Zaisťovanie digitálnych dôkazov v cezhraničných situáciách*

Gathering Digital Evidence in Cross-border Situations

Jozef Záhora**

Abstrakt

Skutočnosť, že internet je médium, ktoré nepozná hranice spôsobuje, že elektronické služby môžu byť poskytované z ktoréhokoľvek miesta na zemi bez toho, aby sa vyžadovala fyzická prítomnosť poskytovateľa v štáte, kde sa elektronické služby ponúkajú. Internet však môže byť tiež zneužitý ako prostriedok na páchanie alebo uľahčenie páchania trestného činu, vrátane závažnej kriminality ako napr. teroristických útokov. V tomto prípade kyberpriestor je často jediným miestom, kde vyšetrovatelia môžu zistiť a zaistiť stopy, na základe ktorých sa preukáže, kto trestný čin spáchal a získané dôkazy môžu byť použite pri súdnom konaní. Preto je potrebné vytvorenie účinných mechanizmov na získanie digitálnych dôkazov aj v cezhraničných situáciách. Súčasná situácia sa javí ako neuspokojivá a často prináša zastavenie trestného stíhania z dôvodu dôkaznej núdze. S cieľom uľahčiť a zrýchliť získanie elektronických dôkazov justičnými orgánmi, ktoré sú potrebné na vyšetrovanie trestného činu a následnú obžalobu, Komisia predstavila nové pravidlá, ktoré zabezpečia vytvorenie Európskeho príkazu na predloženie dôkazov, Európskeho príkazu na uchovanie elektronických dôkazov v trestných veciach a zavádza povinnosť poskytovateľov elektronických služieb určiť právneho zástupcu v Európskej únii.

Klíčová slova

E-dôkaz; elektronický dôkaz; elektronické služby; príkaz na predloženie dôkazov; príkazu na uchovanie elektronických dôkazov.

Abstract

The borderless of the Internet, causes that electronic services can be provided from anywhere in the world and it is not necessarily required a presence of this person in a State where the services are offered. However, the Internet can also be misused as tools to commit or facilitate crimes, including serious crimes such as terrorist attacks. When that happens, the cyberspace is often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in court. They can be often the only evidence law which can be collected by enforcement authorities. Therefore, effective mechanisms to obtain digital evidence are of the essence also in cross-border situations. However, present-day solutions too often prove unsatisfactory, bringing investigations to a halt because lack of evidence. To make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists, the Commission proposed new rules which will create a European Production Order, create a European Preservation Order and oblige electronic service providers to designate a legal representative in the Union.

* Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-15-0272/ This work was supported by the Slovak Research and Development Agency under the contract no. APVV-15-0272.

** Prof. JUDr. Jozef Záhora, PhD., Fakulta práva, Paneurópska vysoká škola, Bratislava, Slovensko / Faculty of Law, Paneuropean University, Bratislava, Slovak Republic / E-mail: jozef.zahora@paneurouni.com

Keywords

E-evidence; Electronic Evidence; Electronic Services; Production Order; Preservation Order.

Úvod

Koniec minulého a začiatok tohto storočia je charakteristický masovým rozvojom využívania počítačov. Počítače sa dnes používajú skoro vo všetkých oblastiach ľudského života, či už v oblastiach komunikácie, výroby, vzdelávania, zdravotníctva a v neposlednom rade aj v oblasti zábavy. Postupom času počítače stále viac nahradzujú a podporujú rôzne ľudské činnosti. Spolu zo zavádzaním počítačov sa vyskytuje aj „nový" fenomén, a to páchanie trestnej činnosti, ktorá súvisí s počítačmi. Tento fenomén býva označovaný ako „*počítačová kriminalita"*, „*kriminalita informačných technológií",* v anglickom jazyku sa môžeme stretnúť s označením „*Computer crime",* „*Cybercrime", „Computer-related crime",* „*Information Technology crime,"* a „*High-tech crime*".[1]

Počítačová kriminalita ako jedna z oblastí súčasnej kriminálnej činnosti, ktorej rozmach je zaznamenaný najmä v ostatných desaťročiach v súvislosti s nástupom digitálneho veku, je súborom protiprávnych konaní, ktorých hlavným znakom je využívanie informačných technológií, najmä počítačov, na páchanie trestnej činnosti. Jej rozmach je priamoúmerný postupujúcej informatizácii a „internetizácii" spoločnosti.[2] Keďže odhaľovanie, dokumentovanie počítačovej kriminality a zaisťovanie digitálnych stôp, vzhľadom na nadnárodný rozmer je zložité, počítačová trestná činnosť dokáže pri malom riziku prinášať vysoké zisky.[3]

Podľa prieskumu spoločnosti Norton,[4] v on-line prostredí sa odohráva čoraz viac našich každodenných aktivít a obchodných transakcií. To isté platí aj pre páchanie trestnej činnosti – každým dňom sa stáva obeťou počítačovej kriminality viac ako milión ľudí na celom svete. V uvedenom prieskume, ktorý bol vykonaný na vzorke 21 549 dospelých respondentov z 20 najväčších ekonomík[5] sa zistilo, že v uvedených krajinách bolo počítačovou kriminalitou postihnutých 978 miliónov ľudí. V dôsledku toho, obete počítačovej kriminality, celosvetovo utrpeli ujmu 172 miliárd USD – v priemere 142 USD

1 Bližšie ZÁHORA, J. Počítačová kriminalita v európskom kontexte. In: *Justičná revue: časopis pre právnu prax*, 2005, roč. 57, č. 2, s. 207 a nasl.

2 Porovnaj ZÁHORA, J. Aktuálne trendy v postihu počítačovej kriminality v Slovenskej republike. In: *Justičná revue: časopis pre právnu teóriu a prax*, 2016, roč. 68, č. 3, s. 324.

3 Porovnaj Návrh Smernice Európskeho parlamentu a Rady o útokoch na informačné systémy**,** ktorou sa zrušuje rámcové rozhodnutie Rady 2005/222/SVV {SEK(2010) 1122 final} {SEK(2010) 1123 final}.

4 2017 Norton Cyber Security Insights Report. *Norton By Symantec* [online]. Dostupné z: http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

5 Severná Amerika: USA a Kanada; Európa a Stredný východ: Francúzsko, Nemecko, Taliansko, Holandsko, Španielsko, Švédsko, Spojené arabské emiráty, Veľká Británia; Ázia a Pacifik: Austrália, Čína, Hongkong, India, Indonézia, Japonsko, Nový Zéland, Singapur; Latinská Amerika: Brazília a Japonsko.

na obeť – a každá obeť sa musela takmer 24 hodín (tri pracovné dni), venovať odstraňovaním následkov spáchaného trestného činu.

Ako už bolo uvedené, počítačová kriminalita je nadnárodný fenomén a preto sa riešeniu tejto problematiky venujú viaceré medzinárodné resp. nadnárodné organizácie. Z medzinárodných nástrojov možno spomenúť predovšetkým Dohovor o počítačovej kriminalite[6], ktorý možno považovať za najkomplexnejší nástroj na boj proti počítačovej kriminalite, obsahujúci jednak hmotnoprávne ustanovenia ale aj procesné ustanovenia a ustanovenia o medzinárodnej spolupráci.[7]

Hoci tento Dohovor možno považovať za výrazný pokrok v boji proti počítačovej kriminalite, ešte stále existuje množstvo prekážok, ktoré na európskej úrovni bránia účinnému vyšetrovaniu počítačovej kriminality a stíhaniu páchateľov. Patria medzi ne predovšetkým: hranice jurisdikcie, nedostatočná schopnosť výmeny spravodajských informácií, technické problémy pri pátraní po pôvode páchateľov počítačovej kriminality, odlišná úroveň odborných kapacít v oblasti vyšetrovania a forenznej vedy, nedostatok školeného personálu a nekonzistentná spolupráca s ostatnými zúčastnenými stranami zodpovednými za kybernetickú bezpečnosť'.[8]

Na získanie digitálnych dôkazov je nevyhnutná justičná spolupráca a vzájomná právna pomoc, no tento proces je v súčasnosti príliš pomalý a zdĺhavý. Takmer dve tretiny zločinov páchaných v súčasnosti, pri ktorých sa elektronické dôkazy nachádzajú v inej krajine, nie je možné riadne vyšetriť alebo trestne stíhať, najmä vzhľadom na čas potrebný na zhromaždenie týchto dôkazov alebo kvôli roztrieštenosti právneho rámca.[9]

1 Digitálny dôkaz

Pri odhaľovaní a vyšetrovaní počítačovej kriminality digitálne dôkazy predstavujú kľúčový nástroj na preukázanie spáchania trestného činu a zistenie páchateľa.[10] Vzhľadom na to, že spomínaný Dohovor o počítačovej kriminalite neuvádza definíciu elektronického dôkazu, pre potreby tohto článku sa pokúsime na základe dostupných zdrojov vymedziť pojem elektronický dôkaz.

---

6 Dohovor o počítačovej kriminalite. Oznámenie MZV SR č. 137/2008 Z. z.

7 Bližšie ZÁHORA, J. Počítačová kriminalita v európskom kontexte. In: *Justičná revue: časopis pre právnu prax*, 2005, roč. 57, č. 2, s. 207 a nasl.; IVOR, J., L. KLIMEK a J. ZÁHORA. *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky*. Žilina: Eurokódex, 2013, s. 316 a nasl.

8 Oznámenie Komisie Rade a Európskemu parlamentu. Riešenie otázok trestnej činnosti v digitálnom veku: zriadenie európskeho centra boja proti počítačovej kriminalite. V Bruseli 28. 3. 2012, COM(2012) 140 final, s. 3.

9 Pozri Európska komisia – Tlačová správa. Bezpečnostná únia: Komisia uľahčuje prístup k elektronickým dôkazom, Brusel 17. apríl 2018.

10 ABELOVSKÝ, T. Zaistenie elektronického dôkazu vo svetle rekodifikácie. In: *Revue pro právo a technologie*, 2015, č. 11, s. 30.

Americkí autori[11] digitálny dôkaz resp. elektronický dôkaz definujú ako údaje obsahujúce akékoľvek dôkazné informácie, uložené alebo prenášané v digitálnej forme, ktoré môže strana súdneho konania použiť na súde. Uvedení autori zdôrazňujú rozdiel medzi elektronicky uloženými informáciami (*Electronically Stored Information – ESI*) a elektronicky prezentovanými dôkazmi, čím rozumejú proces používania počítača a projektora resp. video monitora na zobrazenie obrázkov alebo videa na súde alebo hlavnom pojednávaní.

Podľa definície Európskej Komisie, elektronickými dôkazmi sa rozumejú rôzne druhy údajov v elektronickej forme, jednak samotné „**obsahové údaje**" napr. IP adresy, e-maily, fotografie, videá alebo používateľské mena, alebo „**prevádzkové údaje**"[12] ktoré sú dôležité pre trestné konanie. Tieto typy údajov sú často nenahraditeľné pri vyšetrovaní počítačových trestných činov s cieľom identifikovať osobu alebo získať informácie o jej aktivitách.[13]

Na základe uvedeného, za digitálny dôkaz budeme považovať všetky druhy údajov prenášaných do počítačového systému, z neho, alebo v jeho rámci, alebo uchovávaných v elektronickej forme na príslušnom médiu ako počítačové údaje. Počítačovými údajmi budeme rozumieť záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť.[14] Tieto počítačové údaje môžu mať jednak charakter obsahových alebo prevádzkových údajov.

2 Dohovor o počítačovej kriminalite

Ako už bolo uvedené, najkomplexnejším nástrojom pre kontrolu počítačovej kriminality je Dohovor o počítačovej kriminalite. Prijatiu uvedeného Dohovoru predchádzali dve odporúčania. Jedno z roku 1989, týkajúce sa predovšetkým hmotnoprávnych otázok[15] a druhé z roku 1995, týkajúce sa procesných otázok.[16] Krátko na to, v novembri 1996 bola zriadená expertná skupina, ktorej úlohou bolo zaoberať sa počítačovou kriminalitou

---

11 ALLEN, J. a A. HALLENE. Digital Evidence. In: *American Journal of Family Law*, 2018, roč. 32, č. 1, Spring, s. 21.

12 Údaje týkajúce sa komunikácie prostredníctvom počítačového systému vytvorené počítačovým systémom, ktorý tvoril súčasť komunikačného reťazca, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu a trvania komunikácie alebo typu služby [čl. 1 písm. d) Dohovoru o počítačovej kriminalite].

13 European Commission – Fact Sheet. Frequently Asked Questions: New EU rules to obtain electronic evidence Brussels, 17 April 2018.

14 Porovnaj čl. 1 písm. b) Dohovoru o počítačovej kriminalite.

15 Recommendation č. R. (89) 9 of the Committee of Ministers to member states concerning on computer-related crime (*Adopted by the Committee of Ministers on 13 September 1989, at the 428th meeting of the Ministers' Deputies*).

16 Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology (*Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies*).

a navrhnúť riešenie. Od apríla 1997 do decembra 2000 mala skupina viacero zasadnutí a pracovných stretnutí, výsledkom čoho bol návrh Dohovoru o počítačovej kriminalite.[17] Dohovor bol schválený 23. novembra 2001 členskými štátmi a otvorený na podpis. Okrem Ruskej federácie, dohovor podpísalo všetkých ostatných 46 štátov Rady Európy, z toho dva štáty (Írsko a Švédsko) ho zatiaľ neratifikovali. Hoci ide o dohovor Rady Európy, už pri jeho príprave sa uvažovalo, že by sa mal aplikovať medzinárodne aj mimo Európu, a preto v zmysle čl. 37 cit. Dohovoru môže Výbor ministrov Rady Európy po konzultácii a získaní jednomyseľného súhlasu zmluvných štátov dohovoru prizvať ktorýkoľvek nečlenský štát Rady, ktorý sa nezúčastnil na jeho vypracovaní, aby pristúpil k dohovoru. Rozhodnutie sa prijme väčšinou ustanovenou v článku 20 písm. d) Štatútu Rady Európy a jednomyseľným hlasovaním zástupcov zmluvných štátov oprávnených zasadať vo Výbore ministrov. Doposiaľ dohovor ratifikovalo 19 nečlenských štátov Rady Európy.[18]

Slovenská republika dohovor o počítačovej kriminalite podpísala 4. februára 2005 a ratifikovala 8. januára 2008 s účinnosťou od 1. 5. 2008.[19] Česká republika dohovor o počítačovej kriminalite podpísala 9. februára 2005 a ratifikovala 22. augusta 2013, s účinnosťou od 1. decembra 2013.[20]

Uvedený dohovor pozostáva okrem vymedzenia pojmov, hmotnoprávnych ustanovení aj z ustanovení procesného práva a ustanovení o medzinárodnej spolupráci.

2.1 Špecifické vyšetrovanie

Jedným z najväčších problémov pri odhaľovaní a vyšetrovaní počítačovej kriminality je nestálosť digitálnych dôkazov. Takýto dôkaz môže byť ľahko zničený a nemusí byť zachovaný tak aby sa mohol obnoviť. Ďalším problémom pri zaisťovaní digitálnych dôkazov a zabezpečovaní ich integrity je skutočnosť, že sa často vyžaduje spolupráca s expertami, nakoľko je to činnosť, ktorá vyžaduje špecifické odborné znalosti. Je preto potrebné zabezpečiť, aby sa vyšetrovacie oprávnenia mohli uplatňovať aj v digitálnom prostredí. Je to obzvlášť významné, pretože, digitálne dôkazy sa nemusia zaisťovať výlučne pri počítačových trestných činoch ale aj pri ďalších trestných činoch.[21]

Z uvedených dôvodov, cit. dohovor v čl. 14 stanovuje signatárom povinnosť prijať potrebné legislatívne a iné opatrenia na vymedzenie právomocí a postupov ustanovených v tomto oddiele na účely špecifického vyšetrovania alebo konania v trestných veciach,

17 Bližšie *Explanatory Report to the Convention on Cybercrime*, s. 4.

18 Zoznam štátov, ktoré podpísali a ratifikovali uvedený dohovor, je dostupný z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Lc4x7z67

19 Dohovor o počítačovej kriminalite, oznámenie MZV SR č. 137/2008 Z. z.

20 Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s. o sjednání Úmluvy o počítačové kriminalitě.

21 Bližšie CLOUGH, J. The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World. In: *Criminal Law Forum*, 2012, roč. 23, č. 4, s. 363. DOI 10.1007/s10609-012-9183-3

okrem iných oblastí aj „zhromažďovanie dôkazov o trestnom čine v **elektronickej forme**“. Dohovor o počítačovej kriminalite zaviedol nasledovné špecifické vyšetrovacie oprávnenia:

- urýchlené uchovanie uložených počítačových údajov,
- urýchlené uchovanie a čiastočné sprístupnenie prevádzkových údajov,
- príkaz na predloženie počítačových údajov,
- prehliadka a zaistenie uložených počítačových údajov,
- zhromažďovanie prevádzkových údajov v reálnom čase,
- zachytenie obsahových údajov.

Predmetné ustanovenia rozlišujú medzi uchovaním (angl. *preservation*) a zaistením (angl. *seizure*) elektronických dôkazov. Uchovanie je chápané ako dočasný inštitút, ktorý sa má použiť v prípade, že hrozí riziko straty alebo zničenia dôkazu. Je časovo obmedzené na to, aby príslušné orgány mohli vykonať príslušné kroky na ich získanie. Zaistenie by malo nasledovať až po uchovaní.[22]

Urýchlené **uchovanie** uložených počítačových údajov (čl. 16 Dohovoru o počítačovej kriminalite) a urýchlené uchovanie a čiastočné sprístupnenie prevádzkových údajov[23] (čl. 17 Dohovoru o počítačovej kriminalite) sa môže použiť vo vzťahu k uloženým údajom, ktoré už boli zhromaždené a uchovávajú ich držitelia údajov, ako sú poskytovatelia služieb. Nevzťahujú sa na zber údajov v reálnom čase a uchovávanie budúcich prevádzkových údajov alebo prístupu k obsahu v reálnom čase komunikácie.[24] Takýto postup je možný najmä vtedy, ak existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov. Držiteľ takýchto elektronických dôkazov je povinných ich uchovať a udržať v celistvosti na potrebný čas, najviac však 90 dní, aby príslušné orgány mohli urobiť kroky na ich sprístupnenie.

Príkaz na **predloženie** počítačových údajov – *Production order* (čl. 18 Dohovoru o počítačovej kriminalite) umožňuje príslušným orgánom nariadiť:

a) každej osobe v rámci ich jurisdikcie predloženie určených počítačových údajov, ktoré sú v držbe alebo pod kontrolou tejto osoby, uložených v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov, a

---

22 Pozri ZÁHORA, J. Európsky príkaz na zabezpečenie dôkazov v trestných veciach. In: *Harmonizácia procesných úprav v trestnom konaní v členských štátoch Európskej únie*. Zborník materiálov z medzinárodného vedeckého seminára konaného v rámci projektu VEGA č. 1/0011/08 v Trnave dňa 10. 6. 2009. Trnava: Typi Universitatis Trnaviensis, 2009, s. 74.

23 Prevádzkové údaje znamenajú počítačové údaje týkajúce sa komunikácie prostredníctvom počítačového systému vytvorené počítačovým systémom, ktorý tvoril súčasť komunikačného reťazca, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu a trvania komunikácie alebo typu služby, ktorá bola jej podkladom [čl. 1 písm. d) Dohovoru o počítačovej kriminalite].

24 Bližšie Explanatory Report to the Convention on Cybercrime, s. 24.

b) poskytovateľovi služieb, ktorý ponúka svoje služby na území tejto strany, predloženie informácií o predplatiteľovi týkajúcich sa takých služieb, ktoré sú v držbe alebo pod kontrolou poskytovateľa.

Príkaz na predloženie predstavuje flexibilný nástroj, ktorý môžu príslušné orgány aplikovať vo viacerých prípadoch, namiesto viac rušivých alebo viac zaťažujúcich vyšetrovacích opatrení. Podobne ako pri urýchlenom uložení počítačových údajov, aj príkaz na predloženie sa vzťahuje iba na uložené alebo existujúce údaje a nevzťahuje sa na budúce údaje, ktoré ešte neexistujú, ako napr. prevádzkové údaje alebo údaje o obsahu súvisiace s budúcou komunikáciou.

2.2 Medzinárodná spolupráca

V štvrtej kapitole Dohovoru o počítačovej kriminalite sú obsiahnuté ustanovenie o medzinárodnej spolupráci na účely vyšetrovania alebo konania o trestných činoch súvisiacich s počítačovými systémami a údajmi alebo na zhromažďovanie dôkazov o trestnom čine v elektronickej forme. Okrem všeobecných foriem medzinárodnej justičnej spolupráce v trestných veciach ako napr. extradícia či právna pomoc, Dohovor obsahuje aj osobitné ustanovenia týkajúcich sa zaisťovania a poskytovania elektronických dôkazov v cezhraničných situáciách. Takýmito opatreniami sú predovšetkým:

- urýchlené uchovanie uložených počítačových údajov,
- urýchlené sprístupnenie uchovaných prevádzkových údajov,
- vzájomná pomoc týkajúca sa prístupu k uloženým počítačovým údajom,
- cezhraničný prístup k uloženým počítačovým údajom so súhlasom alebo v prípadoch, keď sú verejne prístupné,
- vzájomná pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase,
- vzájomná pomoc týkajúca sa zachytenia obsahových údajov.

V zmysle čl. 29 Dohovoru o počítačovej kriminalite, každá strana môže požiadať inú stranu, aby nariadila alebo inak zabezpečila urýchlené uchovanie údajov uložených prostredníctvom počítačového systému umiestneného na území tej inej strany a vo vzťahu ku ktorému má dožadujúca strana záujem zaslať žiadosť o právnu pomoc týkajúcu sa prehliadky alebo podobného prístupu, zaistenia alebo podobného zabezpečenia alebo sprístupnenia údajov. Náležitosti žiadosti sú uvedené v ods. 2 cit. ustanovenia. Po doručení žiadosti inej strany prijme dožiadaná strana všetky vhodné opatrenia na urýchlené uchovanie určených údajov v súlade s jej vnútroštátnym právnym poriadkom. Na účely vybavenia žiadosti ako podmienka na zabezpečenie takého uchovania údajov sa nevyžaduje obojstranná trestnosť. Každé uchovanie vykonané na základe takejto žiadosti trvá najmenej počas 60 dní, aby dožadujúca strana mohla predložiť žiadosť o prehliadku alebo podobný prístup, zaistenie alebo podobné zabezpečenie, alebo sprístupnenie údajov. Ak dožiadaná strana počas vybavovania žiadosti o uchovanie prevádzkových údajov

týkajúcich sa určenej komunikácie zaslanej podľa článku 29 dohovoru zistí, že do prenosu tej komunikácie bol zapojený poskytovateľ služieb v inom štáte, dožiadaná strana urýchlene sprístupní dožadujúcej strane dostatočné množstvo prevádzkových údajov na určenie totožnosti tohto poskytovateľa služieb a trasy, po ktorej sa uskutočnila komunikácia.

Každá strana má v zmysle čl. 35 cit. dohovoru určiť kontaktné miesto dostupné 24 hodín denne 7 dní v týždni (**Sieť 24/7 – *24/7 Network***) na zabezpečenie poskytovania okamžitej pomoci na účel vyšetrovania alebo konania v prípade trestných činov súvisiacich s počítačovými systémami a údajmi, alebo na účel zhromažďovania dôkazov o trestnom čine v elektronickej forme. Taká pomoc zahŕňa uľahčenie, alebo ak to jej vnútroštátny právny poriadok a prax umožňujú, priame vykonanie týchto opatrení: poskytovanie technického poradenstva, uchovávanie údajov podľa článkov 29 a 30 a zhromažďovanie dôkazov, poskytnutie právnych informácií a lokalizovanie podozrivých osôb.

3 Európsky príkaz na predloženie a uchovanie elektronických dôkazov v trestných veciach

S rozvojom Európskej únie a rozširovaním voľného pohybu osôb, sú aktivity kriminálnych skupín často páchané na nadnárodnej úrovni. V týchto prípadoch pri odhaľovaní a vyšetrovaní takýchto trestných činov je nevyhnutná spolupráca medzi príslušnými orgánmi jednotlivých štátov.[25] Právny základ pre justičná spoluprácu v trestných veciach možno nájsť v čl. 82 Zmluvy o fungovaní Európskej únie[26] (ďalej len ZFEÚ) ktorá umožňuje aproximáciu zákonov a iných právnych predpisov členských štátov vo viacerých oblastiach. Zmienený čl. 82 ZFEÚ upravuje dva právne základy pre vydávanie legislatívnych aktov v oblasti trestného práva procesného. Prvý právny základ je upravený v druhom pododseku čl. 82 ods. 1, ktorý vytvára imperatív pre Európsky parlament a Radu v súlade s riadnym legislatívnym postupom prijať **opatrenia** zamerané na vytvorenie pravidiel a postupov na zabezpečovanie **uznávania všetkých foriem rozsudkov a iných justičných rozhodnutí** v celej Únii. Druhý právny základ je upravený v čl. 82 ods. 2 ZFEÚ, ktorý fakultatívne umožňuje Európskemu parlamentu a Rade v súlade s riadnym legislatívnym postupom prostredníctvom smerníc ustanoviť **minimálne pravidlá** s cieľom uľahčiť v potrebnom rozsahu **vzájomné uznávanie rozsudkov a iných súdnych rozhodnutí**, ako aj policajnú a justičnú spoluprácu v trestných veciach, ktoré majú cezhraničný rozmer.[27] Tieto minimálne pravidlá zohľadňujú rozdiely

25 Bližšie RIJKEN, C. Re-balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters. In: *Common Market Law Review*, 2010, roč. 47, č. 5, s. 1457.

26 Zmluva o fungovaní Európskej únie (Konsolidované znenie), Ú. v. EÚ C 202, 7. 6. 2016, s. 47–388.

27 Porovnaj ZMIJ, M. Vývoj a súčasný stav acquis trestného práva v právnom poriadku Európskej únie. In: LANTAJOVÁ, D. et al. *Aktuálne otázky medzinárodného trestného práva v kontexte európskych a vnútroštátnych noriem*. Trnava: Trnavská univerzita v Trnave, Právnická fakulta, 2012, s. 292.

medzi právnymi tradíciami a systémami členských štátov. Minimálne pravidlá sa týkajú aj vzájomnej **prípustnosti dôkazov** medzi členskými štátmi EÚ.

V rámci spolupráce pri vyšetrovaní trestných činov s cezhraničným prvkom medzi jednotlivými štátmi, justičné orgány narážali na problémy vyplývajúce z rozdielnej právnej úpravy trestného konania v týchto štátoch.[28] Krátko po podpise Lisabonskej zmluvy[29] Komisia oznámila[30] že rozdiely medzi justičnými systémami jednotlivých členských štátov nemôžu v rámci boja proti cezhraničnej trestnej činnosti brániť činnosti justície. Európska únia by mala vytvoriť komplexný systém získavania dôkazov v cezhraničných veciach. Tento systém musí zahŕňať zavedenie skutočného európskeho príkazu na získanie dôkazov, ktorý nahradí všetky existujúce právne nástroje. V citovanom oznámení Komisia vyjadrila potrebu preskúmať okrem iného aj európsky právny rámec týkajúci sa **dôkazu v elektronickej podobe**. Uvedená požiadavka bola potvrdená aj v Zelenej knihe,[31] kde sa konštatuje, že sa predpokladá vytvorenie komplexného systému získavania dôkazov v cezhraničných veciach. Do tohto nástroja by mohli byť zahrnuté aj pravidlá týkajúce sa **elektronických dôkazov**. Za účelom boja proti počítačovej kriminalite Komisia v januári 2013 vytvorila **Európske centrum boja proti počítačovej kriminalite** ako súčasť Europolu.[32]

Elektronické dôkazy sú dôležité pri vyšetrovaní celého spektra trestnej činnosti. Čoraz častejšie je potrebné, aby justičné orgány podali žiadosť v inej jurisdikcii, aby získali tieto údaje o elektronických dôkazoch od poskytovateľov služieb. Ľahšie a rýchlejšie získavanie týchto dôkazov, a to aj cez hranice je pre vyšetrovanie a stíhanie trestných činov vrátane terorizmu alebo počítačovej kriminality účinným spôsobom veľmi dôležité.[33]

Európska únia už disponuje viacerými nástrojmi na získavanie dôkazov v trestných veciach v rámci justičnej spolupráce napr. Príkaz na zaistenie majetku alebo dôkazov v Európskej únii[34] alebo Európsky vyšetrovací príkaz[35]. Európsky vyšetrovací príkaz síce

---

28 Bližšie ZÁHORA, J. Spoločné vyšetrovanie trestných činov v Európskej únii. In: *Karlovarská právní revue*, 2010, roč. 6, č. 4, s. 111.

29 Lisabonská zmluva, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva, podpísaná v Lisabone 13. decembra 2007, Ú. v. EÚ C 306, 17. 12. 2007, s. 1–229.

30 Oznámenie Komisie Európskemu parlamentu a Rade. Priestor slobody, bezpečnosti a spravodlivosti pre občanov. Brusel, 10. 6. 2009, KOM(2009) 262 v konečnom znení.

31 Zelená kniha o získavaní dôkazov v trestných veciach medzi členskými štátmi a o zabezpečení ich prípustnosti. Brusel, 11. 11. 2009, KOM(2009)624 v konečnom znení.

32 Bližšie KLIMEK, L. Európske centrum boja proti počítačovej kriminalite. In: *Justičná revue*, 2015, roč. 67, č. 8–9, s. 1032–1043.

33 Porovnaj Oznámenie Komisie Európskemu parlamentu, Európskej Rade a Rade. Šestnásta správa o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie, Brusel 10. 10. 2018 COM(2018) 690 final.

34 Rámcové rozhodnutie Rady 2003/577/SVV z 22 júla 2003 o vykonaní príkazu na zaistenie majetku alebo dôkazov v Európskej únii, Ú. v. EÚ L 196, 2. 8. 2003, s. 45–55.

35 Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach, Ú. v. EÚ L 130, 1. 5. 2014, s. 1–36.

zahŕňa aj prístup k elektronickým dôkazom, v smernici o Európskom vyšetrovacom príkaze sa však nenachádzajú žiadne osobitné opatrenia týkajúce sa tohto druhu dôkazov

Ministri spravodlivosti EÚ 9. júna 2016 rokovali o zlepšení trestnej justície v kybernetickom priestore. Prijali dva súbory záverov[36], v ktorých sa stanovujú praktické opatrenia na zlepšenie spolupráce, ako aj harmonogram ďalších krokov. V záveroch o zlepšení trestnej justície v kybernetickom priestore[37] sa stanovujú konkrétne opatrenia pre nadväzujúci budúci postup a kroky v troch hlavných oblastiach práce:

- zefektívnenie postupov vzájomnej právnej pomoci a prípadne vzájomného uznávania v súvislosti s kybernetickým priestorom, a to prostredníctvom štandardizovaných elektronických tlačív a nástrojov,
- zlepšenie spolupráce s poskytovateľmi služieb vytvorením spoločného rámca (napr. používaním zjednotených tlačív a nástrojov) medzi nimi na účely vyžadovania konkrétnych kategórií údajov a
- začatie procesu úvah o možných kolíznych kritériách právomoci presadzovania práva v kybernetickom priestore.

Rada vyzvala Komisiu, aby výsledky týkajúce sa týchto troch pracovných oblastí predložila do júna 2017. Na základe uvedených návrhov Komisia 17. apríla 2018 predstavila nové pravidlá, ktoré policajným a justičným orgánom umožnia získať jednoduchší a rýchlejší prístup k elektronickým dôkazom, ktoré potrebujú pri vyšetrovaní, stíhaní a usvedčovaní páchateľov trestných činov. Uvedené pravidlá sú obsiahnuté v dvoch dokumentoch:

1. Návrh Nariadenia Európskeho Parlamentu a Rady o **európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach**, 17. 4. 2018, COM/2018/225 final – 2018/0108 (COD) (ďalej len „*návrh nariadenia*“),
2. Návrh Smernice Európskeho Parlamentu a Rady, ktorou sa stanovujú harmonizované **pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní**, 17. 4. 2018, COM(2018) 226 final, 2018/0107/COD (ďalej len „*návrh smernice*“).

Cieľom navrhovaných nástrojov nie je nahradiť Európsky vyšetrovací príkaz na účely získania elektronických dôkazov, ale predstavujú doplňujúce nástroje pre príslušné justičné orgány. Vytvorenie nového nástroja zameraného na elektronické dôkazy predstavuje lepšiu alternatívu než zmena smernice o Európskom vyšetrovacom príkaze, pretože so získavaním elektronických dôkazov sú spojené osobitné výzvy, ktoré nemajú vplyv na ostatné vyšetrovacie opatrenia zahrnuté do rozsahu pôsobnosti smernice o Európskom vyšetrovacom príkaze.

---

36 Závery Rady o zlepšení trestnej justície v kybernetickom priestore a Závery Rady o Európskej justičnej sieti na boj proti počítačovej kriminalite.

37 Council conclusions on improving criminal justice in cyberspace. Council of the European Union, Council Conclusions, Luxembourg, 9. 6. 2016.

Pri príležitosti predstavenia návrhu k uvedeným návrhom, niektorí členovia Komisie poskytli vyhlásenie. Prvý podpredseda Komisie **Frans Timmermans** v tejto súvislosti uviedol: *„Elektronické dôkazy sú v trestnom konaní čoraz dôležitejšie. Nemôžeme dovoliť, aby zločinci a teroristi využívali moderné a elektronické komunikačné technológie na utajenie svojej trestnej činnosti a unikanie spravodlivosti. V Európe nesmú existovať žiadne skrýše pre zločincov a teroristov, online ani offline. Dnešnými návrhmi sa zavádzajú bezprecedentné nástroje umožňujúce príslušným orgánom nielen získavať elektronické dôkazy rýchlo, efektívne a cez hranice, ale aj poskytovať silné záruky v oblasti ochrany práv a slobôd všetkých dotknutých osôb."* **Věra Jourová**, komisárka EÚ pre spravodlivosť, spotrebiteľov a rodovú rovnosť, dodala: *„Kým orgány presadzovania práva ešte stále používajú zastarané metódy, zločinci pri svojej činnosti využívajú rýchle a ultramoderné technológie. Orgánom presadzovania práva preto musíme na boj so zločinom poskytnúť metódy hodné 21. storočia, lebo zločinci na páchanie trestných činov metódy 21. storočia už používajú."*[38]

Obsahom uvedených návrhov je predovšetkým:

a) Európsky príkaz na predloženie [elektronických] dôkazov – *European Production Order*,
b) Európsky príkaz na uchovanie [elektronických] dôkazov – *European Preservation Order*,
c) sankcie za porušovanie resp. neplnenie stanovených povinností adresátmi uvedených príkazov,
d) záruky a prostriedky nápravy,
e) povinnosť určiť právneho zástupcu v Európskej únii pre poskytovateľov služieb.

Ad a) Európsky príkaz na predloženie dôkazov (čl. 2 ods. 1, čl. 4 ods. 1, 2 návrhu nariadenia) je rozhodnutie vydávajúceho orgánu členského štátu, ktorým sa poskytovateľovi služieb, ktorý ponúka služby v Únii a je usadený alebo zastúpený v inom členskom štáte, nariaďuje predložiť elektronické dôkazy. Európsky príkaz na predloženie dôkazov musí byť nevyhnutný a primeraný na účely trestného konania *a môže* sa vydať iba vtedy, keď je vo vydávajúcom štáte dostupné podobné opatrenie týkajúce sa toho istého trestného činu v porovnateľnej vnútroštátnej situácii. Návrh nariadenia obsahuje dva druhy príkazov na predloženie dôkazov:

1. Európsky príkaz na predloženie dôkazov týkajúci sa **údajov o predplatiteľoch a údajov o prístupe** (čl. 4 ods. 1 návrhu nariadenia) – sa môže vydať v prípade **všetkých trestných činov**,
2. Európsky príkaz na predloženie dôkazov týkajúci sa **údajov o transakciách a obsahových údajov** (čl. 4 ods. 2 návrhu nariadenia) – sa môže vydať len k trestným činom, za ktoré možno vo vydávajúcom štáte uložiť trest odňatia slobody s hornou hranicou minimálne 3 roky, alebo k trestným činom, ak boli úplne alebo čiastočne spáchané prostredníctvom informačného systému.

---

38 Pozri Európska komisia – Tlačová správa. Bezpečnostná únia: Komisia uľahčuje prístup k elektronickým dôkazom, Brusel, 17. 4. 2018.

Ad b) Európsky príkaz na uchovanie dôkazov [čl. 2 ods. 2, čl. 4 ods. 3 návrhu nariadenia] je záväzné rozhodnutie vydávajúceho orgánu členského štátu, ktorým sa poskytovateľovi služieb, ktorý ponúka služby v Únii a je usadený alebo zastúpený v inom členskom štáte, nariaďuje uchovať elektronické dôkazy vzhľadom na následnú žiadosť o predloženie dôkazov. Môže byť vydaný v prípade, že je nevyhnutné a primerané zabrániť odstráneniu, vymazaniu alebo zmene údajov vzhľadom na následnú žiadosť o predloženie týchto údajov prostredníctvom vzájomnej právnej pomoci, európskeho vyšetrovacieho príkazu alebo európskeho príkazu na predloženie dôkazov. Európsky príkaz na uchovanie dôkazov sa môže vydať v prípade všetkých trestných činov.

Európsky príkaz na predloženie dôkazov a európsky príkaz na uchovanie dôkazov sa môžu vydávať len v súvislosti s trestnými konaniami, a to tak počas štádia pred súdnym konaním, ako aj počas neho. Príkazy sa môžu vydávať aj v konaniach týkajúcich sa trestných činov, za ktoré môže byť vo vydávajúcom štáte pričítaná zodpovednosť právnickej osobe alebo za ktoré môže byť právnická osoba vo vydávajúcom štáte potrestaná. Európsky príkaz na predloženie dôkazov a európsky príkaz na uchovanie dôkazov sa adresujú priamo právnemu zástupcovi, ktorého určí poskytovateľ služieb na účely zhromaždenia dôkazov v trestnom konaní. Európsky príkaz na predloženie alebo uchovanie dôkazov sa zašle adresátovi podľa článku 7 návrhu nariadenia prostredníctvom osvedčenia o európskom príkaze na predloženie dôkazov alebo osvedčenia o európskom príkaze na uchovanie dôkazov. V prípade potreby sa preloží do úradného jazyka Európskej únie, ktorý adresát akceptuje.

Po prijatí príkazu **na predloženie dôkazov** adresát zabezpečí zaslanie požadovaných údajov priamo vydávajúcemu orgánu alebo orgánom presadzovania práva, ktoré sú uvedené v príkaze, najneskôr do **10 dní** po prijatí príkazu, pokiaľ vydávajúci orgán neuvedie dôvody pre skoršie zverejnenie. V núdzových prípadoch adresát zašle požadované údaje bezodkladne, najneskôr **do 6 hodín** od prijatia príkazu.

Po prijatí príkazu **na uchovanie dôkazov** adresát bezodkladne uchová požadované údaje. Uchovávanie sa skončí **po 60 dňoch**, ak vydávajúci orgán nepotvrdí, že bol začatý postup následnej žiadosti o predloženie údajov.

Ad c) Návrh nariadenia v čl. 13 a nasl. zavádza **sankcie** za porušenie resp. neplnenie povinností uvedených v návrhu nariadenia zo strany adresátov príkazov. Členské štáty majú zabezpečiť, aby boli dostupné účinné, primerané a odrádzajúce finančné pokuty v situáciách, keď poskytovatelia služieb nesplnia svoje povinnosti podľa článkov 9, 10 alebo 11 návrhu nariadenia. Týmto nebudú dotknuté vnútroštátne právne predpisy týkajúce sa ukladania trestných sankcií v takýchto situáciách. V prípade, že adresát nesplní svoje povinnosti vyplývajúce z uznaného príkazu, ktorého vykonateľnosť bola potvrdená vykonávajúcim orgánom, uvedený orgán uloží peňažnú sankciu v súlade so svojím vnútroštátnym právom. Voči rozhodnutiu o uložení pokuty je k dispozícii účinný súdny prostriedok nápravy.

Ad d) V čl. 15 a nasl. návrhu nariadenia sa zavádza možnosť aby osoby dotknuté európskym príkazom na predloženie dôkazov mali k dispozícii **účinné prostriedky nápravy**. Tieto prostriedky nápravy sú jednak na strane adresáta príkazu ale na strane obvinených a podozrivých osôb. Ak sa **adresát príkazu** domnieva, že vykonanie európskeho príkazu na predloženie dôkazov by bolo v rozpore s uplatniteľným právom tretej krajiny, ktorým sa zakazuje zverejnenie dotknutých údajov z dôvodov, že je buď potrebné chrániť základné práva dotknutých jednotlivcov, alebo základné záujmy tretej krajiny týkajúce sa národnej bezpečnosti alebo obrany, informuje vydávajúci orgán o svojich dôvodoch na nevykonanie európskeho príkazu na predloženie dôkazov v súlade s postupom uvádzaným v článku 9 ods. 5 návrhu nariadenia.

Obvinené a **podozrivé osoby**, ktorých údaje sa získali prostredníctvom európskeho príkazu na predloženie dôkazov, majú právo na účinné prostriedky nápravy voči európskemu príkazu na predloženie dôkazov počas trestného konania, v súvislosti s ktorým bol príkaz vydaný, bez toho, aby boli dotknuté prostriedky nápravy podľa smernice (EÚ) 2016/680[39] a nariadenia (EÚ) 2016/679[40]. Ak osoba, ktorej údaje sa získali, **nie je podozrivou** alebo **obvinenou osobou** v trestnom konaní, v súvislosti s ktorým bol príkaz vydaný, táto osoba má právo na účinné prostriedky nápravy voči európskemu príkazu na predloženie dôkazov vo vydávajúcom štáte bez toho, aby boli dotknuté prostriedky nápravy v zmysle citovaných smerníc. Takéto právo na účinný prostriedok nápravy sa uplatní pred súdom vo vydávajúcom štáte v súlade s jeho vnútroštátnym právom a zahŕňa možnosť napadnúť **zákonnosť opatrenia** vrátane jeho **nevyhnutnosti** a **primeranosti**.

Ad e) V záujme zabezpečenia, aby sa na všetkých poskytovateľov služieb, ktorí ponúkajú služby v Európskej únii, vzťahovali rovnaké povinnosti, a to aj vtedy, ak sa ich ústredie nachádza v tretej krajine, sú títo poskytovatelia povinní **určiť právneho zástupcu** v Únii na prijímanie, dodržiavanie a vykonávanie rozhodnutí a príkazov vydaných príslušnými orgánmi členských štátov na účely zhromažďovania elektronických dôkazov v trestnom konaní. Členské štáty, v ktorých je usadený poskytovateľ služieb, ktorý ponúka služby v Európskej únii, by mali zabezpečiť, aby poskytovateľ služieb určil aspoň jedného právneho zástupcu v Európskej únii na prijímanie, dodržiavanie a vykonávanie rozhodnutí a príkazov vydaných príslušnými orgánmi v členských štátoch na účely zhromažďovania elektronických dôkazov v trestnom konaní. Právnym zástupcom

---

39 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, Ú. v. EÚ L 119, 4. 5. 2016, s. 89–131.

40 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Text s významom pre EHP), Ú. v. EÚ L 119, 4. 5. 2016, s. 1–88.

je právnická alebo fyzická osoba, ktorú písomne určil poskytovateľ služieb na uvedené účely. Právny zástupca musí mať pobyt alebo byť usadený v jednom z členských štátov, v ktorom je usadený alebo ponúka služby poskytovateľ služieb. Členské štáty zabezpečia, aby sa rozhodnutia a príkazy vydané ich príslušnými orgánmi na účely zhromažďovania dôkazov v trestnom konaní zasielali právnemu zástupcovi určenému na tento účel poskytovateľom služieb. Uvedený zástupca bude poverený prijímaním, dodržiavaním a vykonávaní daných rozhodnutí a príkazov, a to v mene dotknutého poskytovateľa služieb (čl. 3 návrhu smernice).

Záver

Zaujímavosťou je, že na Európsky príkaz na predloženie dôkazov a Európsky príkaz na uchovanie dôkazov Komisia zvolila formu právneho aktu – nariadenie. Ako už bolo uvedené, právnym základom na vydávanie legislatívnych aktov v tejto oblasti je článok 82 ods. 1 ZFEÚ. Tento právny základ sa uplatňuje na mechanizmy, ktoré sú predmetom tohto nariadenia. V citovanom článku sa stanovuje, že „*Európsky parlament a Rada môžu v súlade s riadnym legislatívnym postupom* ***prostredníctvom smerníc*** *ustanoviť minimálne pravidlá s cieľom uľahčiť v potrebnom rozsahu vzájomné uznávanie rozsudkov a iných justičných rozhodnutí*“. V návrhu nariadenia Komisia zdôrazňuje, že v článku 82 ods. 1 ZFEÚ sa zákonodarcom v Únii poskytuje možnosť prijímať nariadenia a smernice. Podľa názoru Komisie, keďže návrh nariadenia sa týka cezhraničných postupov, pri ktorých sa vyžadujú jednotné pravidlá, **nie je potrebné členským štátom nechávať voľný priestor na transponovanie týchto pravidiel**. Nariadenie je **priamo uplatniteľné**, zabezpečuje **jednoznačnosť** a **väčšiu právnu istotu** a **zamedzuje rôznym** výkladom v členských štátoch a iným problémom pri transpozícii, ktoré sa vyskytli pri rámcových rozhodnutiach o vzájomnom uznávaní rozsudkov a justičných rozhodnutí. Okrem toho sa nariadením umožňuje uloženie **tej istej povinnosti jednotným spôsobom** v rámci celej Európskej únie. Z týchto dôvodov sa za najvhodnejšiu formu pre tento akt o vzájomnom uznávaní Komisia považuje formu nariadenia.

Na druhej strane, pre povinnosť zriadiť právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní, ako právny nástroj bola zvolená **smernica**. Ako právny základ sa tu Komisia odvoláva na čl. 53 a 62 ZFEÚ, v ktorých sa stanovuje prijatie opatrení na koordináciu ustanovení zákonov, iných právnych predpisov alebo správnych opatrení v členských štátoch o zavedení služieb a ich poskytovaní. Komisia môže podľa citovaných článkov navrhnúť smernice a nezáväzné nástroje, ako sú napríklad odporúčania. Vzhľadom na potrebu poskytnúť právnu istotu a odstrániť prekážky v slobode poskytovať služby, čo sa nedá dosiahnuť prijatím nezáväzného nástroja, bola **zvolená forma smernice**.

V predstavených návrhoch možno vidieť veľký potenciál na zefektívnenie uchovávania a zaisťovania digitálnych dôkazov v jednotlivých štátoch Európskej únie.

Veľkým prínosom je tiež stanovenie lehôt na vykonanie príkazu na – do 10 dní a v núdzových prípadoch do 6 hodín. V porovnaní so 120 dňami pri existujúcom európskom vyšetrovacom príkaze alebo 10 mesiacmi pri postupe vzájomnej právnej pomoci to možno považovať za podstatné zrýchlenie. Perspektívnou myšlienkou je aj skutočnosť, že aj globálne podniky poskytujúce elektronické služby v Európskej únie budú musieť pre tento účel zriadiť „právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní". Vzhľadom na bezhraničnú povahu internetu môžu byť takéto služby v zásade poskytované odkiaľkoľvek vo svete a nemusia si nevyhnutne vyžadovať fyzickú infraštruktúru, prítomnosť podniku ani zamestnancov v členských štátoch EÚ, v ktorých sa služby ponúkajú, alebo na vnútornom trhu ako celku preto možno predpokladať, že uvedený príkaz, sa budú snažiť niektoré spoločnosti snažiť obchádzať.

Uvedené návrhy, boli v nedávnej dobe podrobené viacerým kritickým analýzam a hodnoteniam[41]. V porovnaní s existujúcimi nástrojmi justičnej spolupráce pre získanie dôkazov, navrhované nástroje prinášajú zásadný posun v oblasti získavania dôkazov. Zavedením mechanizmu priamej spolupráce medzi príslušnými orgánmi členských štátov a poskytovateľmi elektronických služieb v EU sa môže zabezpečiť rýchly a efektívny prístup justičných údajov k elektronickým dôkazom. Pre čitateľa možno zostane nezodpovedaná otázka implementácie Európskeho príkazu na predloženie a uchovanie elektronických dôkazov v trestných veciach. Táto skutočnosť je spôsobená tým, že zatiaľ ide len o návrh legislatívneho nástroja, ktorý ešte nebol definitívne schválený, a stále sa navrhujú ďalšie zmeny a doplnky, takže nie je zatiaľ známe v akej podobe bude schválený. Ako už bolo uvedené, Komisia ako legislatívny nástroj zvolila formu nariadenia – t. j. právneho nástoja, ktorý sa neimplementuje (netransponuje) do vnútroštátneho právneho poriadku, je priamo uplatniteľné, čím sa má zamedziť rôznym výkladom v členských štátoch a možným problémom pri transpozícii.

41 Napr. BÖSE, M. *An assessment of the Commission's proposals on electronic evidence* [online]. [cit. 26. 3. 2019]. Dostupné z: http://www.europarl.europa.eu/supporting-analyses; TOSZA, S. The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks. In: *Eucrim*, 2018, č. 4, s. 212–219.