PRÁVNA PRAX

Digitálne dokazovanie v trestnom konaní

Digitálne dokazovanie v trestnom konaní

JUDr. Miroslav Srholec, PhD.

C·H·BECK

Vzor citácie:

Srholec, M. Digitálne dokazovanie v trestnom konaní, 1. vydanie. Bratislava : C. H. Beck, 2026, 204 s.

Publikáciu napísal JUDr. Miroslav Srholec, PhD.
Vydalo Nakladatelství C. H. Beck, s. r. o., organizačná zložka v Bratislave roku 2026
Michalská 9, 811 01 Bratislava, beck@beck.sk
Prvé vydanie
Redaktori publikácie: JUDr. Jana Amorová, Mgr. Ľuba Nitrová
Tlač: Marten, spol. s r. o.

ISBN 978-80-8232-093-3

O autorovi

JUDr. Miroslav Srholec, PhD.

sa narodil v roku 1989 v Lučenci. Štúdium práva absolvoval na Právnickej fakulte Univerzity Pavla Jozefa Šafárika v Košiciach, kde v roku 2025 ukončil aj doktorandské štúdium v odbore trestné právo. Od roku 2009 je príslušníkom Policajného zboru, kde postupne prešiel viacerými útvarmi, pričom od roku 2015 pôsobí na trestnom úseku ako vyšetrovateľ hospodárskej a ekonomickej kriminality. Počas praxe absolvoval viaceré špecializované kurzy a absolvoval pracovné pobyty v Haagu, Madride a Lille. V súčasnosti pôsobí na Krajskom riaditeľstve PZ v Košiciach.

Je autorom viacerých publikačných výstupov zameraných na trestné právo, na ktoré eviduje množstvo ohlasov. V minulosti pravidelne prispieval do odborného časopisu Právne listy.sk. Aktuálne sa venuje aj vzdelávacej činnosti v rámci Policajného zboru.

Recenzenti:

prof. JUDr. Sergej Romža, PhD.

prof. JUDr. Ivan Šimovček, CSc.

prof. JUDr. Jozef Záhora, PhD.

prof. JUDr. Peter Polák, PhD.

Obsah

Kapitola 3.
Cezhraničné získavanie digitálnych dôkazov

1. Priblíženie problematiky cezhraničného získavania dig. dôkazov

26 V súčasnosti je mimoriadne zložité vypozorovať také trestné konanie o kyberkriminalite, v ktorom by nebolo potrebné akékoľvek cezhraničné získavanie dôkazných prostriedkov. Uvedený prvok v súčasnosti už opúšťa výhradné teritórium kybernetických trestných činov a pozorujeme nárast okruhu trestných konaní, či ide o vraždu, lúpež alebo krádeže či iné trestné činy, kde je trestné konanie nutné pre úplnosť dokazovania dopĺňať aj o výťažky aplikácie cezhraničných elektronických dôkazných prostriedkov. Akékoľvek priblíženie problematiky elektronických dôkazných prostriedkov bez priblíženia právneho rámca, procedúr a stavu cezhraničného získavania dôkazov nemožno považovať za úplné, pretože ide o validnú časť samotnej problematiky.

Technické zázemie elektronických dôkazných prostriedkov je jedným z najdynamickejších odvetví vôbec. Už v súčasnosti možno badať oligopolizáciu trhu nielen internetových služieb. Podiel na trhu užívateľov je prevažne rozdelený medzi veľkých hráčov, ako sú spoločnosti Meta[272], Google, Microsoft, Apple a pod., ktoré disponujú ohromným množstvom dát. Internetové služby sa poskytujú rôznymi buď nadnárodnými alebo regionálnymi poskytovateľmi globálne. Uvedená situácia vedie k stavu, keď je veľká časť dostupných dát, ktoré v zásade nemajú teritoriálnu povahu, mimo klasických štátnych hraníc, a tým sa údaje o páchaní trestnej činnosti spáchanej napr. na území Slovenska zdigitalizujú, fragmentujú medzi rôzne nosiče, častokrát delokalizujú z miesta páchania trestnej činnosti a najmä prostredníctvom internetu a globalizujú sa nabraním virtuálnej povahy. Virtuálnu povahu by sme mohli priblížiť práve stavom *ubiquity*, teda všadeprítomnosti a všadeprístupnosti k údajom nehmotného charakteru.

Len obmedzené množstvo užívateľských dát potrebných pri dnes už zvyčajných vyšetrovaniach s medzinárodným prvkom, možno lokalizovať na území SR. Problematika elektronických dôkazných prostriedkov bezprostredne obrusuje základnú charakteristiku štátneho trestného práva, a to teritorialitu trestného práva.

---

[272] Sociálna site Facebook, spoločnosti Meta získava napr. z mobilného zariadenia o užívateľovi, pre komerčné účely až 98 osobných údajov v 32 základných okruhoch informácií ako napríklad lokalizačné informácie, IP adresu, históriu platieb, profilové informácie, históriu vyhľadávania ale aj obsahové údaje zariadenia či taktiež využíva inštalované príslušenstvo ako napr. kamery a mikrofóny. Naviac sociálna sieť Facebook, nie je vo svete BIG TECH nijak zvedavá na súkromie svojich užívateľov. V porovnaní so spoločnosťami Google, Twitter, Amazon, Apple skončil Facebook až na predposlednom mieste so skóre 14, pričom víťazná spoločnosť Google dosiahla skóre až 39. Bližšie pozri: SECURITY.ORG. 2025. The Data Big Tech Companies Have On You. Dostupné na: https://www.security.org/resources/data-tech-companies-have/ (citované 2025-04-21).

Uvedená situácia nie je špecifikom len Slovenska, ide o všeobecný, globálny trend. Dnes už určite obsolentný prieskum EÚ ešte z roku 2018 realizovaný medzi európskymi LEA priniesol výsledok, že až 85 % trestných konaní je s prítomným prvkom elektronických dôkazných prostriedkov a až v 50 % trestných konaní je potrebná cezhraničná aplikácia EDP. V súčasnosti možno dôvodne predpokladať, že údaje by boli v aktualizovanom prieskume ešte vyššie.[273] K podobnému stavu sa určitým tempom približuje tuzemská prax.

Z uvedeného dôvodu preto musíme medzi EDP zaradiť aj nástroje cezhraničnej spolupráce pri obstarávaní digitálnych stôp v súvislosti s vyšetrovaním trestnej činnosti.

Význam a rozsah cezhraničnej spolupráce ilustrujeme na problematike *Cloud Computing,* zjednodušene *cloudu*, a následne by sme priblížili progresívne možnosti cezhraničnej aplikácie EDP.

2. *Cloud*

„*Cloud computing je model umožňujúci všadeprítomný, pohodlný sieťový prístup na požiadanie k zdieľanému fondu konfigurovateľných výpočtových zdrojov (siete, servery, úložiská, aplikácie a služby), ktoré môžu byť rýchlo poskytnuté a uvoľnené s minimálnym úsilím o riadenie interakcie poskytovateľa služieb*“[274]. Jednou z najväčších výhod *cloudových* služieb je okamžitý prístup k dostačujúcemu dátovému výkonu či úložnému priestoru. *Cloud* však nemožno stotožňovať s klasickým *hostingom*[275]. 27

Ako hlavný problematický moment sa v súčasnosti javí skutočnosť, že väčšina veľkých poskytovateľov *cloudových* služieb ako napríklad Amazon (*AWS*), Microsoft (*Azure*), Google (*Google App Engine*), Apple (*iCloud*) a pod. nie je poskytovaná z územia SR, a teda je mimo dostupnosti zvyčajných teritoriálnych inštitútov trestného práva.

Trestné činy s prvkom *Cloudu* sa vyznačujú nezávislosťou od geografickej lokalizácie, a to či už užívateľa, prevádzkovateľa či technického zázemia samotnej technológie. Hlavnou výhodou *cloudových* služieb, ako už bolo uvedené, je okrem iného flexibilné a bezprostredné poskytovanie dátového či úložného priestoru podľa aktuálnych potrieb subjektu, bezproblémový rozvoj IT infraštruktúry bez nutnosti veľkých investícií do technického zázemia či kvalifikovanej pracovnej sily, IT *security* manažment, cenová úspora, okamžitý

[273] Commission Staff Working Document Impact Assessment. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. 2018. Dostupné na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN (citované 2025-04-19).

[274] National Institute of Standards and Technology (NIST) Mell, Grace 2011.

[275] *Hlaváčová, K., Chorvát, O.* Přístup orgánu činných v trestním řízení k datům uloženým v cloudu. Revue pro právo a technologie, 2016, roč. 7, č. 14.

prístup k veľkým výpočtovým výkonom, ako aj ďalšie[276]. V súčasnosti je populárny tzv. hybridný *Cloud*, teda využívanie niekoľkých *cloudových* architektúr súčasne[277]. Navyše podľa predikcie Gartnerovej štúdie z roku 2023 by malo byť roku 2028 až 70 % podnikovej pracovnej záťaže v *Cloude*[278].

S prihliadnutím na stav danej technológie nie ja reálne, aby orgány činné v trestnom konaní efektívne zistili konkrétne cieľové úložisko dát potrebných na realizáciu inštitútov trestného konania pre praktickú aplikáciu trestných inštitútov cezhraničného prístupu k dôkazom. Nie je nezvyčajná ani situácia, keď ani samotní poskytovatelia *Cloudu* nemajú presné informácie, kde presne je využívaný dátový výkon a kde je aktuálne využívané dátové úložisko pre služby *Cloudu*. Technické zázemie *cloudových* služieb, tzv. (data)farmy sú zvyčajne rozmiestnené naprieč viacerými štátmi či svetadielmi. Navyše viaceré *cloudové* spoločnosti dynamicky využívajú svoje výpočtové, ako aj úložné kapacity za účelom zabezpečenia efektivity poskytovaných služieb.

Technické zázemie *Cloudu* kladie pred OČTK náročnú výzvu, od ktorého štátu požadovať sprístupnenie údajov formou cezhraničnej spolupráce[279]. Uvedený problém bol riešený v USA pomerne jednoduchou cestou, priamym príkazom prevádzkovateľovi ponad jurisdikčné kompetencie okresných súdov[280,281]. Uvedený prístup sa snaží adoptovať aj Európska únia.

Problematiku si môžeme priblížiť na príklade výkonu domovej prehliadky, kde orgány činné v trestnom konaní zaistia notebook. Navzdory skutočnosti fyzického zaistenia tohto elektronického zariadenia aj s prístupovými údajmi orgány činné v trestnom konaní nie sú v zmysle zvyčajného výkladu oprávnené realizovať prihlásenie do *cloudovej* služby, stiahnuť uložené dáta a zabezpečiť

---

[276] Bližšie pozri: ETREND.SK. 2019. Dostupné na: https://www.trend.sk/biznis/cloud-moderny-pohlad-riesenia-erp (citované 2025-04-21).

[277] Bližšie pozri: ETREND.SK. 2022. Dostupné na: https://www.trend.sk/spravy/ako-hybridny-cloud-odpoved-najdete-konferencii-cloudy (citované 2025-04-21).

[278] Bližšie pozri: GARTNER.COM. 2023. Dostupné na: https://www.gartner.com/en/publications/devising-an-effective-cloud-strategy resp. https://www.techrepublic.com/article/gartner-cloud-computing-future/ (citované 2025-04-21).

[279] V rámci poznatkov zo spolupráce v rámci JIT Monkey/Washer od príslušníkov Nemeckej spolkovej polície Baden-Württemberg, jednotka Esslingen bolo zistené, že problematika Cloudu je aktuálne veľmi diskutovanou témou aj v zahraničí, pričom za veľký prínos je považovaný práve 2. dodatkový protokol k Budapeštianskemu dohovoru.

[280] Za prvý trestný čin v súvislosti s Cloud Computing bol riešený v USA už v roku 2011, avšak prvé zoznamovanie sa s technológiou možno vysledovať do roku 2006. Problematiku cezhraničného prístupu k elektronickým dátam možno vysledovať k prípadu *United States v. Drew (2009)*. Bližšie pozri: *Dykstra, J.* Seizing Electronic Evidence from Cloud Computing Environments. In: Cloud Technology. 2015, s. 156 – 185.

[281] Neskorším rozhodnutím vo veci *United States v. Microsoft Corp.*, 584 U.S., 138 S. Ct. 1186, už súd konštatoval, že spoločnosť Microsoft nemá povinnosť sprístupňovať cezhraničné údaje. Uvedený záver súdu viedol v USA k prijatiu tzv. CLOUD ACT, H.R.494, ktorý umožňuje cezhraničný prístup k dátam v zahraničí. Rozhodnutie dostupné na: https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412 z 15. 4. 2025.

tak podklady určené pre trestné konanie uvedené v príkaze na domovú prehliadku. Tuzemské orgány by uvedeným postupom *de facto* sťahovali dáta z teritória iného štátu, resp. štátov, čím by bezprostredne zasahovali do základnej zásady medzinárodného práva, a to teritoriálnej suverenity, a teda do výlučnej kompetencie cudzoštátnych justičných orgánov.

Takmer celá právna náuka o zaisťovacích inštitútoch trestného práva procesného je smerovaná najmä k fyzickému nosiču, pričom pri *Cloude* ide práve o skutočnosť, že ide o nosič zdanlivý či virtuálny, ktorý je po obsahovej stránke len v obmedzenej miere k dispozícii poskytovateľa *Cloudu*. Z právneho a technického hľadiska totiž poskytovateľ *cloudovej* služby nie je osobou – držiteľom či supervízorom, ktorá by mohla vydať dáta pre potreby orgánov činných v trestnom konaní[282].

Podľa Halasa[283] možno na danú problematiku aplikovať čl. 19 ods. 2 Budapeštianskeho dohovoru[284]. V prvom rade je odkaz na uvedené ustanovenie možné považovať za problematický z hľadiska činnosti OČTK, pretože uvedené ustanovenie zaväzuje najmä legislatívny orgán zmluvného štátu k prijatiu príslušnej právnej úpravy, ktorá však nebola priamo implementovaná. Tiež je potrebné vzniesť námietku najmä voči skutočnosti, že aj v prípade prijatia uvedeného záveru je potrebné uviesť, že je problematické na mieste činnosti OČTK zistiť, či sú dáta uložené práve na území signatára Dohovoru o počítačovej kriminalite. Ak by boli dáta uložené v Rusku, Číne, Indii a pod., akákoľvek extrakcia dát by mohla byť namietaná ako extrateritoriálny zásah zo strany OČTK bez príslušného právneho základu. K postrehu Halasa ohľadne možnosti aplikácie č. 19 ods. 2 Budapeštianskeho dohovoru uvádzame, že uvedený výklad ustanovenia sa neetabloval a problematika *Cloudu* nebola do súčasnosti uspokojivo vyriešená ani na medzinárodnej úrovni.

Ako aplikačne prístupné sa teda javia prostriedky medzinárodnej právnej pomoci (MLA), postupu podľa Budapeštianskeho dohovoru či postupy podľa právnych aktov EÚ (EIO).

Pri problematike cezhraničného získavania údajov by sme však radi priblížili aj asertívny prístup belgických justičných orgánov voči technologickým spoločnostiam v ostro sledovanej súdnej veci tzv. „*Yahoo Case*“[285], v ktorom belgic-

---

[282] V uvedenom prípade by do úvahy pripadal len analogicky § 3 TP prípadne zaisťovacie inštitúty napr. prehliadka iných priestorov a pozemkov podľa § 101 TP. Pri uvedených inštitútoch však je potrebné zdôrazniť ich celkovú aplikačnú nevhodnosť a prevažujúce nedostatky.

[283] *Halas, N.* Dokazovanie počítačovej kriminality. Praha : Leges, 2023, 140 s.

[284] Čl. 19 ods. 2 Budapeštianskeho dohovoru *„Každá strana prijme potrebné legislatívne alebo iné opatrenie na zabezpečenie toho, aby v prípade, keď jej príslušné orgány prehliadajú alebo podobne vstupujú do určeného počítačového systému alebo jeho časti podľa odseku 1 písm. a) a majú dôvody domnievať sa, že hľadané údaje sú uložené v inom počítačovom systéme alebo jeho časti na jej území a že takéto údaje sú zákonne prípustné z pôvodného systému, alebo sú pre tento systém prístupné, tieto organ boli oprávnené urýchlene rozšíriť prehliadku alebo podobný prístup aj na tento iný systém.“*

[285] Uvedený prípad bol justičnými orgánmi Belgicka vedený voči spoločnosti Yahoo Inc. a prebiehal v rokoch 2009 – 2015. Týkal sa povinnosti spoločnosti Yahoo ku skutku z roku

ký prokurátor požadoval dôsledné dodržiavanie zásady *lex loci regit actum*[286], pričom uvedený prístup v určitej miere korešponduje aj s návrhom smernice o vzájomnej prípustnosti dôkazov a elektronických dôkazov v trestných veciach, o ktorom sa zmienime v ďalšej časti.

Otázku *Cloudu* sme otvorili najmä z dôvodu, že v prípade jej neriešenia by vznikla situácia, v ktorej páchatelia trestnej činnosti môžu veľmi jednoducho úmyselne presúvať svoje dáta na *cloudové* platformy v rámci vlastných zariadení a takto ich *de facto* vyčleniť z dosahu OČTK.

Problematiku *Cloudu* sa snaží riešiť aj navrhovateľ v rámci legislatívneho návrhu LP/2025/607, čo považujeme za prínosné. Zlepšenie prístupu ku dátam z *Cloudu* sme priblížili pri § 100 TP.

3. Výskum stavu aplikačnej praxe cezhraničného získavania dôkazov

28 V nasledujúcej časti priblížime výsledky vlastného výskumu vychádzajúceho z dát inštitúcií EÚ[287]. Cieľom uvedeného výskumu bola identifikácia schopností tuzemských OČTK na získavanie cezhraničných údajov v trestnom konaní v porovnaní so zahraničím. Prvá časť spracovaných údajov pochádza z *Pracovného dokumentu*[288]. V rámci prípravnej časti pracovného dokumentu autori pristúpili

---

2007 k vydaniu údajov z emailovej služby vrátane IP adries vo veci nákupov špičkových technológii s falošnými platobnými kartami a to napriek skutočnosti, že spoločnosť Yahoo nemala v Belgicku zastúpenie a ani technické zázemie. Spoločnosť tvrdila, že ako americká spoločnosť nepodlieha belgickej jurisdikcii. S uvedeným tvrdením nesúhlasil prokurátor, ktorý vo svojej pozícií uvádza, že ak spoločnosť podniká na území Belgicka, konkludentne sa podriaďuje aj tamojšej jurisdikcii. Po viac inštančných súdnych rozhodnutiach, belgický kasačný súd v treťom rozhodnutí z 1. 12. 2015 zamietol odvolanie spoločnosti Yahoo Inc. a teda potvrdil, povinnosť spoločnosti podriadiť sa právnemu poriadku, ak na území vykonáva podnikateľskú činnosť. Rozhodnutie Nr.P.13.2082.N. Dostupné na: https://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiN49icqqyMAxUw8bsIHQfiKMwQFnoECDIQAQ&url=https%3A%2F%2Fjournals.sas.ac.uk%2Fdeeslr%2Farticle%2FviewFile%2F2310%2F2261&usg=AOvVaw2icTqs4IoZwvx3dkArNAPz&opi=89978449 (citované 2025-04-25).

[286] V zmysle čl. 3 písm. d) návrhu smernice o vzájomnom uznávaní dôkazov a elektronických dôkazov v trestnom konaní: *„lex loci znamená právo miesta, kde boli zhromaždené dôkazy. Ak toto miesto nie je známe, za lex loci sa považuje právo miesta, kde bol poskytnutý prístup k dôkazom"*.

[287] *Srholec, M.* OČTK pri cezhraničnom prístupe k elektronickým dôkazom. In: Banskobystrické zámocké dni práva. Vígľaš : Univerzita Mateja Bela, 2023, s. 257 – 269. Dostupné na: https://www.prf.umb.sk/veda-a-vyskum/konferencne-on-line-vystupy/vi-banskobystricke-zamocke-dni-prava/ (citované 2025-04-25).

[288] Commission Staff Working Document Impact Assessment. 2018. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Dostupné na: https://eur-lex