu/wex/fourth_amendment

24 JURKOWSKI, S. Electronic Surveillance. In: *Legal Information Institute*. Cornell Law School, 2017. [online] (cit. 1. 4. 2021). Dostupné na: https://www.law.cornell.edu/wex/electronic_surveillance

25 Bližšie pozri *Illinois v. Gates Case*, 462 U.S. 213 (1983).

čestné vyhlásenie (tzv. *affidavit*) alebo zaznamenaná svedecká výpoveď či výpoveď poškodeného, ktoré preukazujú existenciu dôvodného podozrenia.²⁶ Sudca teda môže vydať príkaz na odpočúvanie alebo oznámenie elektronického obsahu telekomunikačnej prevádzky, ak čestné vyhlásenie poskytuje dostatok dôveryhodných informácií na zistenie a ustálenie podmienky „probable cause“.²⁷ Existuje všeobecná domnienka, že policajti sú spoľahlivým zdrojom informácií, a preto čestné vyhlásenia obsahujú častokrát skutočnosti vyplývajúce z ich činnosti, ktoré sa stávajú relevantnými faktormi pri posudzovaní naplnenia podmienky „probable cause“.²⁸

V naznačenom kontexte teda možno vysloviť konštatovanie, že v zmysle ustálenej praxe Najvyššieho súdu USA je podmienka „probable cause“ splnená vtedy, ak zo zadovážených skutočností, ktoré má vláda k dispozícii, a ktoré príslušnému súdu predložila, plynú dostatočne dôveryhodné informácie a tieto samé o sebe oprávňujú u osoby s dostatočnou opatrnosťou nadobudnúť presvedčenie, že bol spáchaný alebo sa pácha trestný čin a požadovaný účet (e-mail, telefónne číslo) obsahuje dôkazy o spáchaní alebo páchaní trestného činu. Pri zasielaní žiadostí o právnu pomoc do USA je potrebné preukázať, že skutočnosti vyplývajúce z vyšetrovacieho spisu majú spojitosť s účtom, ktorý patrí pod správu americkej spoločnosti, a ktorého obsah sa žiada na základe právnej pomoci sprístupniť. V tejto súvislosti je teda potrebné preukázať spojenie medzi skutočnosťami a požadovaným úkonom, pričom relevantné skutočnosti musia byť popísané samostatne vo vzťahu ku každej e-mailovej adrese (napr. ak patrí do správy spoločnosti Google) alebo telefónnemu číslu či užívateľskému účtu (ak sa jedná o zabezpečenie údajov z mobilnej aplikácie, napr. Snapchat²⁹).³⁰

V súvislosti s vydávaním príkazov na oznámenie obsahu elektronickej komunikácie je ďalej potrebné uviesť, že v prípade, ak prokurátor predkladá návrh na vydanie príkazu na oznámenie údajov o telekomunikačnej prevádzke alebo na odpočúvanie a záznam telekomunikačnej prevádzky vnútroštátnemu súdu postupom podľa slovenského Trestného poriadku, príslušnému súdu na účely rozhodovania predloží aj celý obsah na vec sa vzťahujúceho vyšetrovacieho spisu. K žiadostiam o právnu pomoc sa však rovnopis vyšetrovacieho spisu neprikladá, a preto musí byť žiadosť odôvodnená aj s poukazom na zdroj informácií. Len samotná konštatácia o tom, že osoba často komunikuje e-mailom, na základe čoho možno predpokladať, že sa v ňom budú nachádzať aj dôkazy o spáchaní vyšetrovaného trestného činu, je abstraktná, všeobecná a nedostatočná.³¹ V žiadosti

26 *Whiteley v. Warden Case*, 401 U.S. 560, 564 (1971).

27 *Prosecutor's Manual for Arrest, Search and Seizure*, § 3-2(c) (2004).

28 Bližšie pozri napr. *Franks v. Delaware Case*, 438 U.S. 154, 171 (1978) alebo *United States v. Mick Case*, 263, 553, 566 (2001).

29 Vo vzťahu k mobilnej aplikácii Snapchat možno pre zaujímavosť uviesť, že za určitých okolností môžu mať príslušné subjekty USA k dispozícii aj obsah správ, a to v prípade, ak ešte neboli užívateľom otvorené. Po otvorení sa správa automaticky zmaže, pričom po 30-tich dňoch od odoslania sa automaticky vymaže aj neprečítaná správa.

30 Vyžaduje sa teda spojenie konkrétneho užívateľa s účtom a trestným činom, uvedenie dôkazov, ktorých zadováženie sa predpokladá požadovaným úkonom právnej pomoci atď.

31 BOHÁČIK, B. Zabezpečovanie elektronických dôkazov najmä vo vzťahu k USA. Seminár Justičnej akadémie Slovenskej republiky, Krpáčovo, 19. 5. 2016.

je z pohľadu aplikačnej praxe potrebné uviesť konkrétne skutkové okolnosti, modus operandi, výšku škody a ďalšie súvislosti. V prípade, že žiadosť o právnu pomoc nespĺňa náležitosti vyžadované v zmysle štandardu „probable cause“, americkí prokurátori žiadosť nepredložia príslušnému súdu.³² V naznačenom kontexte však možno pre úplnosť uviesť, že justičné orgány USA sú v niektorých prípadoch oprávnené žiadať najskôr poskytnutie prevádzkových údajov, a až v prípade, ak sa preukáže, že predmetné údaje boli pre vyšetrovaný trestný čin relevantné, môžu žiadať aj poskytnutie obsahu.³³

3 Európsky vyšetrovací príkaz na účely odpočúvania a záznamu telekomunikačnej prevádzky

Z hľadiska kontextu prijatia dôvodov Európskeho vyšetrovacieho príkazu (ďalej len „EVP“) je potrebné uviesť, že členské štáty na účely potláčania trestnej činnosti už dlhodobo prijímajú a zavádzajú osobitné mechanizmy cezhraničnej spolupráce. Je však potrebné zdôrazniť, že neexistuje jeden kódex procesného práva upravujúceho problematiku justičnej spolupráce v trestných veciach, nakoľko daná problematika je upravená predovšetkým v primárnom práve EÚ a v osobitných právnych aktoch prijatých orgánmi EÚ.³⁴ Predmetné právne normy je však potrebné transponovať do vnútroštátnych právnych poriadkov členských štátov EÚ, nakoľko tieto nedisponujú priamym účinkom. V kontexte uvedeného tak možno konštatovať, že justičná spolupráca má svoj fundamentálny základ v normách práva EÚ, avšak je závislá na vnútroštátnom práve konkrétneho členského štátu.³⁵ V súvislosti s naznačeným výkladom je na tomto mieste ďalej potrebné uviesť multilaterálny dohovor, ktorý vo svojich ustanoveniach po prvýkrát explicitne upravil aj problematiku cezhraničného odpočúvania. Predmetným dohovorom je Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, ktorý sa v hlave III. zaoberal aj možnosťou právnej pomoci medzi členskými štátmi pri vykonávaní odpočúvania telekomunikačnej prevádzky.³⁶

32 V aplikačnej praxi sa častokrát stáva, že žiadosť o právnu pomoc je pre vydanie požadovaného príkazu neúplná, a tak USA požiadajú dožadujúci štát o zaslanie doplňujúcich informácií (napr. ak v žiadosti uvádzame, že osoba, ktorej obsah komunikácie sa žiada sprístupniť, mala pracovať pre Mikuláša Černáka, USA môžu zaslať žiadosť o doplnenie informácií s cieľom ozrejmienia, kto je to Mikuláš Černák).

33 BOHÁČIK, B. Zabezpečovanie elektronických dôkazov najmä vo vzťahu k USA. Seminár Justičnej akadémie Slovenskej republiky, Krpáčovo, 19. 5. 2016.

34 IVOR, J. Európsky vyšetrovací príkaz na účely odpočúvania a záznamu telekomunikačnej prevádzky. In: Košické dni trestného práva – Perspektívy vývoja európskeho trestného práva, Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2018, str. 10.

35 IVOR, J., KLIMEK, L. a J. ZÁHORA. Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky. Žilina: Eurokódex, 2013, s. 505.

36 ZÁHORA, J. Európsky vyšetrovací príkaz na odpočúvanie telekomunikačnej prevádzky. In: Justičná revue, 2020, roč. 72, č. 8–9, s. 987–988.

3.1 Právny rámec týkajúci sa Európskeho vyšetrovacieho príkazu

Podľa čl. 82 ods. 1 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“) má byť justičná spolupráca v trestných veciach v rámci EÚ založená na zásade vzájomného uznávania justičných rozhodnutí. Uvedená zásada býva všeobecne označovaná ako základný kameň justičnej spolupráce v trestných veciach v EÚ. Nástroje justičnej spolupráce založené na zásade vzájomného uznávania justičných rozhodnutí však zvykli byť označované za nedostatočné, a to predovšetkým s poukazom na to, že sa vzťahovali len na určitý typ dôkazov, pričom vymedzovali rozsiahly výpočet dôvodov zamietnutia vykonania príkazu.³⁷ S poukazom na uvedené bola dňa 3. apríla 2014 prijatá Smernica Európskeho parlamentu a Rady 2014/41/EÚ o európskom vyšetrovacom príkaze v trestných veciach, ktorá zaviedla univerzálny nástroj získavania dôkazov v trestných veciach s horizontálnou pôsobnosťou, založený na zásade vzájomného uznávania súdnych rozhodnutí v zmysle čl. 82 ods. 1 ZFEÚ, a to európsky vyšetrovací príkaz. Transponovaním smernice 2014/41/EÚ došlo zároveň aj k novelizácii zákona č. 650/2005 Z. z. o vykonaní príkazu na zaistenie majetku alebo dôkazov v EÚ v tom smere, že z textu zákona boli vypustené ustanovenia ohľadom zaistenia dôkazov, v dôsledku čoho došlo k zjednoteniu zaistenia dôkazov medzi členskými štátmi EÚ prostredníctvom EVP.³⁸

Členské štáty EÚ boli povinné prijať potrebné vnútroštátne opatrenia za účelom dosiahnutia súladu so smernicou 2014/41/EÚ do 22. mája 2017, pričom predmetnú smernicu do svojich právnych poriadkov doposiaľ transponovali všetky členské štáty s výnimkou Írska a Dánska. Pokiaľ ide o implementáciu dotknutej smernice do právneho poriadku Slovenskej republiky, dňa 15. októbra 2017 nadobudol účinnosť zákon č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov (ďalej len „zákon o EVP“). Trestný poriadok sa na konanie pri vydávaní a vykonávaní EVP použije len vtedy, ak zákon o EVP neustanovuje inak, v dôsledku čoho možno konštatovať, že Trestný poriadok má na účely rozhodovania o EVP podporné použitie. Vo vzťahu k zákonu o EVP je potrebné uviesť, že tento v § 2 ods. 1 vylučuje použitie Európskeho dohovoru Rady Európy o vzájomnej pomoci v trestných veciach spolu s oboma dodatkovými protokolmi, Dohovoru, ktorým sa vykonáva Schengenská dohoda, ako aj Dohovoru o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ a protokolom k nemu.

V zmysle smernice 2014/41/EÚ v spojení so zákonom č. 236/2017 Z. z. možno EVP vo všeobecnosti charakterizovať ako rozhodnutie, ktoré bolo vydané alebo schválené justičným orgánom jedného členského štátu, o vykonaní vyšetrovacieho opatrenia v inom členskom štáte za účelom získania dôkazov v trestných veciach v súlade so smernicou 2014/41/EÚ.³⁹ Vykonávajúci orgán je povinný zabezpečiť vykonanie žiadosti inej krajiny EÚ

37 ZÁHORA, J. Európsky vyšetrovací príkaz. In: *Iustitia Omnibus – Pocta prof. JUDr. Pavlovi Balážovi, CSc.* Kraków: Spolok Slovákov v Poľsku, 2014, s. 347.

38 IVOR, J. Európsky vyšetrovací príkaz na účely odpočúvania a záznamu telekomunikačnej prevádzky. In: *Košické dni trestného práva – Perspektívy vývoja európskeho trestného práva*, Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2018, str. 10–11.

39 EUROPEAN JUSTICE. Získavanie dôkazov v trestnom konaní, 2019. [online] (cit. 05.04.2021). Dostupné na: https://ejustice.europa.eu/content_european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams-92-sk.do

rovnakým spôsobom a za tých istých podmienok, ako by vyšetrovacie opatrenie nariadil jeho vlastný vnútroštátny justičný orgán. EVP možno vydať aj na získanie dôkazov, ktoré už existujú a príslušné orgány vykonávacieho štátu tieto majú v držbe. Vo všeobecnosti možno konštatovať, že rozhodnutie, ktoré je vo vykonávajúcim štáte potrebné uznať, nahrádza pri zabezpečovaní dôkazov medzi jednotlivými členskými štátmi EÚ žiadosť o právnu pomoc. Taktiež je dôležité uviesť, že v zmysle smernice 2014/42/EÚ patrí právo požiadať o vydanie EVP aj podozrivému, obvinenému alebo obhajcovi obvineného v jeho mene, a to v súlade s ustanoveniami vnútroštátneho trestného práva. Cieľom zavedenia EVP bolo zjednodušenie a zrýchlenie cezhraničného zabezpečovania vyšetrovacích opatrení, pričom uvedené sa podarilo dosiahnuť predovšetkým zavedením formulárového konania, stanovením lehôt na rozhodnutie a dôrazom na priamu komunikáciu medzi členskými štátmi. EVP sa vydáva ako záväzný formulár preložený do úradného jazyku vykonávajúcего štátu, ktorý je podpísaný, pričom presnosť a správnosť jeho obsahu osvedčuje vydávajúcí orgán. Samotné formuláre sú prílohou smernice 2014/41/EÚ. V zmysle čl. 5 predmetnej smernice musia byť z obsahu EVP zrejme najmä:

- informácie o vydávajúcim (prípadne i overujúcom) orgáne,
- predmet, dôvody vydania EVP,
- identifikačné údaje o osobe, ktorej sa EVP týka,
- opis trestného činu,
- relevantné ustanovenia trestného práva vydávajúcего štátu,
- uvedenie vyšetrovacieho opatrenia, ktoré sa žiada vykonať,
- dôkazy, ktoré sa majú EVP získať.⁴⁰

Vydávajúcí orgán je pri vydaní EVP povinný skúmať požiadavku primeranosti, pričom jeho vydanie sa s poukazom na práva podozrivého alebo obvineného musí javiť ako nevyhnutné a primerané. Ďalšou podmienkou vydania EVP je, aby sa vyšetrovacie opatrenie v ňom uvedené mohlo nariadiť aj podľa právneho poriadku štátu vydania za rovnakých podmienok v obdobnom prípade. V kontexte vydávania EVP je potrebné uviesť podmienky, ktoré sa uplatňujú, in concreto:

- podmienku overovania obojstrannej trestnosti (v zmysle uvedeného režimu sa vyžaduje, aby bol skutok trestným činom tak podľa právneho poriadku štátu pôvodu, ako aj podľa právneho poriadku vykonávajúcего štátu), a
- vydanie EVP bez overovania obojstrannej trestnosti (ak sa EVP týka trestného činu, ktorý je zahrnutý v zozname 32 trestných činov uvedených v prílohe a za tento trestný čin možno v štáte pôvodu uložiť trest odňatia slobody s hornou hranicou trestnej sadzby najmenej 3 roky).

Pokiaľ ide o vnútroštátny orgán Slovenskej republiky oprávnený vydať EVP, je v prvom rade dôležité rozlíšiť, či sa EVP vydáva v prípravnom konaní alebo v konaní pred súdom. V prípravnom konaní je na vydanie EVP oprávnený spravidla prokurátor, pokiaľ § 20 ods. 3 zákona o EVP neustanovuje inak. Právomoc vydať EVP v konaní pred súdom má predseda senátu alebo sudca. V prípade, ak je Slovenská republika vykonávajúcim štátom,

⁴⁰ Ustanovenie § 6 zákona o EVP sa nad rámec smernice 2014/41/EÚ spresňuje, že obsahom EVP musí byť opis skutku, pre ktorý je vedené trestné konanie, spolu s uvedením času, miesta a spôsobu spáchania, skutkovú podstatu trestného činu s právnou kvalifikáciou, ako aj meno, priezvisko, odtlačok úradnej pečiatky a podpis zástupcu vydávajúcего orgánu.

na zabezpečenie vybavenia EVP je príslušná krajská prokuratúra, v ktorej obvode sa má vyšetrovací úkon v zmysle EVP vykonať.

V zmysle čl. 7 smernice 2014/41/EÚ sa EVP zasiela priamo, pričom vydávajúcí štát je povinný zistiť orgán príslušný na jeho vykonanie podľa Atlasu Európskej justičnej siete. Prijatie sa potvrdzuje na určenom „B“ formulári.

V čl. 11 smernice 2014/41/EÚ sú ustanovené dôvody neuznania alebo nevykonania EVP, ku ktorým možno zaradiť napr. existenciu imunity alebo výsady znemožňujúcej vykonať EVP, prípadne ak by bolo vykonanie EVP v rozpore so zásadou ne bis in idem, alebo ak skutok, ktorého sa EVP týka, nie je trestný podľa právneho poriadku vykonávajúceho štátu.⁴¹ K nepochybným pozitívam, ktoré zavedenie EVP prinieslo, je potrebné poukázať na stanovenie presnej lehoty jeho uznania, ktorá je v zmysle čl. 12 smernice 2014/41/EÚ určená na 30 dní od doručenia EVP;⁴² ako aj lehoty jeho vykonania, podľa ktorej je vykonávajúci orgán povinný realizovať vyšetrovacie opatrenie najneskôr do 90 dní od uznania EVP. Ustanovenie presných lehôt na uznanie a vykonanie EVP výrazne prispelo k urýchleniu cezhraničného vykonávania a zabezpečovania dôkazov.

3.2 Odpočúvanie s technickou pomocou iného členského štátu a bez technickej pomoci iného členského štátu, cezhraničné odpočúvanie

V kontexte EVP a odpočúvania je potrebné poukázať na V. kapitolu smernice 2014/41/EÚ, ktorá v čl. 30 a čl. 31 osobitne upravuje odpočúvanie telekomunikačnej prevádzky. V zmysle dotknutých článkov smernica 2014/41/EÚ rozlišuje:

- a) odpočúvanie s technickou pomocou iného členského štátu, a
- b) odpočúvanie bez technickej pomoci iného členského štátu.

Pokiaľ ide o odpočúvanie s technickou pomocou iného členského štátu EÚ podľa čl. 30 smernice 2014/41/EÚ, vyžaduje sa, aby EVP vydaný a zaslaný do členského štátu, ktorého technická pomoc s odpočúvaním sa vyžaduje, obsahoval okrem všeobecných náležitostí podľa čl. 5 dotknutej smernice tiež informácie za účelom zistenia totožnosti osoby, ktorá sa má odpočúvať, trvanie odpočúvania a technické údaje v dostatočnom rozsahu (najmä identifikátor cieľa). EVP musí taktiež obsahovať aj primerané zdôvodnenie, a to predovšetkým s cieľom preukázania, že odpočúvanie je na účely trestného konania relevantným vyšetrovacím opatrením. V aplikačnej praxi môže vzniknúť aj situácia, kedy môže technickú pomoc k odpočúvaniu poskytnúť viacero členských štátov. Vydávajúcí štát je v danom prípade povinný zaslať EVP tomu členskému štátu, na území ktorého sa

41 Z posledného demonštratívne uvedeného dôvodu odmietnutia vykonania EVP však existuje výnimka, a to v prípade, ak je trestný čin uvedený v zozname kategórií trestných činov v prílohe D, ak zaň možno vo vydávajúcom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou sadzby najmenej tri roky.

42 Pričom môže byť predĺžená o ďalších 30 dní.

odpočúvaná osoba nachádza, alebo možno predpokladať, že sa v ňom bude nachádzať.⁴³ Príslušný členský štát, ktorému bolo doručené EVP, je oprávnený odmietnuť jeho vykonanie v prípade, ak by sa odpočúvanie nepovolilo v obdobnom vnútroštátnom prípade. Pokiaľ ide o samotný výkon EVP, tento je v zmysle čl. 30 ods. 6 smernice 2014/41/EÚ možný vzájomnej dohody medzi vydávajúcim orgánom a vykonávajúcim orgánom buď:

- zaslaním telekomunikačnej prevádzky, a to bezodkladne, alebo
- vykonaním odpočúvania, záznamom a až následného zaslania výsledkov odpočúvania.

Pri vydávaní EVP alebo počas vykonávania odpočúvania môže vydávajúci štát požiadať štát výkonu EVP aj o prepis, dekódovanie alebo dešifrovanie záznamu za podmienky, že je riadne zdôvodnené⁴⁴ a vykonávajúci štát dal s uvedením postupom súhlas.

Odpočúvanie podľa smernice 2014/41/EÚ možno vykonať aj v prípade, že technická pomoc členského štátu, v ktorom sa nachádza odpočúvaná osoba, nie je potrebná, a to postupom podľa čl. 31 dotknutej smernice. Je potrebné uviesť, že v predmetnom prípade nie je potrebný EVP a postačuje vyplnenie formuláru v prílohe „C“. Pri odpočúvaní, ktoré je možné vykonať bez technickej pomoci iného členského štátu, je potrebné rozlíšiť tzv. odpočúvajúci členský štát a informovaný členský štát. Odpočúvajúcim členským štátom je štát, ktorý povolil odpočúvanie a informovaný členský štát je štát, na území ktorého sa používa komunikačná adresa dotknutej odpočúvanej osoby. Keďže pri danom type odpočúvania nie je technická pomoc informovaného štátu potrebná, odpočúvajúci štát má smernicou 2014/41/EÚ stanovenú len informačnú povinnosť vo vzťahu k informovanému členskému štátu o realizácii odpočúvania, a to buď:

- pred odpočúvaním (ak je už pri nariadení odpočúvania známe, že odpočúvaná osoba sa nachádza na území informovaného členského štátu, alebo sa tam bude nachádzať),
- bezodkladne počas odpočúvania alebo po jeho vykonaní (len čo sa dozvie, že odpočúvaná osoba sa nachádza alebo sa nachádzala na území informovaného štátu).⁴⁵

Príslušný orgán informujúceho štátu je oprávnený bezodkladne, najneskôr do 96 hodín po tom, ako ho odpočúvajúci štát informoval o odpočúvaní, rozhodnúť o nepovolení odpočúvania alebo o jeho ukončení, ako aj o zákaze alebo obmedzení použitia materiálu získaného z odpočúvania.⁴⁶

⁴³ Čl. 30 ods. 2 smernice 2014/41/EÚ.

⁴⁴ Bližšie KOVÁČOVÁ, A. Európsky vyšetrovací príkaz – Smernica Európskeho parlamentu a Rady 2014/41/EÚ. Aplikácia prax – odporúčané postupy. Eurojust – EJN. Seminár Justičnej akadémie Slovenskej republiky konaný online dňa 23. 11. 2020.

⁴⁵ Čl. 31 smernice 2014/41/EÚ.

⁴⁶ Vo vzťahu k cezhraničnému odpočúvaniu bez technickej pomoci iného členského štátu EÚ bola venovaná rozsiahla diskusia na stretnutí zástupcov Eurojustu dňa 19 až 20. septembra 2018, a to predovšetkým s poukazom na čl. 30 smernice 2014/41/EÚ, ktorá ukladá odpočúvajúcemu štátu povinnosť informovať členský štát, na území ktorého sa odpočúvanie vykonáva, alebo sa bude vykonávať. Účastníci stretnutia zástupcov Eurojustu intenzívne diskutovali najmä o tom, do akej miery môže notifikovaný orgán členského štátu skontrolovať, či by odpočúvanie nebolo povolené v podobnom domácom prípade tak, ako to vyžaduje

Pokiaľ ide o právnu úpravu odpočúvania a záznamu telekomunikačnej prevádzky podľa zákona o EVP, táto je obsiahnutá v § 33 až § 36 predmetného zákona, pričom ju možno rozdeliť na:

- odpočúvanie a záznam telekomunikačnej prevádzky s technickou pomocou iného členského štátu (§ 33),
- odpočúvanie a záznam telekomunikačnej prevádzky s technickou pomocou Slovenskej republiky (§ 34),
- cezhraničné odpočúvanie bez technickej pomoci iného členského štátu (§ 35),
- cezhraničné odpočúvanie bez technickej pomoci Slovenskej republiky (§ 36).

Nad rámec právnej úpravy uvedenej a popísanej v smernici 2014/41/EÚ je potrebné uviesť, že v prípade, ak je SR vykonávajúcim štátom a jej technická pomoc je potrebná, na výkon odpočúvania na základe EVP je potrebné naplnenie podmienok odpočúvania podľa § 115 Trestného poriadku. V predmetnom prípade je potrebné predložiť návrh na vydanie príkazu okresnému súdu v sídle krajského súdu, ktorý sa nachádza v obvode krajskej prokuratúry, ktorá je oprávnená zabezpečiť vybavenie EVP.⁴⁷ V naznačenom kontexte je ďalej potrebné uviesť, že na vybavenie EVP na účely odpočúvania na území SR s technickou pomocou je v zmysle § 34 ods. 2 zákona o EVP príslušná Krajská prokuratúra Bratislava. Ak sa v konkrétnom prípade po preskúmaní EVP zistí, že sú splnené podmienky na odpočúvanie a záznam telekomunikačnej prevádzky podľa § 115 ods. 1 Trestného poriadku príslušný prokurátor Krajskej prokuratúry Bratislava predloží návrh na vydanie príkazu na odpočúvanie a záznam telekomunikačnej prevádzky Okresnému súdu Bratislava I.

čl. 31 ods. 3 smernice 2014/41/EÚ. V tejto súvislosti je potrebné uviesť, že hoci väčšina účastníkov súhlasila s tým, že v uvedenom prípade by sa malo jednať len o formálnu procesnú kontrolu, časť účastníkov uviedla, že v niektorých členských štátoch EÚ sa preskúmava vecná správnosť, pri ktorej preskúmaní sa na účely posúdenia vyžadujú i ďalšie informácie. Uvedené často vedie k rozhodnutiam o ukončení odpočúvania, ak stále prebieha a /alebo k zákazu použitia informácií získaných odpočúvaním. Väčšina účastníkov však odmietla potrebu podrobného a vecného preskúmania a tvrdila, že uvedený postup nie je v súlade s ratio legis čl. 31 smernice 2014/41/EÚ. Účelom informačnej povinnosti nie je vydanie príkazu na uznanie vyšetrovacieho opatrenia (podľa prílohy A – EVP), ale iba odraz rešpektovania zvrchovanosti inej krajiny. Účastníci taktiež skonštatovali, že ak by sa v súvislosti s príslušným formulárom prílohy C vyžadovali rovnako alebo dokonca viac informácií ako v rámci formulára prílohy A, bolo by vzniknutú situáciu potrebné označiť za paradoxnú. Účastníci diskusie prijali záver, že ustanovenie by sa malo vykladať s poukazom na princípy slobody, bezpečnosti a spravodlivosti, ktoré sú založené na vzájomnej dôvere a rešpektovaní rôznych právnych systémov členských štátov EÚ. Na základe prezentovaných skutočností sa väčšina účastníkov vyjadrila spôsobom, že článok 31 ods. 3 smernice 2014/41/EÚ by sa nemal vykladať extenzívne. Účastníci predmetného stretnutia ďalej diskutovali aj o dôsledkoch nedostatku oznámenia odpočúvajúceho štátu alebo nedostatku súhlasu, pričom v danom smere vyjadrili obavy týkajúce sa prípustnosti dôkazov. Hoci niektorí účastníci diskusie v uvedenom kontexte vyhlásili, že získané dôkazy nemožno považovať za prípustné, ostatní účastníci skonštatovali, že v prípadoch, keď neoznámenie odpočúvajúceho členského štátu bolo spôsobené tým, že príslušné orgány nevedeli, kde sa odpočúvaná osoba nachádza, táto skutočnosť nemôže viesť k záveru o neprípustnosti dôkazov.; Bližšie pozri GUERRA, J. E. and Ch. JANSSENS. Legal and Practical Challenges in the Application of the European Investigation Order. Summary of the Eurojust Meeting of 19–20 September 2018. In: EUCRIM. [online]. (cit. 7. 4. 2021). Dostupné na: <https://eucrim.eu/articles/legal-and-practical-challenges-application-european-investigation-order/>

47 Pozri primerane § 7 ods. 4 zákona o EVP.

Zákon o EVP v súvislosti s odpočúvaním stanovuje v § 34 ods. 3 dôvod odmietnutia vykonania EVP navyše,⁴⁸ a to v prípade, ak by príkaz na odpočúvanie nebolo možné vydať v obdobnom vnútroštátnom prípade na účely trestného konania, ktoré by bolo vedené v SR. Na základe dohody medzi vykonávajúcim orgánom SR a vydávajúcim orgánom je následne možné EVP vykonať buď priamym prístupom k telekomunikačnej prevádzke v SR zo štátu pôvodu, alebo vykonaním odpočúvania a záznamu telekomunikačnej prevádzky v SR.⁴⁹

Pokiaľ ide o situáciu, kedy je v zmysle § 36 ods. 1 zákona o EVP uskutočňované odpočúvanie bez technickej pomoci SR, je nad rámec úpravy podľa smernice 2014/41/EÚ potrebné uviesť vnútroštátny justičný orgán príslušný na rozhodovanie. O udelení súhlasu s odpočúvaním, ktoré je, bolo alebo má byť realizované z iného členského štátu EÚ na území SR, s jeho pokračovaním, ako aj na súvisiace úkony, rozhoduje Okresný súd Bratislava I. po splnení podmienok podľa § 115 Trestného poriadku.

V naznačenom kontexte možno pre úplnosť uviesť, že EVP, ktoré bolo vydané na účely vykonania odpočúvania je spojené so zásahom do základných ľudských práv, a to najmä práva na súkromie. Z uvedeného dôvodu je preto v aplikačnej praxi nevyhnutné podrobné zdôvodnenie potreby zásahu spolu s uvedením očakávaného výsledku. Alternatívou môže byť priloženie zdôvodneného rozhodnutia súdu k EVP.⁵⁰

Pre úplnosť je potrebné uviesť, že spolupráca členských štátov EÚ na základe smernice 2014/41/EÚ by mala byť umožnená aj na účely zhromažďovania a poskytovania prevádzkových údajov a lokalizačných údajov spojených s telekomunikačnou prevádzkou. V dôsledku uvedeného by tak malo byť príslušným vnútroštátnym orgánom umožnené vydať EVP aj na účely získania menej rušivých údajov, ktoré sa týkali uskutočnenej telekomunikačnej prevádzky, pričom uvedený úkon je potrebné považovať za invazívne vyšetrovacie opatrenie.⁵¹

4 Evaluácia a návrhy *de lege ferenda*

S poukazom na skutočnosti uvedené v spracovanom príspevku možno konštatovať, že problematika digitálnych dôkazov je z hľadiska ich cezhraničného zaistovania, teda v prípade ich uloženia mimo teritoriálne územie Slovenskej republiky na zahraničných serveroch (najčastejšie pri využívaní služieb tzv. cloud computing ako GoogleDrive, OneDrive, prípadne služieb rozličných chatových aplikácií apod.), dlhodobo aktuálna. Pri zabezpečovaní elektronických dôkazov, resp. počítačových údajov je nevyhnutné aplikovať jestvujúce nástroje medzinárodnej spolupráce v trestných veciach, a to či už

⁴⁸ K dôvodom odmietnutia vykonania EVP podľa zákona o EVP pozri bližšie § 11 zákona o EVP.

⁴⁹ § 34 ods. 5 písm. a) a b) zákona o EVP.

⁵⁰ KOVÁČOVÁ, A. Európsky vyšetrovací príkaz – Smernica Európskeho parlamentu a Rady 2014/41/EÚ. Aplikačná prax – odporúčané postupy. Eurojust – EJNI. Seminár Justičnej akadémie Slovenskej republiky konaný online dňa 23. 11. 2020.

⁵¹ Bod 30 smernice 2014/41/EÚ.

v rámci EÚ alebo mimo územia EÚ, na základe právnej pomoci bez zmluvného základu na úrovni EÚ, a to EVP, alebo na základe existujúcej medzinárodnej zmluvy.

Mimoriadne pozitívne možno hodnotiť predovšetkým prebiehajúcu iniciatívu a rokovania medzi EÚ a USA⁵² v oblasti cezhraničného získavania elektronických príkazov na báze reciprocity od poskytovateľov elektronických služieb, ako aj rokovania v Rade Európy o druhom dodatkovom protokole k Dohovoru o počítačovej kriminalite.⁵³ Vzhľadom na skutočnosť, že v súčasnosti má prevažná väčšina poskytovateľov elektronických služieb, a to najmä chatových aplikácií či sociálnych sietí sídlo v USA, je viac než žiaduce snažiť sa o precizovanie a zefektívnenie získavania digitálnych dôkazov nachádzajúcich sa na teritoriálnom území USA, nakoľko z aplikačnej praxe orgánov činných v trestnom konaní je zrejmé, že súčasné zabezpečovanie a poskytovanie digitálnych dôkazov medzi Slovenskou republikou a USA je zdĺhavé a častokrát (predovšetkým z dôvodu dobrovoľnosti ich poskytnutia) neisté. V nadväznosti na uvedené je na tomto mieste možné uviesť myšlienku Any Birchall, podľa ktorej: „Zločinci sa nezastavia na hraniciach Európy. V súčasnosti využívajú na organizovanie svojich nezákonných činností rýchle a moderné technológie a následne zmažú stopy. Mnohé údaje potrebné na vypátranie týchto zločincov sa uchovávajú v USA alebo amerických spoločnostiach. Dohoda medzi EÚ a USA o urýchlčení prístupu našich orgánov presadzovania práva k elektronickým dôkazom je preto mimoriadne dôležitá. Vďaka nej bude Európa bezpečnejšia, ale zároveň sa musí zaručiť ochrana osobných údajov, súkromia a procesných práv našich občanov.“⁵⁴

Vo vzťahu k tzv. legislatívnemu balíku EÚ v oblasti získavania elektronických dôkazov, a to návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov a návrhu smernice, ktorou sa stanovujú pravidlá pre určovanie právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní možno hodnotiť mimoriadne kladne predovšetkým stanovenie lehôt na vykonanie predmetných príkazov, ako aj zavedenie inštitútu právneho zástupu, prostredníctvom ktorého sa budú z iného členského štátu dôkazy priamo poskytovať. Taktiež možno v naznačenej súvislosti konštatovať, že forma legislatívneho nástroja prostredníctvom nariadenia je priamo uplatniteľná bez nutnosti jeho implementácie do vnútroštátnych právnych poriadkov, vďaka čomu sa má zamedziť odlišným výkladom v členských štátoch EÚ, ako aj možným problémom pri transpozícii v prípade, ak by bola zvolenou formou smernica. Pre úplnosť je však potrebné uviesť, že potenciálne zmeny v právnom poriadku Slovenskej republiky možno

52 Európska únia – Rada Európskej únie. Rada dala Komisii mandát na rokovania o medzinárodných dohodách týkajúcich sa elektronických dôkazov v trestných veciach. Dostupné online na: <https://www.consilium.europa.eu/sk/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>

53 European Data Protection Board. Vyhlásenie 2/2021 o návrhu nových ustanovení druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite (ďalej len „Budapešťiansky dohovor“). Dostupné online na: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_sk

54 Európska únia – Rada Európskej únie. Rada dala Komisii mandát na rokovania o medzinárodných dohodách týkajúcich sa elektronických dôkazov v trestných veciach. Dostupné online na: <https://www.consilium.europa.eu/sk/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>

očakávať pri transpozícii smernice, ktorá upravuje zriadenie právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní. Na druhej strane je však potrebné uviesť, že určité nedostatky z hľadiska pripravovaných zmien v oblasti získavania elektronických dôkazov na úrovni EÚ možno nájsť napríklad v porušení Európskym súdom pre ľudské práva akcentovaným princípom rovnosti zbraní, keďže napriek tomu, že spomínané nariadenie o európskom príkaze na predloženie a uchovanie elektronických dôkazov dáva oprávnenie vyžiadať si elektronické dôkazy od poskytovateľa služieb orgánom činným v trestnom konaní, resp. súdu, neexistuje však ustanovenie, ktoré by umožňovalo prístup k digitálnym dôkazom aj obžalovanému či jeho obhajcovi. Rovnako sa možno zamyslieť nad prípadným doplnením podmienky vydania metadát vzťahujúcich sa k elektronickým dôkazom, ktoré častokrát predstavujú súbor informácií dôležitých pre vyšetrovaný trestný čin.

Po analýze skúmanej problematiky, s poukazom na súčasnú prax súdov a orgánov činných v trestnom konaní v oblasti zabezpečovania digitálnych stôp nachádzajúcich sa na území iného štátu, možno na tomto mieste vymedziť základné požiadavky, ktoré by mali byť príslušnými orgánmi zohľadnené vo vývoji cezhraničného zaistovania elektronických dôkazov. Prvou požiadavkou je potreba urýchlenia zasielania žiadostí o právnu pomoc, resp. príkazov na poskytnutie požadovaných údajov, keďže v súčasnosti je častokrát zdĺhavý už samotný proces zasielania žiadostí cez jednotlivé zložky a odbory vnútroštátnych orgánov, resp. cez orgány im nadriadené až k príslušnému orgánu cudzieho štátu. V dôsledku uvedeného nastavenia fungovania vnútroštátnych aparátov tak môže dôjsť k situácii, že hoci by príslušné orgány dožiadaného štátu vybavili žiadosť obratom, v dôsledku neprimeranej byrokracie zo strany štátnych orgánov alebo orgánov štátnej správy, ktoré nie sú v niektorých prípadoch oprávnené vypracúvať a zasielať žiadosti priamo, už cudzie justičné orgány takýmito údajmi nemusia disponovať. Z hľadiska návrhov *de lege ferenda* sa možno zamyslieť nad tým, či by nebolo za účelom zefektívnenia a zrýchlenia procesu, kedy je žiadosť o právnu pomoc, resp. príkaz na predloženie elektronických dôkazov výlučne vo sfére vnútroštátneho orgánu, vhodné prostredníctvom zmeny ustanovení interných predpisov toho-ktorého štátneho orgánu odstrániť potrebu ich zasielania cez nadriadené orgány⁵⁵ a zaviesť možnosť zaslať žiadosť o právnu pomoc príslušnému subjektu cudzieho štátu priamo orgánom „prvého kontaktu“, s prípadnou správovou povinnosťou nadriadenému orgánu za účelom garantovania kontroly nad dodržiavaním zákonov, ostatných právnych predpisov a medzinárodných zmlúv.

Obdobná situácia nastáva aj v prípade absencie zavedenia presných lehôt na vybavenie žiadostí o právnu pomoc, nakoľko nie ojedinele sa stáva, že proces poskytnutia digitálnych dôkazov z cudzieho štátu mimo EÚ (predovšetkým z USA) trvá v priemere 10 až 12 mesiacov.

Riešením, ktoré by mohlo okrem zjednodušenia procesu vypracovania žiadostí o právnu pomoc vzniknuté problémy odstrániť, je zavedenie priamej spolupráce vnútroštátneho orgánu (a to napr. či už súdu alebo prokurátora) s poskytovateľmi služieb cudzieho štátu,

⁵⁵ V súčasnosti je v určitých prípadoch prokurátor okresnej prokuratúry povinný podať prostredníctvom krajskej prokuratúry podnet generálnej prokuratúre na zaslanie žiadosti, pričom celý proces môže trvať až niekoľko dní.

ktorá by zabezpečila relatívne okamžitý prístup k elektronickým dôkazom, ako aj s tým súvisiace zavedenie striktných lehôt vybavovania žiadostí a poskytnutia požadovaných údajov, ktoré by bolo, vzhľadom na nestálu povahu digitálnych stôp, možné určiť napríklad na 14 dní odo dňa doručenia žiadosti alebo odo dňa doplnenia žiadosti.

Vývoj justičnej spolupráce v oblasti zabezpečovania elektronických dôkazov si bezpochyby vyžiada i príslušné zmeny zo strany zákonodarcu. Vzhľadom na absenciu presného stanovenia zákonnej maximálnej lehoty uchovávaní jednotlivých počítačových údajov (resp. aj údajov, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahuje ochrana osobných údajov, t. j. tie údaje, ktoré možno považovať za údaje podľa § 116 Trestného poriadku; lokalizačných údajov, prevádzkových údajov a obsahových údajov), je potrebné apelovať na slovenského zákonodarcu, a to aj s poukazom na tú skutočnosť, že v prípade pasívnej právnej pomoci Slovenská republika nedokáže dať cudzím justičným orgánom jednoznačnú odpoveď na otázku dĺžky uchovávaní jednotlivých údajov poskytovateľmi telekomunikačnej prevádzky. Uvedené je spôsobené predovšetkým tým, že po zrušení tzv. celoplošného monitoringu osôb v podmienkach Slovenskej republiky v súčasnosti nie sú určené jasné zákonné lehoty uchovávaní jednotlivých údajov najmä zo strany mobilných operátorov, ktorí sú oprávnení stanoviť vo svojich interných predpisoch rôzne lehoty ich uchovávaní na marketingové či účtovné účely na základe zmluvy uzatvorenej s fyzickou alebo právnickou osobou. Za úvahu by v tomto smere stálo legislatívne zjednotenie praxe poskytovateľov telekomunikačnej prevádzky v oblasti uchovávaní jednotlivých údajov (výpisu prijatých a odchádzajúcich hovorov, výpisu odoslaných a prijatých SMS správ, obsahu SMS správ apod.) stanovením rovnakej dĺžky ich uchovávaní, ako i možné vyňatie tejto pôsobnosti z možnosti jej internej úpravy, prípadne aspoň ustanovenie zákonnej povinnosti pre operátorov zverejniť dĺžku uchovávaní údajov na marketingové a účtovné účely na ich webových sídlach.

V súvislosti s návrhmi *de lege ferenda* možno ďalej uviesť, že budúcemu vývoju v problematike cezhraničného zabezpečovania digitálnych dôkazov, a to predovšetkým s poukazom na pripravovaný tzv. legislatívny balík EÚ v oblasti získavania elektronických dôkazov, ako aj s poukazom na prebiehajúce rokovania Európskej komisie s USA o medzinárodných dohodách týkajúcich sa elektronických dôkazov v trestných veciach môže dopomôcť i zákonná definícia pojmu *elektronický dôkaz*, v možnom znení:

„Elektronickým dôkazom sú informácie, údaje alebo dáta vytvorené, spracované, prenášané, uložené, pozmenené, skopírované alebo inak modifikované prostredníctvom počítačového systému, ktoré obsahujú skutočnosti dôležité pre trestné stíhanie, alebo nimi môžu byť takéto skutočnosti zistené, a ktoré môžu dopomôcť k objasneniu trestného činu a zisteniu jeho páchatela.“

Vzhľadom na špecifickosť uvedeného pojmu sa ako najvhodnejšie javí jeho systematické zaradenie do § 119 ods. 4 Trestného poriadku, pričom súčasný odsek 4 a odsek 5 by sa číslovali ako odsek 5 a odsek 6. V tomto smere je potrebné prisvedčiť argumentácii o nemožnosti subsumpcie definície elektronického dôkazu pod ustanovenia o vecnom

alebo listinnom dôkaze, nakoľko ňou nemožno postihnúť všetky osobitosti digitálnych dôkazov.⁵⁶

S cieľom efektívneho zaistenia digitálnych údajov nachádzajúcich sa na serverových farmách, spravidla na cloudovom úložisku mimo teritoriálneho územia Slovenskej republiky je potrebné snažiť sa o neustále legislatívne zjednodušenie režimov žiadostí o vzájomnú právnu pomoc týkajúcich sa uchovávaní a predkladania elektronických dôkazov, pričom dôraz je nevyhnutné kláď najmä na priamu spoluprácu medzi justičnými orgánmi a poskytovateľmi služieb v iných jurisdikciách. Rovnako tak je esenciálnou požiadavkou kladenou na inštitúty zaistovania elektronických dôkazov stanovenie jasných záruk a požiadaviek na určenie lehoty uchovávaní údajov, nakoľko súčasný slovenský právny poriadok je v uvedenej oblasti nejasný, čo môže v konečnom dôsledku spôsobovať i problémy pri cezhraničnom zaistovaní elektronických dôkazov.

Záver

Ako bolo uvedené v príspevku, v súčasnej dobe, ktorá sa vyznačuje pravidelným a uľahčeným cestovaním do krajín celého sveta, či v rámci Európskej únie i voľným pohybom osôb a tovaru, sa možno čoraz častejšie stretnúť s trestnou činnosťou, ktorá siaha až za hranice toho-ktorého štátu. Z pohľadu aplikačnej praxe nie je výnimkou presun páchatelov – občanov jedného štátu, do cudziny, a to nielen za účelom ich skrývania sa, ale aj na účel zorganizovania, prípravy či spáchania trestného činu. Je dôležité uviesť, že po zavedení a rozšírení Schengenského priestoru môžu osoby a tovar „prekračovať“ hranice ktoréhokoľvek zmluvného štátu bez hraničných kontrol. V dôsledku uvedených skutočností tak dochádza k páchaniu závažných druhov cezhraničnej trestnej činnosti, akou je napríklad drogová trestná činnosť, kedy páchatelia vyrábajú omamné a psychotropné látky na území jedného členského štátu, vyrobený tovar transportujú na územie iného členského štátu, kde ho následne predávajú. Taktiež sa možno stretnúť so situáciou, keď dôjde k spáchaniu napr. trestného činu úkladnej vraždy a páchatel v úmysle ukryť dôkazy a stopy trestného činu, ukryje telo poškodeného na odľahlom mieste v susednom štáte. Okrem demonštratívne uvedených druhov cezhraničnej trestnej činnosti sa možno stretnúť i s ďalšími závažnými kriminálnymi javmi, ktoré presahujú hranice jedného štátu, akými sú i obchodovanie s ľuďmi, vykorisťovanie detí či neoprávnené odoberanie orgánov.

V naznačenom kontexte možno ďalej uviesť, že v súčasnosti má stúpajúci trend páchanie počítačovej kriminality, kedy je počítač buď prostriedkom na spáchanie útoku, alebo cieľom útoku. V súvislosti s páchaním trestných činov proti životu a zdraviu nie je zriedkavé, že v mobilnom telefóne alebo počítači páchatela sa nájdu stopy, resp. dôkazy, ako napríklad komunikácia s inou osobou o pripravovanom, páchanom alebo dokonanom trestnom čine, komunikácia s poškodeným, fotografie z miesta činu či obrazovo-zvukové záznamy vyhotovené počas páchania trestného činu.

56 KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, s. 405.

Cezhraničné zaistovanie digitálnych dôkazov významne uľahčuje prácu orgánov činných v trestnom konaní predovšetkým v tom smere, že v prípade, ak je určitá komunikácia alebo záznam zo zariadenia odstránený, prípadne sa od začiatku nachádza iba na cloudovom úložisku, na základe nástrojov právnej pomoci môže byť napriek tomu na účely trestného konania zaistený a poskytnutý inému štátu než je štát, na území ktorého sa nachádza. Vzhľadom na to, že v súčasnosti dochádza čoraz častejšie k vzniku elektronických dôkazov, ktoré sú uložené v elektronickej podobe poskytovateľmi služieb so sídlom v rôznych štátoch, pričom sociálne médiá, chatové aplikácie, webmail alebo iné služby na prenos správ či uchovávanie digitálnych údajov sú relatívne častým nástrojom, prostriedkom alebo nositeľom určitého dôkazu, v podmienkach medzinárodnej a európskej justičnej spolupráce vyvstáva neustála potreba urýchľovania a zefektívnenia cezhraničného zaistovania elektronických dôkazov, ktorá má za cieľ predovšetkým uľahčiť vyšetrovanie a dokazovanie trestných činov, ktoré majú presah za teritoriálne územie príslušného štátu.

Okrem príslušných vnútroštátnych úprav jednotlivých krajín týkajúcich sa zabezpečovania informácií pre trestné konanie však majú štáty na účel uľahčenia cezhraničného získavania dôkazov a spolupráce v trestných veciach k dispozícii aj určité univerzálne nástroje. Predmetné nástroje justičnej spolupráce sú vymedzené niekoľkými dohovormi, smernicami či medzinárodnými zmluvami, ktoré príslušné štáty transponovali do svojich právnych poriadkov, resp. ku ktorým pristúpili. Pokiaľ ide o otázku zabezpečovania dôkazov medzi členskými štátmi EÚ, príspevok sa zamieraval predovšetkým na nástroj právnej pomoci, ktorým je európsky vyšetrovací príkaz. Predmetný nástroj zjednodušil postup justičných orgánov v prípade, ak žiadajú dôkazy nachádzajúce sa v inom členskom štáte EÚ. EVP spočíva na zásade vzájomného uznávania, a tak je každý členský štát EÚ povinný uznať a vykonať žiadosť dožadujúceho štátu rovnako, ako by konal v prípade rozhodnutia vydaného vlastnými vnútroštátnymi orgánmi.⁵⁷

Na záver možno v súvislosti s cezhraničným odpočúvaním vykonávaným na základe právnej pomoci uviesť, že počet žiadostí adresovaných na jednotlivé prokuratúry SR má od roku 2018 klesajúci trend.⁵⁸ Uvedené je potrebné pripísať predovšetkým zavedeniu EVP, nakoľko justičná spolupráca formou EVP zaznamenala od jeho zavedenia výrazný vzostup. Pokiaľ ide o pasívnu právnu pomoc, zo správy generálnej prokuratúry SR o činnosti prokuratúry za rok 2019 vyplýva, že odpočúvanie telekomunikačnej prevádzky bolo ako úkon právnej pomoci zaslané na Krajskú prokuratúru Bratislava 11 krát a Krajskú prokuratúrou Trenčín 1 krát. Odpočúvanie telekomunikačnej prevádzky na základe EVP bolo Krajskou prokuratúrou Bratislava v roku 2019 realizované 13 krát, pričom 1 krát bolo vykonané Krajskou prokuratúrou Nitra. V súvislosti s aktívnou právnou pomocou je potrebné uviesť, že za rok 2019 nebolo zo strany prokuratúr Slovenskej republiky požadované žiadne odpočúvanie na základe dožiadania o právnu pomoc do cudziny. Odlišná však bola situácia pri odpočúvaní na základe EVP, kedy o vykonanie odpočúvania

57 EURÓPSKE NOVINY. Európsky vyšetrovací príkaz zjednoduší a urýchli cezhraničné vyšetrovania trestných činov. [online]. (cit. 16. 3. 2021). Dostupné na: <https://europskenoviny.sk/2017/05/24/europsky-vysetrovaci-prikaz-zjednodusi-urychli-cezhranicne-vysetrovania-trestnych-cinov/>

58 Správa generálneho prokurátora Slovenskej republiky o činnosti prokuratúry v roku 2019 a poznatkoch prokuratúry o stave zákonnosti v Slovenskej republike.

telekomunikačnej prevádzky žiadala Krajská prokuratúra Trnava 6 krát a Krajská prokuratúra Nitra 1 krát.⁵⁹

Literatúra

1. BOHÁČIK, B. *Zabezpečovanie elektronických dôkazov najmä vo vzťahu k USA*. Seminár Justičnej akadémie Slovenskej republiky, Krpáčovo, 19. 5. 2016.
2. DATA RECOVERY SPECIALIST: What is volatile data? There are two types of data sources, persistent and volatile, but how does this effect an investigation? [online] Dostupné na: <http://www.datarecoveryspecialists.co.uk/blog/what-is-volatile-data>
3. European Justice. Získavanie dôkazov v trestnom konaní. [online] Dostupné na: https://e-justice.europa.eu/content_european_investigation_order_mutual_legal_assistance_and_joint_investigatiojn_teams-92-sk.do
4. EURÓPSKE NOVINY. Európsky vyšetrovací príkaz zjednoduší a urýchli cezhraničné vyšetrovania trestných činov. [online]. (cit. 16. 3. 2021). Dostupné na: <https://europskenoviny.sk/2017/05/24/europsky-vysetrovaci-prikaz-zjednodusi-urychliecezhranicne-vysetrovania-trestnych-cinov/>
5. European Parliament: 4th Working Document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Relation with third country law. [online]. Dostupné na: <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE636.343&format=PDF&language=EN&secondRef=01>
6. Európska únia – Rada Európskej únie. Rada dala Komisii mandát na rokovania o medzinárodných dohodách týkajúcich sa elektronických dôkazov v trestných veciach. Dostupné online na: <https://www.consilium.europa.eu/sk/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>
7. European Data Protection Board. Vyhlásenie 2/2021 o návrhu nových ustanovení druhého dodatkového protokolu k Dohovoru Rady Európy o počítačovej kriminalite (ďalej len „Budapešťiansky dohovor“). Dostupné online na: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_sk
8. GUERRA, J. E. and Ch. JANSSENS. *Legal and Practical Challenges in the Application of the European Investigation Order*. Summary of the Eurojust Meeting of 19–20 September 2018. In: EUCRIM. [online]. Dostupné na: <https://eucrim.eu/articles/legal-and-practical-challenges-application-european-investigation-order/>
9. IVOR, J. Európsky vyšetrovací príkaz na účely odpočúvania a záznamu telekomunikačnej prevádzky. In: *Košické dni trestného práva – Perspektívy vývoja európskeho trestného práva*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2018, str. 9–14. ISBN 978-80-8152-613-8.

⁵⁹ Bližšie pozri *Správa generálneho prokurátora Slovenskej republiky o činnosti prokuratúry v roku 2019 a poznatkoch prokuratúry o stave zákonnosti v Slovenskej republike*.

10. IVOR, J., L. KLIMEK a J. ZÁHORA. *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky*. Žilina: Eurokódex, 2013, 888 s. ISBN 978-80-8155-017-1.
11. JURKOWSKI, S. Electronic Surveillance. In: *Legal Information Institute*. Cornell Law School, 2017. [online]. Dostupné na: https://www.law.cornell.edu/wex/electronic_surveillance
12. KIM, J. Fourth Amendment. In: *Legal Information Institute*. Cornell Law School, 2017. [online] Dostupné na: https://www.law.cornell.edu/wex/fourth_amendment
13. KLIMEK, L., J. ZÁHORA a K. HOLCR. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, 2016, 448 s. ISBN 978-80-8168-538-5.
14. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, 524 s. ISBN 978-80-88168-18-8.
15. KOVÁČOVÁ, A. Európsky vyšetrovací príkaz – Smernica Európskeho parlamentu a Rady 2014/41/EÚ. Aplikačná prax – odporúčané postupy. Eurojust – EJNI. Seminár Justičnej akadémie Slovenskej republiky konaný online 23. 11. 2020.
16. POLČÁK, R. a kol. *Elektronické dôkazy v trestnom řízení*. Brno: Masarykova univerzita, Právnická fakulta, 2015. 253 s. ISBN 978-80-210-8073-7.
17. U.S. INTERNET SERVICE PROVIDER ASSOCIATION. Electronic Evidence Compliance – A Guide for Internet Service Providers. In: *Berkeley Technology Law Journal*. Volume 18, Issue 4. University of California, Berkeley School of Law, 2003, 945 s.
18. ZÁHORA, J. Európsky vyšetrovací príkaz na odpočúvanie telekomunikačnej prevádzky. In: *Justičná revue*, 2020, roč. 72, č. 8–9, s. 986–999. ISSN 1335-6461.
19. ZÁHORA, J. Európsky vyšetrovací príkaz. In: *Iustitia Omnibus – Pocta prof. JUDr. Pavlovi Balážovi*, CSc. Kraków: Spolok Slovákov v Poľsku, 2014, s. 343–355. ISSN 978-83-7490-728-8.
20. Illinois v. Gates Case, 462 U.S. 213 (1983).
21. Franks v. Delaware Case, 438 U.S. 154, 171 (1978).
22. United States v. Mick Case, 263, 553, 566 (2001).
23. Whiteley v. Warden Case, 401 U.S. 560, 564 (1971).
24. Zákon č. 236/2017 Z. z. o európskom vyšetrovacom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov.
25. Smernica Európskeho parlamentu a Rady 2014/41/EÚ o európskom vyšetrovacom príkaze v trestných veciach z 3. apríla 2014.
26. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17. 4. 2018 COM(2018) 225 final, 2018/0108(COD).
27. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Strasbourg, 17. 4. 2018 COM(2018) 226 final, 2018/0107(COD).
28. Prosecutor's Manual for Arrest, Search and Seizure, § 3-2(c) (2004).
29. Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), Brussels, 5. 2. 2019, COM(2019) 71 final.

30. Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 5. 2. 2019, COM(2019) 70 final.
31. Správa generálneho prokurátora Slovenskej republiky o činnosti prokuratúry v roku 2019 a poznatkoch prokuratúry o stave zákonnosti v Slovenskej republike.
32. Správa o činnosti Úradu špeciálnej prokuratúry a poznatky Úradu špeciálnej prokuratúry o stave zákonnosti za rok 2019.