https://doi.org/10.5817/RPT2019-1-2

CEZHRANIČNÝ PRÍSTUP K ELEKTRONICKÝM DÔKAZOM V TRESTNÝCH VECIACH. VISÍ VO VZDUCHU EURÓPSKY CLOUD ACT?

KATARÍNA KESSELOVÁ[1]

ABSTRAKT

Článok sa venuje regulácii cezhraničného prístupu k elektronickým dôkazom v trestných veciach. Popisuje, ako zákon CLOUD Act (i) vyriešil právnu otázku nastolenú v prípade Microsoft Ireland a znížil význam teritoriálneho umiestnenia dát v prospech kritéria držby a kontroly požadovaných údajov; (ii) vytvoril alternatívny mechanizmus pre orgány činné v trestnom konaní v EÚ na získanie dát z USA mimo pôsobnosť zmlúv o právnej pomoci. Príspevok ďalej rozoberá právne základy prenosu osobných údajov do tretích krajín podľa GDPR a vákuum, v ktorom sa poskytovatelia služieb budú pohybovať až do uzavretia vykonávacej dohody medzi Úniou a Spojenými štátmi. Záverom článok načrtáva, ako sa navrhovaným nariadením o cezhraničnom prístupe k elektronickým dôkazom vytvára nový rámec priamej spolupráce medzi orgánmi činnými v trestnom konaní a poskytovateľmi služieb elektronických komunikácií.

KĽÍČOVÁ SLOVA

elektronické dôkazy, cezhraničná spolupráca, CLOUD Act, GDPR, príkaz na predloženie a uchovanie, extrateritorialita

[1] JUDr. Mgr. Katarína Kesselová je absolventkou Právnickej fakulty Univerzity P. J. Šafárika v Košiciach a Prešovskej univerzity v Prešove. V súčasnosti pôsobí ako advokátska koncipientka v Košiciach. Kontaktný e-mail je katka.kessel@gmail.com

ABSTRACT

The article describes regulation on cross border access to e-evidence in criminal matters. It explains how CLOUD Act (i) resolved the legal issue posed in the Microsoft Ireland case and made the territorial location of data less relevant than possession and control of the data sought; (ii) created an alternative mechanism for law enforcement authorities in EU to obtain the U.S. held data outside the scope of MLATs. It further discusses legal grounds for transfers of personal data to third countries under GDPR and grey area in which providers will operate until an executive agreement between the EU and US is reached. Lastly, the article outlines how proposed regulation on transborder access to e-evidence aims to establish a new framework of direct cooperation between law enforcement and electronic communications providers.

KEYWORDS

electronic evidence, cross-border cooperation, CLOUD Act, GDPR, production and preservation order, extraterritoriality

1. ÚVOD

Elektronické dôkazy v trestnom konaní môžeme vo všeobecnosti rozdeliť z dvoch hľadísk. Po prvé rozlišujeme a) získavanie uložených údajov vzniknutých v minulosti a b) zachytávanie dát počas ich prenosu. Po druhé sa do samostatných kategórií vyčleňujú a) tzv. „neobsahové údaje“ a b) samotný obsah komunikácie.[2] Pod pojmom neobsahové údaje sa rozumejú základné údaje o používateľoch elektronickej služby, ako je e-mailová adresa registrovaného používateľa, informácie týkajúce sa on-line účtu používateľa, napr. IP adresa, z ktorej je k účtu pristupované alebo fakturačné záznamy zákazníka služby. Pod obsahové údaje patrí samotné znenie e-mailov a iných textových správ, fotografie, videá a ďalšie dáta, ktoré vytvoril používateľ služby. Odlišovanie uvedených kategórií sa premieta do samostatných procesných prostriedkov zabezpečovania informácií dôležitých pre

[2] 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. ISSN: 1086-3818.

trestné konanie. Možno skonštatovať, že získanie obsahových údajov je procesne náročnejšie než získanie neobsahových údajov.

V tomto príspevku sa zameriame na elektronické dôkazy nachádzajúce sa v dispozícii poskytovateľa elektronickej komunikačnej služby, ktorý sídli v inom štáte než orgán vyšetrujúci trestný čin. Popis získavania digitálnych stôp od všetkých typov poskytovateľov služieb informačnej spoločnosti[3] (ďalej len „ISP“) presahuje možnosti tohto príspevku. Preto rozsah zúžime na poskytovateľov webmailu, aplikácií na výmenu správ, prevádzkovateľov sociálnych sietí, teda tých služieb, u ktorých je ukladanie dát kľúčovým prvkom poskytovanej služby.

Pri vyšetrovaní a stíhaní trestných činov s cezhraničným charakterom môže orgán jedného štátu požiadať o právnu pomoc inú krajinu na základe medzinárodnej zmluvy o právnej pomoci (ďalej len „MLAT“[4]) alebo v prípade absencie takejto zmluvy na základe všeobecného princípu reciprocity[5] a v súlade s vlastným právnym poriadkom. Zmluvy o vzájomnej právnej pomoci napomáhajú získavaniu dôkazov fyzicky umiestnených v jednej krajine, ale relevantných pre vyšetrovanie trestného činu v inej krajine.

Vnútroštátne orgány členských krajín Európskej únie sa pri získaní elektronických dôkazov uložených v zahraničí, resp. v správe poskytovateľa služieb sídliaceho v inej krajine, spoliehajú na existujúce zmluvné nástroje justičnej spolupráce.[6] Dožiadania do inej členskej krajiny Únie môžu byť založené na európskom vyšetrovacom príkaze v trestných veciach[7] (ďalej len „EIO“)[8] a dožiadania do tretích krajín na základe medzinárodných zmlúv

---

[3] Viac k pojmu ISP a príkladom typov služieb informačnej spoločnosti pozri POLČÁK, Radim. Internet a proměny práva. Praha: AUDITORIUM, 2012. str. 140 – 144. ISBN 978-80-87284-22-3.

[4] Mutual legal assistance treaty.

[5] Princíp vzájomnosti je upravený v § 479 slovenského Trestného poriadku.

[6] Európska Komisia. *Factsheet - Security Union - Facilitating Access to electronic evidence* [online]. 17.04.2018. [cit. 13.4.2019]. Dostupné na: http://europa.eu/rapid/attachment/MEMO-18-3345/en/Factsheet%20E-evidence.pdf

[7] Smernica Európskeho parlamentu a Rady 2014/41/EÚ zo 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.

[8] European Investigation Order.

o právnej pomoci.[9] Avšak pokiaľ ide o elektronické dôkazy, ktoré možno premiestniť a vymazať kliknutím myši, jestvujúce mechanizmy právneho styku s cudzinou sa často javia ako príliš pomalé.[10] V súčasnosti vybavenie dožiadania EIO môže trvať 120 dní a dožiadanie podľa MLAT aj 10 mesiacov.[11]

Dôvodom, pre ktorý tradičné MLAT nie sú postačujúce, je aj to, že elektronické údaje, o ktoré môže mať záujem zahraničný orgán činný v trestnom konaní, sú čoraz častejšie uchovávané u poskytovateľov služieb cloud computingu a nie na zaradeniach a serveroch nachádzajúcich sa výhradne na území jednej krajiny. Poskytovatelia navyše z dôvodu optimalizácie ponúkaných cloudových služieb dáta uchovávajú aj v decentralizovanej podobe, teda po častiach na serveroch vo viacerých krajinách.[12] Musí byť v takom prípade žiadosť o súčinnosť adresovaná každému štátu, na ktorého území sa uchováva časť dát? V príspevku objasníme vznikajúci globálny konsenzus, podľa ktorého fyzické umiestnenie údajov nebude rozhodujúcim faktorom.[13] Namiesto geografického umiestenia sa kontrola nad dátami (faktická držba, možnosť ich správy) stala princípom, ktorý prevážil tak v americkom zákone *Clarifying Lawful Overseas Use of Data Act*, ako aj

---

[9] Európsky dohovor o vzájomnej pomoci v trestných veciach podpísaný dňa 20.04.1959 v Štrasburgu, pozri oznámenie Federálneho ministerstva zahraničných vecí publikované pod č. 550/1992 Zb. a Dohovor o počítačovej kriminalite podpísaný dňa 23.11.2001 v Budapešti, pozri oznámenie Ministerstva zahraničných vecí Slovenskej republiky publikované pod č. 137/2008 Z. z.

[10] Tamtiež 6.

[11] McCann FitzGerald. *Changes to Cross-Border Access to Electronic Evidence Mean it's Decision Time for Ireland* [online]. 20.06.2018. [cit. 23.4.2019]. Dostupné na: https://www.mccannfitzgerald.com/knowledge/disputes/changes-to-cross-border-access-to-electronic-evidence

[12] KRISHNAMURTHY, Vivek. Cloudy with a Conflict of Laws. In: *Berkman Center Research Publication No. 2016-3.* No. 2016-3. Harvard University - Berkman Klein Center for Internet & Society. [online]. 16.02.2016. [cit. 23.4.2019]. Dostupné na: https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y

[13] Hogan Lovells. *Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR* [online]. 15.01.2019. [cit. 13.4.2019]. Dostupné na: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf

v pripravovanom európskom *Nariadení o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach*.

Je potrebné uviesť, že sa paralelne vyvinul aj alternatívny spôsob získavania neobsahových údajov, a to dobrovoľná spolupráca medzi orgánmi činnými v trestnom konaní a poskytovateľmi digitálnych služieb, ktorí sídlia predovšetkým v Spojených štátoch amerických. Táto krajina dostáva najviac žiadostí o vzájomnú právnu pomoc týkajúcu sa prístupu k elektronickým dôkazom nielen od členských štátov Európskej únie, ale z celého sveta.[14] Súčasný právny poriadok Spojených štátov umožňuje poskytovateľom služieb sprístupňovať zahraničným orgánom presadzovania práva neobsahové údaje na dobrovoľnom základe podľa vlastných, interných pravidiel[15] vyhodnocovania žiadostí. Podľa Únie takejto spolupráci chýba spoľahlivosť, transparentnosť, zodpovednosť a právna istota.[16]

2. MICROSOFT IRELAND

Článok o prístupe orgánov činných v trestnom konaní k používateľským údajom, ktoré poskytovateľ služieb elektronickej komunikácie uchováva v tzv. cloude, a na serveroch lokalizovaných v zahraničí, začneme opisom súdneho prípadu *Microsoft Ireland*. Napriek tomu, že tento právny spor prebehol na americkej pôde a podľa tamojšieho práva, právna otázka v centre tohto prípadu (a jej legislatívne nie judikatórne rozuzlenie) má vplyv aj na európsky breh Atlantiku.

---

[14] Európska Komisia. Odporúčanie: Rozhodnutie rady o poverení začať rokovania so zreteľom na dohodu medzi Európskou úniou a Spojenými štátmi americkými o cezhraničnom prístupe k elektronickým dôkazom v oblasti justičnej spolupráce v trestných veciach [online]. 5. 2. 2019. [cit. 13.4.2019]. Dostupné na: http://ec.europa.eu/transparency/regdoc/rep/1/2019/SK/COM-2019-70-F1-SK-MAIN-PART-1.PDF

[15] Pozri napr. *Apple Legal Process Guidelines for Government and Law Enforcement outsidethe United States*. Dostupné na: https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf, *Legal process for user data requests FAQs* Dostupné na: https://support.google.com/transparencyreport/answer/7381738?hl=en

[16] Európska Komisia. *Factsheet - Security Union - Facilitating Access to electronic evidence* [online]. 17.04.2018. [cit. 13.4.2019]. Dostupné na: http://europa.eu/rapid/attachment/MEMO-18-3345/en/Factsheet%20E-evidence.pdf

Odvolanie predložené na rozhodnutie Najvyššiemu súdu Spojených štátov vo veci *United States* v. *Microsoft Corporation*[17] (ďalej skrátene len ako „*Microsoft Ireland*“) bolo vyústením nasledovnej genézy prípadu. Federálny vyšetrovací úrad žiadal spoločnosť Microsoft na základe súdom vydaného príkazu k prehliadke[18] o vydanie e-mailov a iných počítačových údajov spojených s používateľským kontom jej zákazníka. Akceptujúc, že federálni agenti preukázali dôvodné podozrenie, že dotknutý používateľ využíva konto na obchodovanie s drogami, spoločnosť predložila tú časť údajov, ktorú uchovávala v Spojených štátoch. Microsoft však odmietol vydať údaje uložené v írskom datacentre s argumentom, že *Stored Communications Act*[19] (ďalej len „zákon o uloženej komunikácii“ alebo „SCA“ upravujúci predmetný súdny príkaz) sa nevzťahuje na údaje, ktoré sú uchovávané v zahraničí. Spoločnosť žiadala súd o zrušenie tejto „cezhraničnej“ časti príkazu na vydanie údajov.

Prvostupňový súd návrh Microsoftu zamietol, pretože dospel k záveru, že aj údaje uchovávané mimo územia Spojených štátov podliehajú príkazu na vydanie v zmysle SCA. Odvolací súd sa s týmto záverom nestotožnil. Skonštatoval, že vydanie záznamov o elektronickej komunikácii by v tomto prípade vytváralo extrateritoriálne účinky SCA, preto vyhovel návrhu Microsoftu na zrušenie tejto časti príkazu. Ministerstvo spravodlivosti sa odvolalo na Najvyšší súd, ktorý prípad prijal na posúdenie.

Podľa názoru vlády rozhodnutie odvolacieho súdu vytvorilo stav, že vyšetrovací orgán sa musí so žiadosťou o vydanie dát obrátiť na zahraničné orgány, a to aj v prípade, ak žiada o údaje o americkom občanovi, prístupné americkému poskytovateľovi elektronických komunikačných služieb a na účely vyšetrenia trestného činu spáchaného v Amerike. Jediná spojitosť so zahraničím je skutočnosť, že údaje sú uložené mimo amerického územia, resp. v niektorých prípadoch ani nie je známe, kde sú údaje uchovávané, a teda ktorej krajine adresovať žiadosť o súčinnosť.

[17] United States v. Microsoft Corp. (Microsoft Ireland), No. 17-2, (Apr. 17, 2018) In the Matter of a Warrant to Search a Certain E‐Mail Account Controlled and Maintained by Microsoft Corporation

[18] Warrant under Section 2703 of the Stored Communications Act (18 U.S. Code § 2703.

[19] Stored Communications Act, Pub. L. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986).

Spoločnosť Microsoft argumentovala, že príkazy na vydanie údajov majú teritoriálne obmedzenie. Varovala, že inak by každá krajina mohla vyžadovať prístup k dátam len preto, že do jej územnej pôsobnosti spadá poskytovateľ služieb elektronickej komunikácie alebo jeho pobočka, bez ohľadu na lokalizáciu samotných dát. Podľa spoločnosti je zmena vymedzenia pôsobnosti príkazov na vydanie záznamov o elektronickej komunikácii v kompetencii Kongresu nie súdu. K zmene právnej úpravy skutočne došlo, a to ešte predtým, než Najvyšší súd prípad *Microsoft Ireland* meritórne rozhodol.

Prijatím zákona *Clarifying Lawful Overseas Use of Data Act* (ďalej len „zákon o objasnení zákonného využívania údajov v zámorí" alebo „CLOUD Act")[20] sa novelizoval *zákon o uloženej komunikácii* (SCA) a upravil dve hlavné skutočnosti:

(1) pôsobnosť príkazu na vydanie údajov o elektronickej komunikácii (t.j. otázka nastolená v prípade *Microsoft Ireland*) a

(2) prístup zahraničných orgánov k obsahu elektronickej komunikácie uchovávanej na území Spojených štátov.

Obe strany sporu *Microsoft Ireland* súhlasili so zastavením konania pred Najvyšším súdom bez vydania rozhodnutia, ktoré by sa z dôvodu vyriešenia právnej otázky prijatím CLOUD Act ihneď stalo obsoletným.

3. CLOUD ACT

Ako prezrádza akronym právneho predpisu, jeho zámerom je objasniť, že orgány presadzovania práva môžu od poskytovateľov služieb vyžadovať aj predkladanie dát nachádzajúcich sa v zahraničí. Zákon CLOUD Act upresňuje, že poskytovatelia služieb „elektronickej komunikácie alebo vzdialenej počítačovej služby" sú povinní uchovať, vyhotoviť kópie alebo vydať obsah komunikácie a akýkoľvek záznam alebo iné informácie týkajúce sa zákazníka alebo účastníka, ktoré sú v ich držbe alebo pod ich kontrolou bez

[20] Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018).

ohľadu na to, či sa tieto informácie, záznamy alebo iné informácie nachádzajú na území alebo mimo územia Spojených štátov.[21]

CLOUD Act rozšíril geografickú pôsobnosť zákona SCA. Bez zmeny ponechal definíciu povinných z príkazu (poskytovateľov elektronickej komunikácie alebo vzdialenej počítačovej služby, kam radíme napr. poskytovateľov e-mailu, četovacích služieb, cloudového hostingu), ako aj typ údajov, ktoré spadajú pod vecnú pôsobnosť zákona SCA. Je ním obsah elektronickej komunikácie a dáta uložené v cloude, ako aj neobsahové údaje, týkajúce sa elektronickej komunikácie (údaje o používateľskom konte, záznamy o prenose).[22]

Americké orgány činné v trestnom konaní môžu od poskytovateľov sídliacich v Spojených štátoch požadovať aj „zámorské" dáta o používateľoch týchto služieb, ktoré sú „v držbe alebo pod kontrolou" danej technologickej spoločnosti. Orgány presadzovania práva nie sú oprávnené extrahovať údaje priamo zo systémov poskytovateľov služieb.[23] Procesné záruky proti „nadužívaniu" alebo zneužívaniu žiadostí na vydanie dát ostávajú v platnosti v zmysle zákona SCA, pričom vyššie nároky sú kladené na získanie obsahových dát. Vyšetrovací orgán môže požadovať, aby poskytovateľ elektronických komunikačných služieb zverejnil obsah komunikácie uchovanej v elektronickom systéme po dobu 180 dní alebo menej, len na základe príkazu k prehliadke (*search warrant*) vydaného súdom podľa Federálneho trestného poriadku.[24] Súd vydá príkaz k prehliadke, ak na základe všetkých okolností existuje „primeraná pravdepodobnosť," že v pred-

[21] 18 U.S. Code § 2713: A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

[22] LOEB, Robert, GOLDMAN, Brian a TABATABAI Emily. *The CLOUD Act, Explained* [online]. 06.04.2018 [cit. 14.4.2019]. Dostupné na: https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained

[23] Hogan Lovells. *Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR* [online]. 15.01.2019. [cit. 13.4.2019]. Dostupné na: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf

metnom elektronickom úložisku možno nájsť dôkazy o trestnom čine.[25] Pri obsahových údajov sa vyžaduje najvyššie miera dôvodného podozrenia na spáchanie trestného činu. Príkaz k prehliadke musí špecifikovať miesta, ktoré majú byť prehľadané, ako aj cieľ hľadania.[26] Neobsahové údaje a e-maily, ktoré boli uložené dlhšie ako 180 dní, môže vyšetrovací orgán získať prostredníctvom predvolania (*subpoena*) alebo súdneho príkazu vydaného na základe SCA,[27] pričom pri oboch sa vyžaduje nižšia miera dôvodného podozrenia. Postačuje, ak elektronické dôkazy sú „relevantné pre prebiehajúce vyšetrovanie trestného činu."[28]

Potom čo poskytovateľ služby obdrží príkaz na vydanie dát, má možnosť príkaz napadnúť (navrhnúť zmenu alebo zrušenie príkazu), ak sa odôvodnene domnieva, že 1) dotknutá osoba (zákazník alebo používateľ služby) nie je americkým občanom a nemá bydlisko v Spojených štátoch alebo 2) požadované vydanie dát by spôsobilo značné riziko, že poskytovateľ služby „poruší zákony kvalifikovanej zahraničnej vlády."[29] Termín *kvalifi-*

---

[24] 18 U.S. Code § 2703 (a) A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

[25] Tamtiež 22.

[26] POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7. s. 156.

[27] 18 U.S. Code § 2703 (b).

[28] Tamtiež 22.

[29] A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes: (i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

kovaná zahraničná vláda znamená krajinu, ktorá má so Spojenými štátmi uzavretú bilaterálnu vykonávaciu dohodu o vzájomnom poskytovaní dát. Pod vykonávacou, resp. exekutívnou dohodou máme na mysli dohodu, na uzavretie ktorej sa vyžaduje iba podpis zástupcov americkej vlády (*attorney general* a *secreteary of state*[30]), bez potreby štandardného ratifikačného procesu. (Vykonávacia dohoda nadobudne účinnosť, ak Kongres po dobu 6 mesiacov neuplatní právo veta.[31]) V tomto prípade ide teda o odlišný postup než pri zmluvách o medzinárodnej právnej pomoci (MLAT), ktoré sú dnes využívané v oblasti právneho styku s cudzinou.

Novela *zákona o uloženej komunikácii* (SCA) sformalizovala dôvody, na základe ktorých môže poskytovateľ navrhnúť zrušenie príkazu súdom. Poskytovateľ služby je oprávnený príkaz napadnúť, ak sa domnieva, že jeho realizáciou spôsobí „značné riziko porušenia zákonov kvalifikovanej zahraničnej vlády." Podľa americkej právnej náuky sa tu uplatňuje tzv. *analýza komity*.[32] Medzinárodná komita je princíp pochádzajúci z common law tradície a týka sa prípadov konfliktu právnych poriadkov (t.j. amerického a zahraničného). Americké súdy používajú doktrínu medzinárodnej komity na obmedzenie dosahu národného práva.[33]

Súd má pri analýze komity zvážiť niekoľko faktorov[34] napríklad pravdepodobnosť, povahu a výšku sankcie, ktorá hrozí poskytovateľovi služby z dôvodu nesúladu právnych požiadaviek (t. j. povinnosti vydať a zákazu vydať požadované údaje), lokalizáciu a národnosť dotknutej osoby, dôleži-

[30] DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. In: *Stanford Law Review*. Vol. 71, 2018. [online]. [cit. 13.4.2019]. Dostupné na: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-law-making-2-0/.

[31] CHRISTAKIS, Theodore. *Lost In The Cloud? Law Enforcement Cross-Border Access To Data After The "Clarifying Lawful Overseas Use Of Data" (Cloud) Act And E-Evidence* [online]. 28.06.2018. [cit. 13.4.2019]. Dostupné na: https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/

[32] Tamtiež 30.

[33] DODGE S. William. International Comity in American Law, In: *Columbia Law Review*. Vol.115 No. 8 [online]. [cit. 13.4.2019]. Dostupné na: https://columbialawreview.org/content/international-comity-in-american-law/

[34] For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

tosť informácie pre vyšetrovanie prebiehajúce v Spojených štátoch a pravdepodobnosť včasného a efektívneho získania dôkazu alternatívnym spôsobom. Za zmienku stojí, že proti príkazu na uchovanie a vydanie počítačových údajov podľa slovenského Trestného poriadku[35] dnes nie je prípustný riadny opravný prostriedok zo strany adresáta príkazu. Do úvahy za určitých podmienok pripadá len ústavná sťažnosť.[36]

4. GDPR A KONFLIKT PRÁVNYCH PORIADKOV

Kolízia právnych poriadkov, o ktorej pojednáva CLOUD Act, môže nastať, ak sa na poskytovateľa, ktorému je doručený príkaz na vydanie záznamov o elektronickej komunikácii, zároveň vzťahuje *Všeobecné nariadenie o ochrane údajov*[37] (ďalej len ako „GDPR"). Nariadenie pritom svoju územnú pôsobnosť jednoznačne rozširuje aj na tých zahraničných (t. j. v Únii nesídliacich) poskytovateľov služieb (v kontexte ochrany osobných údajov prevádzkovateľov a sprostredkovateľov), ktorí buď ponúkajú tovary alebo služby dotknutým osobám v Únii, alebo sledujú ich správanie na území

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure; (B) the interests of the qualifying foreign government in preventing any prohibited disclosure; (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; (E) the nature and extent of the provider's ties to and presence in the United States; (F) the importance to the investigation of the information required to be disclosed; (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

[35] § 90 zákona č. 301/2005 Z. z. (Trestný poriadok).

[36] ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. In: *Revue pro právo a technologie*, Masarykova univerzita, 2015, roč. 6, č. 11, s. 29-48. ISSN 1804-5383.

[37] 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).

Únie.[38] Uvedené extrateritoriálne účinky GDPR sú obhajované „argumentom cielenia“ – ak zahraničný poskytovateľ cieli na zákazníkov v Únii, právo Únie sa zacieli naň.[39]

Prenos osobných údajov poskytovateľom služby z Únie do Spojených štátov na základe vykonávacej dohody v zmysle CLOUD Act nemá v GDPR jednoznačný právny základ a môže predstavovať pre poskytovateľa služby riziko. Riziko plynie buď z nesplnenia súdneho príkazu, alebo z možnosti udelenia sankcie za porušenie ochrany osobných údajov. Prevádzkovateľ a sprostredkovateľ v pôsobnosti GDPR môže uskutočniť prenos osobných údajov mimo územia Únie za splnenia podmienok stanovených v piatej kapitole GDPR.[40] Poskytovateľ služby elektronickej komunikácie, ktorý chce preniesť údaje do Spojených štátov na základe príkazu k prehliadke vydaného podľa CLOUD Act, môže porušiť GDPR, pokiaľ nespĺňa jednu z osobitných podmienok prenosu v článkoch 45 až 49 GDPR. Stručne upozorníme na články stanovujúce jednotlivé právne základy prenosu osobných údajov do tretej krajiny.

Článok 45 umožňuje prenos na základe rozhodnutia Európskej komisie, že daná krajina zaručuje primeranú úroveň ochrany osobných údajov.[41] Na prenos do krajín, ktoré podľa rozhodnutia Komisie spĺňajú podmienku primeranosti, nie je potom potrebné žiadne ďalšie povolenie. Ak neexistuje rozhodnutie o primeranosti, článok 46 dovoľuje uskutočniť prenos osobných údajov, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky (vymenované ďalej v tomto článku) a za podmienky, že dotknuté osoby majú k dispozícii *„vymožiteľné práva a účinné právne prostriedky nápravy.“*

[38] Článok 3 ods. 2 GDPR.

[39] HERT de Paul, CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, 2016, Vol. 6, No. 3. str. 231. [online]. [cit. 13.4.2019]. Dostupné na: https://academic.oup.com/idpl/article-abstract/6/3/230/2447252?redirectedFrom=fulltext.

[40] Pozri GDPR Článok 44 Všeobecná zásada prenosov.

[41] Zoznam krajín s primeranou úrovňou ochrany osobných údajov je odstupný na: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Článok 48 naopak špecifikuje, za akých okolností sa prenos alebo poskytovanie údajov nepovoľuje. Tento článok bol podľa Komisie prijatý práve v reakcii na dožiadania tretích krajín, ako to objasňuje recitál 115, keď uvádza: *„Niektoré tretie krajiny prijímajú zákony, iné právne predpisy a iné právne akty, ktoré priamo regulujú spracovateľské činnosti fyzických a právnických osôb v rámci jurisdikcie členských štátov.“* Recitál varuje: *„extrateritoriálne uplatňovanie týchto zákonov, iných právnych predpisov a iných právnych aktov môže byť v rozpore s medzinárodným právom a môže ohroziť ochranu fyzických osôb zaručenú Úniou v tomto nariadení,“* a záverom zdôrazňuje, že: *„prenosy by mali byť povolené, len ak sa splnia podmienky uvedené v tomto nariadení pre prenosy do tretích krajín.“*

Podľa Komisie článok 48 jasne stanovuje, že zahraničný súdny príkaz na vydanie dát sám osebe nepredstavuje právny základ pre prenos údajov mimo Únie, keď upravuje, že: *„akýkoľvek rozsudok súdu alebo tribunálu a akékoľvek rozhodnutie správneho orgánu tretej krajiny, ktorým sa od prevádzkovateľa alebo sprostredkovateľa vyžaduje preniesť alebo poskytnúť osobné údaje, môže byť uznané alebo vykonateľné akýmkoľvek spôsobom len vtedy, ak sa zakladá na medzinárodnej dohode, ako napríklad zmluve o vzájomnej právnej pomoci, platnej medzi žiadajúcou treťou krajinou a Úniou alebo členským štátom bez toho, aby boli dotknuté iné dôvody prenosu podľa tejto kapitoly*.“[42]

Európska únia a Spojené štáty podpísali zmluvu o vzájomnej právnej pomoci, ktorá nadobudla platnosť v roku 2010.[43] Táto zmluva o justičnej spolupráci ale neupravuje možnosť zahraničného orgánu verejnej moci ad-

[42] Article 48: Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

[43] Dohoda o vzájomnej právnej pomoci medzi Európskou úniou a Spojenými štátmi americkými podpísaná dňa 25. júna 2003. Pozri oznámenie č. 28/2010 Z. z. Ministerstva zahraničných vecí Slovenskej republiky o uzavretí Právneho nástroja medzi Slovenskou republikou a Spojenými štátmi americkými podľa článku 3 odseku 3 Dohody medzi Európskou úniou a Spojenými štátmi americkými o vzájomnej právnej pomoci podpísanej 25. júna 2003.

resovať príkazy na vydanie údajov priamo poskytovateľom elektronických komunikačných služieb. Článok 48 v závere dodáva, že existenciou relevantnej medzinárodnej dohody *„nie sú dotknuté iné právne základy prenosu údajov v zmysle piatej kapitoly*.“ Ak nie je naplnený žiaden z článkov 45 až 47 GDPR (čo je stav, ktorý v čase spísania svojho stanoviska Komisia predpokladá)[44], potom prenos údajov do tretej krajiny je možný, len ak je naplnená niektorá z výnimiek podľa článku 49.

Európska komisia adresovala americkému Najvyššiemu súdu v spomínanom konaní *Microsoft Ireland* podanie *amicus curiae,*[45] v ktorom uviedla, že pri prenose údajov v zmysle článku 49 GDPR sa ako najrelevantnejšie javia tieto výnimky:

- prenos je *nevyhnutný z dôležitých dôvodov verejného záujmu*.[46] Podľa odseku 4 verejný záujem musí byť uznaný v práve Únie alebo práve členského štátu, ktorému prevádzkovateľ podlieha. Komisia uvádza, že boj proti závažným trestným činom môže byť takýmto všeobecným verejným záujmom.
- prenos, ktorý je *nevyhnutný na účely závažných oprávnených záujmov, ktoré sleduje prevádzkovateľ a nad ktorými neprevažujú záujmy alebo práva a slobody dotknutej osoby, pričom prenos nie je opakujúcej sa povahy a týka sa len obmedzeného počtu dotknutých osôb*, *a zároveň prevádzkovateľ posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia poskytol vhodné záruky, pokiaľ ide o ochranu osobných údajov*. Prevádzkovateľ o takomto prenos informuje dozorný orgán. Podľa Komisie môžu „okolnosti“ zahŕňať procesné záruky, podľa ktorých bol zahraničný súdny príkaz vydaný.

Možno zhrnúť, že ak neexistuje rozhodnutie o primeranosti, ani sa nenaplní žiadna z primeraných záruk (vrátane záväzných vnútropodnikových

[44] Európska komisia. *Brief of the European Commission on behalf of the European union as amicus curiae in support of neither party*. [online]. [cit. 13.4.2019]. Dostupné na: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

[45] Tamtiež 44.

[46] Článok 49 ods. 1 písm d) GDPR.

pravidiel podľa článku 47 GDPR), prenos osobných údajov do tretej krajiny sa môže uskutočniť na základe výnimky pre osobitné situácie podľa článku 49 GDPR. Ich výklad má byť podľa Komisie skôr reštriktívny.[47]

5. PRÍSTUP TUZEMSKÝCH ORGÁNOV ČINNÝCH V TRESTNOM KONANÍ K DÁTAM V SPRÁVE AMERICKÉHO POSKYTOVATEĽA ELEKTRONICKÝCH SLUŽIEB

Ak orgány činné v trestnom konaní členských štátov Únie vyšetrujú trestné činy vlastných občanov a potrebujú ako dôkaz obsah elektronickej komunikácie uchovanej pod kontrolou amerického poskytovateľa služby, môžu žiadať o sprístupnenie dát diplomatickou cestou alebo na základe uzavretej dohody o medzinárodnej právnej pomoci. Podľa zmluvy MLAT sa európska krajina v prípade záujmu o obsahové dáta v správe amerického poskytovateľa služieb, musí obrátiť na americké Ministerstvo spravodlivosti a jeho Úrad pre medzinárodné záležitosti.[48] Úrad vykoná prvotný prieskum, aby sa zabezpečilo, že žiadosť obsahuje všetky potrebné informácie v požadovanej forme. Následne žiadosť postúpi do jurisdikcie, kde sa nachádza svedok alebo dôkaz. Americký prokurátor predloží žiadosť federálnemu súdu a navrhne vydanie súdneho príkazu, ktorý oprávňuje Spojené štáty, aby vykonali dožiadanie cudzieho štátu napr. formou federálneho súdneho príkazu na vydanie požadovaných údajov.[49]

Electronic Communications Privacy Act (ďalej ako „zákon o elektronických komunikáciách a ochrane súkromia“ alebo „ECPA“) *z* roku 1986 zakazuje[50] americkým poskytovateľom elektronických komunikačných služieb sprístupňovať zahraničným orgánom obsahové údaje o komunikácii užívateľov služieb.[51] Obsahové dáta môže zahraničný orgán získať iba na základe medzinárodnej dohody o vzájomnej právnej pomoci, pričom tento proces

[47] Tamtiež 44.

[48] Office of International Affairs in the Criminal Division of DOJ.

[49] GARLAND, Jim, BERENGAUT, Alexander a GOODLOE Katharine. *CLOUD Act Creates New Framework for Cross-Border Data Access* [online]. 26.03.2018. [cit. 13.4.2019]. Dostupné na: https://www.insideprivacy.com/cloud-computing/cloud-act-creates-new-framework-for-cross-border-data-access/

[50] 18 U.S. Code § 2702 (Voluntary disclosure of customer communications or records).

trvá v priemere deväť[52] až desať mesiacov.[53] Hlavnými dôvodmi odmietnutia dožiadania zo strany USA je nepreukázanie dôvodného podozrenia na spáchanie trestného činu (probable cause), následne zásada proporcionality (de minimis rule) a sloboda prejavu.[54] Neobsahové údaje môžu poskytovatelia služieb sprístupniť priamo zahraničným orgánom verejnej moci na dobrovoľnej báze. Týka sa to amerických poskytovateľov služieb a v obmedzenejšom rozsahu poskytovateľov so sídlom v Írsku, ktorí dobrovoľne odpovedajú na žiadosti orgánov presadzovania práva členských štátov Únie priamo, pokiaľ sa žiadosti týkajú neobsahových údajov.[55]

Zákon CLOUD Act vo svojej druhej časti zavádza odlišný mechanizmus prístupu zahraničných orgánov k dátam v správe amerických poskytovateľov. V novom režime by sa cudzia, napr. európska krajina mohla obrátiť priamo na poskytovateľa elektronickej komunikačnej služby bez potreby najprv odoslať žiadosť na americké ministerstvo. CLOUD Act však vytvára len predpoklad tohto postupu. Realizácia bude možná vo vzťahu k tým štátom, ktoré s USA uzavrú už spomínanú vykonávaciu dohodu, čím nadobudnú status tzv. kvalifikovanej vlády. Voči „kvalifikovanej krajine“

---

[51] CHRISTAKIS, Theodore. *Lost In The Cloud? Law Enforcement Cross-Border Access To Data After The "Clarifying Lawful Overseas Use Of Data" (Cloud) Act And E-Evidence* [online]. 28.06.2018. [cit. 13.4.2019]. Dostupné na: https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/

[52] KRISHNAMURTHY, Vivek. Cloudy with a Conflict of Laws. In: *Berkman Center Research Publication No. 2016-3.* No. 2016-3. Harvard University - Berkman Klein Center for Internet & Society. [online]. 16.02.2016. [cit. 23.4.2019]. Dostupné na: https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y

[53] Európska Komisia. Odporúčanie: Rozhodnutie rady o poverení začať rokovania so zreteľom na dohodu medzi Európskou úniou a Spojenými štátmi americkými o cezhraničnom prístupe k elektronickým dôkazom v oblasti justičnej spolupráce v trestných veciach [online]. 5. 2. 2019. [cit. 13.4.2019]. Dostupné na: http://ec.europa.eu/transparency/regdoc/rep/1/2019/SK/COM-2019-70-F1-SK-MAIN-PART-1.PDF

[54] Európsky Parlament: 4thWORKING 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]. 11.03.2019. [cit. 22.4.2019]. Dostupné na: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-636.343&format=PDF&language=EN&secondRef=01

[55] Tamtiež 52.

s uzavretou exekutívnou dohodou sa odstráni paušálny zákaz vydávania obsahových dát. Americkí poskytovatelia tak budú oprávnení vydať zahraničnému orgánu obsahovú elektronickú komunikáciu (uloženú ako aj prebiehajúcu *real-time*).[56] Zahraničná vláda sa vo vykonávacej dohode zaväzuje poskytnúť recipročné právo prístupu k údajom v správe „svojich" poskytovateľov elektronických služieb. V čase písania tohto príspevku žiadna exekutívna dohoda uzavretá podľa druhej časti CLOUD Act neexistuje.

Pre európske krajiny predstavuje uzavretie vykonávacej bilaterálnej dohody výhodu v tom, že im umožní žiadať od poskytovateľov služieb elektronickej komunikácie vydanie určitej kategórie údajov lokalizovaných v Spojených štátoch aj bez zdĺhavej diplomatickej cesty. Možno očakávať uzavretie vykonávacej recipročnej dohody o vydávaní dát medzi Európskou úniou a Spojenými štátmi? V samotnom znení CLOUD Act sa uvádza, že vykonávaciu dohodu môže uzavrieť kvalifikovaná zahraničná vláda, čo pojmovo nevystihuje integračné zoskupenie, ako je EÚ.[57] Avšak zrejme z praktických dôvodov Rada EÚ pre spravodlivosť a vnútorné veci podporila vo vzťahu k zákonu CLOUD Act spoločný prístup na úrovni EÚ.[58] Európska komisia odporučila Rade EÚ, aby Komisiu poverila rokovaním v mene Únie o dohode medzi Úniou a Spojenými štátmi americkými o cezhraničnom prístupe justičných orgánov v trestnom konaní k elektronickým dôkazom, ktoré uchováva poskytovateľ služieb.[59]

---

[56] MULLIGAN, P. Stephen. *Report of the Congressional Research Service on Cross-Border Data Sharing Under the CLOUD Act* [online] 23.4.2018. [cit. 13.4.2019]. Dostupné na: https://fas.org/sgp/crs/misc/R45173.pdf

[57] CHRISTAKIS, Theodore. *Lost In The Cloud? Law Enforcement Cross-Border Access To Data After The "Clarifying Lawful Overseas Use Of Data" (Cloud) Act And E-Evidence* [online]. 28.06.2018. [cit. 13.4.2019]. Dostupné na: https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/

[58] Rada Európskej únie: *Výsledky zasadnutia Rady pre spravodlivosť a vnútorné veci, 4. – 5. 6. 2018.* [online] [cit. 13.4.2019]. Dostupné na: https://www.consilium.europa.eu/media/36284/st09680-en18.pdf

[59] Európska komisia: *Odporúčanie - Rozhodnutie rady o poverení začať rokovania so zreteľom na dohodu medzi Európskou úniou a Spojenými štátmi americkými o cezhraničnom prístupe k elektronickým dôkazom v oblasti justičnej spolupráce v trestných veciach*. [online] 5.2.2019. [cit. 13.4.2019]. Dostupné na http://ec.europa.eu/transparency/regdoc/rep/1/2019/SK/COM-2019-70-F1-SK-MAIN-PART-1.PDF

Ak sa vykonávacou dohodou odstráni zákaz brániaci americkým poskytovateľom služieb reagovať na právne dožiadania ohľadom obsahových dát kvalifikovanej vlády, orgány participujúcej krajiny musia dodržiavať niekoľko zásad. Dožiadanie vydané zahraničným orgánom napríklad musí (1) byť vydané za účelom získania informácií týkajúcich sa prevencie, odhaľovania, vyšetrovania alebo stíhania závažnej trestnej činnosti, vrátane terorizmu; (2) sa musí vzťahovať na konkrétnu osobu, konto, účet, osobné zariadenie alebo iný identifikátor, (3) musí byť primerane odôvodnené, vychádzajúc z presných a dôveryhodných skutočností a (4) musí podliehať možnosti preskúmania alebo dohľadu zo strany súdu alebo iného nezávislého orgánu. Príkaz vydaný zahraničnou vládou zároveň nesmie byť použitý na porušovanie slobody prejavu.[60] V prípade príkazu na odpočúvanie sa vyžaduje, aby príkaz (1) bol vydaný na obmedzenú dobu, (2) nesmie trvať dlhšie, než je primerane potrebné na splnenie schválených účelov príkazu; (3) vydáva sa, len ak by sa tie isté informácie nemohli primerane získať inou, menej invazívnou metódou.[61]

Uvedeným spôsobom by orgány presadzovania práva z krajín Únie mohli žiadať o prístup k dátam osôb, ktoré nie sú americkými občanmi a nachádzajú sa mimo územia Spojených štátov. Prístup k obsahovaným údajom o amerických občanoch a osobách trvale usadených v USA bude naďalej možný iba prostredníctvom právnej pomoci najmä MLAT.[62] Uvedená limitácia vychádza z princípu, že štát má trestnú pôsobnosť prioritne nad vlastnými občanmi a cudzincami, ktorí majú na území danej krajiny trvalý pobyt.

[60] CLOUD Act (18 U.S. Code § 2523. Executive agreements on access to data by foreign governments

[61] Tamtiež 60.

[62] DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. In: *Stanford Law Review*. Vol. 71, 2018. [online]. [cit. 13.4.2019]. Dostupné na: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

6. LEGISLATÍVNY NÁVRH KOMISIE O CEZHRANIČNOM PRÍSTUPE K ELEKTRONICKÝM DÔKAZOM

V apríli 2018 Európska komisia predstavila návrh právneho rámca, ktorý umožní adresovať príkazy týkajúce sa elektronických dát priamo poskytovateľom elektronických služieb[63] pôsobiacim v inom členskom štáte EÚ. Legislatívny návrh upravuje predkladanie a uchovávanie elektronických dôkazov na účely trestného konania v inom členskom štáte Únie. Návrh pozostáva z dvoch vzájomne súvisiacich predpisov:

- Nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach
- Smernice, ktorou sa stanovujú harmonizované pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

Síce sa členské štáty svojej suverenity v trestných veciach vzdávajú v prospech aproximácie pomerne neochotne, v tomto prípade niektoré krajiny naopak apelovali na zjednotenie postupu na úrovni Únie.[64] Dôvodom je to, že získanie elektronických dôkazov, ktoré sú spracúvané poskytovateľmi v inom členskom state alebo spoločnosťami „veľkej päťky“ (Apple, Alphabet, Microsoft, Facebook, Amazon),[65] je v trestnom konaní zdĺhavé, nakoľko orgány činné v trestnom konaní sú v zásade limitované svojou územnou pôsobnosťou. V navrhovanom nariadení sa upúšťa od využívania

[63] Do rozsahu pôsobnosti nariadenia patria poskytovatelia elektronických komunikačných služieb; poskytovatelia služieb informačnej spoločnosti, pre ktorých ukladanie údajov predstavuje kľúčový prvok služieb, ktoré poskytujú používateľovi vrátane sociálnych sietí, ak nie sú považované za elektronické komunikačné služby; online trhy umožňujúce transakcie medzi ich používateľmi (ako sú spotrebitelia alebo podniky) a iní poskytovatelia hostingových služieb a poskytovatelia služieb internetových názvov domén a číslovania.

[64] FRANSSEN, Vanessa. *The European Commission's E-Evidence Proposal: Toward An EU-Wide Obligation For Service Providers To Cooperate With Law Enforcement*? [online] 12.10.2018. [cit. 13.4.2019]. Dostupné na: https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

[65] SEN, Conor. *The 'Big Five' Could Destroy the Tech Ecosystem*. [online] 15.11.2017. [cit. 23.4.2019]. Dostupné na https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem

umiestnenia údajov ako rozhodujúceho kolízneho kritéria.[66] Návrh zohľadňuje, že o mieste uloženia dát rozhodujú vo väčšine prípadov samotní poskytovatelia, ktorí v záujme optimalizácie dostupnosti svojich služieb využívajú decentralizované systémy, cloudovú infraštruktúru, siete na doručovanie obsahu (content delivery network), v dôsledku čoho určovanie jurisdikcie podľa umiestnenia dát stráca opodstatnenie.

Novým legislatívnym nástrojom sa upravujú iba cezhraničné dožiadania, tzn. v situácie, ak je poskytovateľ služby usadený alebo zastúpený v inom členskom štáte než dožadujúci orgán činný v trestnom konaní. Dožadujúci orgán členského štátu môže nariadiť poskytovateľovi služieb, ktorý ponúka služby v rámci Únie, aby na základe európskeho príkazu poskytol alebo uchoval elektronické dôkazy. Európsky príkaz na uchovanie dôkazov umožňuje iba uchovanie údajov, ktoré sú v čase prijatia príkazu už uložené, a nie prístup k údajom, ktoré budú uložené v budúcnosti po vydaní príkazu.[67] Nariadenie nevyžaduje od poskytovateľov, aby systematicky zbierali alebo ukladali viac údajov, než zbierajú alebo ukladajú z prevádzkových dôvodov alebo z dôvodu dodržiavania iných právnych požiadaviek.[68]

Adresát príkazu bude poskytovať orgánu iného členského štátu súčinnosť bez zapojenia či kontroly zo strany orgánov členského štátu, v ktorom je poskytovateľ služieb sám usadený alebo zastúpený. Výnimkou je situácia, ak adresát príkaz nevykoná. V takom prípade sa bude vyžadovať vymáhanie príkazu orgánom krajiny, v ktorej sa nachádza zástupca poskytovateľa služby. Navrhovaná lehota na vybavenie žiadosti je 10 dní. V neodkladných prípadoch, ak je ohrozený život alebo „telesná nedotknuteľnosť osoby, alebo kritickej infraštruktúry“, je adresát povinný odpovedať do 6 hodín.

Ak je príkaz neúplný, obsahuje zjavné chyby alebo nedostatočné informácie na vykonanie, adresát môže kontaktovať vydávajúci orgán a požiadať o objasnenie prostredníctvom určeného formulára. Ak poskytovateľ služby

[66] Dôvodová správa návrhu Nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [online] 17. 4. 2018. [cit. 13.4.2019]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

[67] Tamtiež 66.

[68] Tamtiež 66.

nemôže príkaz splniť z dôvodu vyššej moci alebo faktickej nemožnosti (napr. osoba, ktorej údaje sa požadujú, nie je jeho zákazníkom alebo údaje boli vymazané pred prijatím príkazu), takisto je povinný informovať vydávajúci orgán. Adresát môže namietať voči presadzovanému príkazu, ak sa domnieva na „základe informácií, ktoré sú v ňom uvedené, že sa ním zjavne porušuje Charta základných práv EÚ alebo že predstavuje zjavné zneužitie." Vykonanie analýzy súladu príkazu s Chartou súkromnými spoločnosťami namiesto štátnych inštitúcií je kritizované ako „privatizácia presadzovania práva" a túto časť kritizujú aj samotní poskytovatelia služieb.[69] Tak ako v prípade príkazov k prehliadke podľa CLOUD Act, aj príkaz podľa pripravovaného nariadenia bude môcť adresát navrhnúť na preskúmanie, pokiaľ čelí konfliktným právnym povinnostiam. Vyžaduje sa, aby poskytovateľ služby v takom prípade informoval vydávajúci orgán prostredníctvom odôvodnenej námietky, že vykonaním európskeho príkazu na predloženie dôkazov by adresát porušil právne predpisy tretej krajiny. Vydávajúci orgán na základe namietaných dôvodov preskúma vlastný príkaz a môže rozhodnúť, že ho stiahne, čím sa proces končí. Ak vydávajúci orgán má v úmysle potvrdiť európsky príkaz na predloženie dôkazov, požiada o preskúmanie súd vo svojom členskom štáte. Ak súd zistí, že neexistuje relevantný konflikt, súd príkaz potvrdí. Naopak, ak súd dospeje k záveru, že konflikt existuje, musí požiadať o stanovisko príslušnú tretiu krajinu. Pokiaľ tretia krajina potvrdí existenciu konfliktu a namietne proti vykonaniu príkazu, príslušný súd príkaz zruší.[70]

Do pôsobnosti nariadenia budú spadať aj poskytovatelia služieb, ktorí nie sú usadení ani zastúpení v Únii, ale poskytujú služby v rámci Únie.[71]

---

[69] European Telecommunications Network Operators' Association. *ETNO position paper on improving cross-border access to electronic evidence in criminal matters*. [online] [cit. 22.4.2019]. Dostupné na https://etno.eu/datas/positions-papers/2018/ETNO%20position%20paper%20on%20improving%20cross-border%20access%20to%20electronic%20evidence%20in%20criminal%20matters.pdf alebo E-Evidence Proposal: EuroISPA Criticises the Privatisation of Law Enforcement[online] [cit. 22.4.2019]. Dostupné na: http://www.euroispa.org/e-evidence-proposal-euroispa-criticises-privatisation-law-enforcement/

[70] Článok 15 návrhu Nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[71] Článok 3 ods. 1 návrhu Nariadenia: Toto nariadenie sa uplatňuje na poskytovateľov služieb, ktorí ponúkajú služby v Únii.

Samotná dostupnosť webového sídla poskytovateľa podľa dôvodovej správy nie je jedinou podmienkou,[72] poskytovanie služieb v Únii musí byť aktívne. Na uplatňovanie navrhovaného nariadenia bude potrebná podstatná väzba poskytovateľa k daným členským štátom. Takáto podstatná väzba existuje, ak poskytovateľ služieb má v členskom štáte prevádzkareň. V prípade, že v Únii prevádzkareň zriadenú nemá, kritérium podstatnej väzby by sa malo posudzovať na základe existencie významného počtu používateľov v jednom alebo vo viacerých členských štátoch, alebo na základe zamerania činností na jeden alebo viac členských štátov. Zameranie činností možno predpokladať, ak poskytovateľ používa jazyk alebo menu členského štátu, ak umožnil v príslušnom vnútroštátnom obchode stiahnutie jeho aplikácie.[73] Uplatniť možno aj kritérium cielenia podnikateľskej činnosti, ktorý používa Nariadenie o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach.[74] Nariadenie GDPR pokrýva aj prevádzkovateľov, ktorí nemajú fyzickú prítomnosť v Únii, no napriek tomu sa od nich vyžaduje dodržiavanie nariadenia a znášanie vysokých administratívnych pokút.[75] „E-evidence balík" ide ešte ďalej a od zámorských podnikov poskytujúcich služby v Únii (vrátane sociálnych sietí) vyžaduje určenie právnych zástupcov, ktorých úlohou bude prijímať príkazy vydané v zmysle nariadenia. Právny zástupca musí byť v jednom z členských štátov, v ktorom je poskytovateľ služieb usadený alebo v ktorom ponúka služby. Obdobnú požiadavku už má zakotvené Nemecko, ktoré prijalo *zákon na zlepšenie presadzovania práva v sociálnych sieťach*,[76] ktorým ukladá posky-

[72] Dôvodová správa návrhu Nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [online] 17. 4. 2018. [cit. 13.4.2019]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

[73] Recitál 48 návrhu Nariadenia Európskeho Parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[74] Článok 17 ods. 1 písm. c) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 1215/2012 z 12. decembra 2012 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (Ú. v. EÚ L 351, 20.12.2012).

[75] AZZI, Adèle. The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. In: *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*. [online] Release 2018. [cit. 14.4.2019]. Dostupné na: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723/JIPITEC_9_2_2018_126_Azzi

tovateľom sociálnych sietí povinnosť, aby určili osobu v Nemecku, ktorá bude oprávnená prijímať podnety týkajúce sa presadzovania práva.

Predmetom európskeho príkazu na predloženie dôkazov môžu byť štyri kategórie údajov:

- údaje o totožnosti predplatiteľa alebo zákazníka - poskytnuté meno, dátum narodenia, poštová adresa alebo geografická adresa, fakturačné údaje a údaje o platbách, telefónne číslo, e-mail a tiež údaje o type služby a jej trvaní
- údaje o prístupe - súvisiace so začatím a ukončením relácie prístupu používateľa k službe, dátum a čas použitia alebo prihlásenie sa do služby a odhlásenie sa z nej spolu s IP adresou, ktorú poskytovateľ služieb prístupu na internet pridelil používateľovi služby, údajmi identifikujúce použité rozhranie a identifikačné údaje používateľa.
- údaje o transakciách - napríklad zdroj a miesto určenia správy, údaje o umiestnení zariadenia, dátume, čase, trvaní, veľkosti, formáte, použitom protokole, druhu kompresie, pokiaľ tieto údaje nepredstavujú údaje o prístupe.
- obsahové údaje - text, hlas, video, obrázky alebo zvuk.

Návrh nariadenia rozlišuje, aký orgán môže vydať európsky príkaz na predloženie dôkazov týkajúci sa (i) údajov o predplatiteľoch a údajov o prístupe (ii) údajov o transakciách a obsahových údajov (iii) príkaz na uchovanie dôkazov. Presné vymedzenie oprávneného orgánu sa musí posúdiť aj podľa vnútroštátneho práva členského štátu, ktorý príkaz vydáva. Zásah do súkromia dotknutého používateľa a dôkazná hodnota získaných údajov bude vyššia pri údajoch o transakciách a obsahových údajov, preto je príkaz na ich vydanie podmienený súdnym prieskumom. Ostatné príkazy (údajov o predplatiteľoch alebo o prístupe) by v podmienkach SR mohol vydať aj prokurátor, v podmienkach ČR státní zástupce.

[76] Anglická verzia dostupná na: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?_blob=publicationFile&v=2

Oba typy príkazov (na predloženie a na uchovanie dôkazov) je možné vydať len v trestnom konaní. Príkazy na predloženie údajov o predplatiteľoch a údajov o prístupe môžu byť vydané pri akomkoľvek trestnom čine, zatiaľ čo príkaz na predloženie údajov o transakciách alebo obsahových údajov môže byť vydaný len k trestným činom, (i) na ktoré sa vo vydávajúcom štáte vzťahuje trest odňatia slobody s hornou hranicou minimálne 3 roky alebo (ii) k špecifickým trestným činom, ktoré sa uvádzajú v návrhu[77] a boli spáchané prostredníctvom informačného systému (iii) k trestným činom, na ktoré sa vzťahuje smernica o boji proti terorizmu.[78]

7. ZÁVER

V Únii ako aj na medzinárodnej úrovni sa akcentuje potreba zjednodušenia cezhraničného prístupu orgánov presadzovania práva k elektronickým údajom, čo potvrdzujú nové legislatívne iniciatívy EÚ a USA zamerané na umožnenie priameho adresovania zahraničného dožiadania súkromným spoločnostiam poskytujúcim elektronické komunikačné služby.[79] Zákon CLOUD Act vytvoril pre zahraničie možnosť nového spôsobu prístupu k údajom v dispozícii amerických poskytovateľov služieb a tým vytvoril „medzinárodnú normu cestou národnej regulácie.“[80] Na druhej strane je tu tzv. bruselský efekt, snaha Európskej únie externalizovať svoje právne predpisy mimo jej hraníc prostredníctvom trhových mechanizmov, čo takisto

[77] Rámcové rozhodnutie Rady 2001/413/SVV z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov (Ú. v. ES L 149, 2.6.2001, s. 1). Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).

[78] Smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017, s. 6).

[79] STEFAN, Marco, FUSTER Gloria G. Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. In *CEPS Paper in Liberty and Security in Europe* [online]. 2018. [cit. 24.4.2019]. Dostupné na: https://www.ceps.eu/system/files/MS%26GGF_JudicialCooperationInCriminalMatters.pdf

[80] DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. In: *Stanford Law Review*. Vol. 71, 2018. [online]. [cit. 13.4.2019]. Dostupné na: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

vytvára jednostrannú regulačnú globalizáciu.[81] Extrateritoriálny efekt má nepochybne aj navrhované „E-evidence“ nariadenie a smernica. Možno zhrnúť, že jednostranné rozšírenie jurisdikcie mimo vlastných územných hraníc nie je zriedkavým javom a snaží sa o ňu väčšina krajín, najmä vo vzťahu k trestným veciam.[82]

Navrhované právne riešenia musia hľadať rovnováhu medzi početnými záujmami. Orgány činné v trestnom konaní požadujú efektívne prostriedky na zabezpečenie skutočností relevantných pre trestné konanie. Poskytovatelia elektronických služieb žiadajú transparentné a medzištátne nekonfliktné predpisy o vydávaní údajov o používateľoch ich služieb. A používatelia služieb (či už sa voči nim vedie trestné konanie alebo nie) očakávajú dodržiavanie základných práv a princípov trestného konania.

8. ZOZNAM POUŽITÝCH ZDROJOV

8.1 LITERATÚRA

[1] ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. In: *Revue pro právo a technologie*, Masarykova univerzita, 2015, roč. 6, č. 11, s. 29-48. ISSN 1804-5383.

[2] AZZI, Adèle. The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. In: *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*. [online] 2018. [cit. 14.4.2019]. Dostupné na: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723/JIPITEC_9_2_2018_126_Azzi

[3] DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. In: *Stanford Law Review*. Vol. 71, 2018. [online]. [cit. 13.4.2019]. Dostupné na: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

[4] DODGE S. William. International Comity in American Law, In: *Columbia Law Review*. Vol.115 No. 8 [online]. [cit. 13.4.2019]. Dostupné na: https://columbialawreview.org/content/international-comity-in-american-law/

[81] SCOTT, Joanne. Extraterritoriality and Territorial Extension in EU Law. In: *American Journal of Comparative Law*, Vol. 62, No. 1, 2014. Dostupné na: https://ssrn.com/abstract=2276433

[82] AZZI, Adèle. The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. In: *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*. [online] 2018. [cit. 14.4.2019]. Dostupné na: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723/JIPITEC_9_2_2018_126_Azzi

[5] HERT de Paul, CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: *International Data Privacy Law*, 2016, Vol. 6, No. 3. str. 231. [online]. [cit. 13.4.2019]. Dostupné na: https://academic.oup.com/idpl/article-abstract/6/3/230/2447252?redirectedFrom=fulltext.

[6] KRISHNAMURTHY, Vivek. Cloudy with a Conflict of Laws. In: *Berkman Center Research Publication No. 2016-3*. No. 2016-3. Harvard University - Berkman Klein Center for Internet & Society. [online]. 16.02.2016. [cit. 23.4.2019]. Dostupné na: https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y

[7] POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kolektiv. Elektronické důkazy v trestním řízení. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7. s. 156.

[8] SCOTT, Joanne. Extraterritoriality and Territorial Extension in EU Law. In: *American Journal of Comparative Law*, Vol. 62, No. 1, 2014. Dostupné na: https://ssrn.com/abstract=2276433

[9] 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. ISSN: 1086-3818.

8.2 PRÁVNE PREDPISY A JUDIKATÚRA

[10] Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018)

[11] Dohoda o vzájomnej právnej pomoci medzi Európskou úniou a Spojenými štátmi americkými podpísaná dňa 25. júna 2003

[12] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. 4. 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)

[13] Smernica Európskeho parlamentu a Rady 2014/41/EÚ zo 3.4. 2014 o európskom vyšetrovacom príkaze v trestných veciach

[14] Návrh Nariadenia o európskom príkaze na predloženie a uchovanie elektronických ďokazov v trestných veciach. [online] 17. 4. 2018. [cit. 13.4.2019]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

[15] United States v. Microsoft Corp. (Microsoft Ireland), No. 17-2, (Apr. 17, 2018) In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation

8.3 ELEKTRONICKÉ ZDROJE

[16] CHRISTAKIS, Theodore. *Lost In The Cloud? Law Enforcement Cross-Border Access To Data After The "Clarifying Lawful Overseas Use Of Data" (Cloud) Act And E-Evidence* [online]. 28.06.2018. [cit. 13.4.2019]. Dostupné na: https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/

[17] Európska komisia. *Brief of the European Commission on behalf of the European union as amicus curiae in support of neither party*. [online]. [cit. 13.4.2019]. Dostupné na: https://www.-supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

[18] Európska Komisia. *Factsheet - Security Union - Facilitating Access to electronic evidence* [online]. 17.04.2018. [cit. 13.4.2019]. Dostupné na: http://europa.eu/rapid/attachment/MEMO-18-3345/en/Factsheet%20E-evidence.pdf

[19] Európska Komisia. Odporúčanie: Rozhodnutie rady o poverení začať rokovania so zreteľom na dohodu medzi Európskou úniou a Spojenými štátmi americkými o cezhraničnom prístupe k elektronickým dôkazom v oblasti justičnej spolupráce v trestných veciach [online]. 5. 2. 2019. [cit. 13.4.2019]. Dostupné na: http://ec.europa.eu/transparency/regdoc/rep/1/2019/SK/COM-2019-70-F1-SK-MAIN-PART-1.PDF

[20] Európsky Parlament: 4thWORKING 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]. 11.03.2019. [cit. 22.4.2019]. Dostupné na: http://www.europarl.europa.eu/sides/getDoc.dotype=COMPARL&reference=PE-636.343&format=PDF&language=EN&secondRef=01

[21] FRANSSEN, Vanessa. *The European Commission's E-Evidence Proposal: Toward An EU-Wide Obligation For Service Providers To Cooperate With Law Enforcement*? [online] 12.10.2018. [cit. 13.4.2019]. Dostupné na: https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

[22] GARLAND, Jim, BERENGAUT, Alexander a GOODLOE Katharine. *CLOUD Act Creates New Framework for Cross-Border Data Access* [online]. 26.03.2018. [cit. 13.4.2019]. Dostupné na: https://www.insideprivacy.com/cloud-computing/cloud-act-creates-new-framework-for-cross-border-data-access/

[23] Hogan Lovells. *Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR* [online]. 15.01.2019. [cit. 13.4.2019]. Dostupné na: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf

[24] LOEB, Robert, GOLDMAN, Brian a TABATABAI Emily. *The CLOUD Act, Explained* [online]. 06.04.2018 [cit. 14.4.2019]. Dostupné na: https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained

[25] McCann FitzGerald. *Changes to Cross-Border Access to Electronic Evidence Mean it's Decision Time for Ireland* [online]. 20.06.2018. [cit. 23.4.2019]. Dostupné na: https://www.mccannfitzgerald.com/knowledge/disputes/changes-to-cross-border-access-to-electronic-evidence

[26] SEN, Conor. *The 'Big Five' Could Destroy the Tech Ecosystem*. [online] 15.11.2017. [cit. 23.4.2019]. Dostupné na https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem

[27] STEFAN, Marco, FUSTER Gloria G. Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. In *CEPS Paper in Liberty and Security in Europe* [online]. 2018. [cit. 24.4.2019]. Dostupné na: https://www.ceps.eu/system/files/MS%26GGF_JudicialCooperationInCriminalMatters.pdf

---
