COMENIUS: ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLV
2/2026

NÁSTIN PRINCÍPOV PRE ANALÝZU OTVORENÝCH ZDROJOV (OSINT) AKO DÔKAZU V TRESTNOM KONANÍ[1]

doc. JUDr. Marek Kordík, LL.M., PhD., univ. prof.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra Trestného práva, kriminológie a kriminalistiky
marek.kordik@flaw.uniba.sk

Nástin princípov pre analýzu otvorených zdrojov (OSINT) ako dôkazu v trestnom konaní

Článok sa zaoberá možnosťou využitia analýzy otvorených zdrojov ako dôkazu v trestnom konaní a snaží sa vymedziť minimálne štandardy na jeho použitie, tak aby boli naplnené požiadavky Trestného poriadku tak v pozitívnom zmysle princípov ako i princípov vymedzených negatívne. Príspevok sa v svojom texte snaží vysporiadať i s používanou terminológiou v tejto oblasti. Z tohto pohľadu taktiež analyzuje pripravovanú úpravu zmeny zaisťovania elektronických dôkazov, ktorá však z tohto pohľadu neprináša žiadnu relevantnú zmenu. Príspevok taktiež pri svojej argumentácií čerpá z rozhodovacej činnosti Medzinárodného súdneho dvora a poskytuje výklad noriem Budapeštianskeho dohovoru pre možnosť zdieľania OSINT analýzy, ako jedného zo základných prameňov pre zdieľanie digitálnych dôkazov v Európe.

Outline of Principles for the Analysis of Open-Source Intelligence (OSINT) as Evidence in Criminal Proceedings

This article examines the possibility of using open-source analysis as evidence in criminal proceedings and seeks to define minimum standards for its use, so that the requirements of the Criminal Procedure Code are met both in terms of positive principles and those defined negatively. The article also seeks to address the terminology used in this field. From this perspective, it analyzes the proposed amendment

[1] Článok je podporený Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 09-I05-03-V02-00079.

regarding the seizure of electronic evidence, which, however, does not introduce any relevant changes in this regard. In its argumentation, the paper also draws on the case law of the International Court of Justice and provides an interpretation of the provisions of the Budapest Convention regarding the possibility of sharing OSINT analysis as one of the fundamental sources for the sharing of digital evidence in Europe.

Kľúčové slová: dôkaz, vyšetrovanie, OSINT, otvorené zdroje, princípy

Keywords: evidence, investigation, OSINT, open sources, principles

https://doi.org/10.46282/afi.2026.2.01

Úvod

Rozvoj prostredia informačno-komunikačných technológií zásadným spôsobom mení povahu informácií využiteľných v trestnom konaní. Významná časť poznatkov relevantných pre odhaľovanie, vyšetrovanie a dokazovanie trestnej činnosti sa dnes nachádza v digitálnom priestore, pričom nie vždy ide o údaje získavané prostredníctvom tradičných procesných nástrojov. Osobitnú pozornosť si v tomto kontexte zasluhujú informácie pochádzajúce z otvorených zdrojov, označované ako OSINT, ktoré môžu pri splnení zákonných a metodických požiadaviek nadobudnúť význam aj v rovine dokazovania v trestnom konaní. Cieľom článku je vymedziť základné právne a metodické predpoklady využitia analýzy otvorených zdrojov v trestnom konaní, najmä z hľadiska jej prípustnosti, dôkaznej použiteľnosti a súladu so zásadami trestného procesu. Osobitná pozornosť je venovaná odlíšeniu otvorených zdrojov od informácií získaných spôsobom, ktorý by už predstavoval neoprávnený prístup, infiltráciu alebo inú formu zásahu do chráneného informačného priestoru. Článok sa zároveň usiluje pomenovať minimálne štandardy, ktoré by mali byť pri získavaní, uchovávaní, dokumentovaní a vyhodnocovaní OSINT informácií rešpektované. Spracovanie tejto témy má význam nielen z hľadiska aplikačnej praxe orgánov činných v trestnom konaní a súdov, ale aj z pohľadu širšej odbornej diskusie o povahe elektronických dôkazov. Slovenský právny poriadok totiž OSINT výslovne neupravuje ako samostatný procesný inštitút, čo vyvoláva potrebu hľadať jeho miesto v rámci existujúcich pravidiel dokazovania, medzinárodnej justičnej spolupráce a štandardov práce s digitálnymi stopami. Prínos článku

spočíva najmä v systematizácii princípov, ktoré môžu slúžiť ako interpretačný rámec pre zákonné, transparentné a preskúmateľné využívanie otvorených zdrojov v trestnom konaní.

1 Pojem

Dokazovanie tvorí zákonom upravený postup subjektov trestného konania (orgánov činných v trestnom konaní, súdu, obvineného, poškodeného, zúčastnenej osoby atď.), ktorého účelom je vyhľadať, zabezpečiť, vykonávať a zhodnotiť informácie dôležité pre trestné stíhanie.[2] Vzhľadom na absenciu[3] ustanovení, ktoré by sa venovali téme OSINT, je potrebné uviesť niekoľko systémových poznámok k postupu a minimálnym štandardom aby bola OSINT analýza prípustná ako dôkaz. *Pojem OSINT* je skratkou anglického *open source inteligence*, ktorý možno preložiť ako *spravodajstvo otvorených zdrojov* alebo *analýza*

[2] ČENTÉŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín : Heuréka, 2016, s. 328.

[3] Tento stav sa nemení ani pripravovanou reformou zaisťovania elektronických dôkazov v trestnom konaní, ktorá je aktuálne v legislatívnom procese v NR SR. K tomu pozri čl. II vládneho návrhu zákona o niektorých opatreniach súvisiacich s prijatím zákona o medzinárodnej justičnej spolupráci v trestných veciach a o zmene a doplnení niektorých zákonov. Dostupné dňa 20.05.2026 na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=586182. Samotná pripravovaná novela sa dotýka, z pohľadu zamerania článku iba uchovávania a zaisťovania počítačových údajov, zariadení a nosičov v trestnom konaní, pre účely dokazovania, pritom nanovo sa definujú počítačové údaje, nosiče, údaje o používateľovi, kto sa rozumie poskytovateľom služieb a pod. Novela prináša zásadnú zmenu v získavaní rôznych kategórií počítačových údajov. Stanovuje sa povinnosť (všeobecná edičná povinnosť) vydať počítačový údaj, nosič, alebo počítačový systém, avšak len ak nepostačuje vyhotovenie kópie na výzvu policajta, prokurátora, alebo predsedu senátu podľa navrhovaného § 89b Tr. por.- analogicky *lex specialis* k vydaniu veci. Odňatie počítačového údaju, nosiča, alebo počítačového systému bude v zmysle navrhovaného znenia § 91 Tr. por. na príkaz sudcu pre prípravné konanie, alebo predsedu senátu, ak nebolo vydanie veci úspešné a nepostačuje vyhotovenie kópii. Uložené údaje o používateľoch, kontách sa budú získavať na príkaz policajta so súhlasom prokurátora, prokurátora alebo predsedu senátu v zmysle navrhovaného § 116a ods. 3 písm. a) Tr. por. od poskytovateľa služieb. Uložené prevádzkové a lokalizačné údaje sa budú získavať na príkaz sudcu pre prípravné konanie, alebo predsedu senátu podľa navrhovaného § 116a ods. 3 písm. b) Tr. por. od poskytovateľa služieb. Uložené obsahové údaje sa budú získavať na príkaz sudcu pre prípravné konanie alebo predsedu senátu od poskytovateľa služieb podľa navrhovanej právnej úpravy podľa nového § 116a ods. 3 písm. b) Tr. por. Sledovanie prevádzkových a lokalizačných údajov bude možné len na príkaz sudcu pre prípravné konanie alebo predsedom senátu podľa § 115a Tr. por. (v zásade ide o doterajšiu právnu úpravu). Sledovanie obsahu – odpočúvanie zostava čo do podmienok nezmenené, rozširuje sa iba zoznam sa okruh trestných činov podľa novo koncipovaného § 115 Tr. por.

otvorených zdrojov[4]*, alebo otvorené vyšetrovanie*[5]. uvádzajú, že pojem spravodajstva otvorených zdrojov je užším pojmom a podmnožinou najširšieho pojmu informácia z otvorených zdrojov, nakoľko už predstavuje určitý špecifický postup identifikácie, získania a interpretácie *informácie z otvorených zdrojov.*[6] Pričom práve pojem informácie z otvorených zdrojov vhodne vystihuje podstatu a kľúčové aspekty tejto problematiky a súčasne predstavuje nepochybne pojem širší. Všetky pojmy sa používajú *promiscue* a v praxi nespôsobuje táto rozšírená definícia problém. Je však pravdou, že využívanie analýzy otvorených zdrojov pre získanie elektronických dôkazov v slovenskom trestnom stíhaní je pramalé až zanedbateľné. Možno i tento článok prispeje k širšiemu využívaniu OSINT analýzy v praxi trestného stíhania.[7] Jeho pojmovou súčasťou a základnou podmienkou je skutočnosť, že musí ísť výlučne o dostupné zdroje, ktoré sú prístupne neohraničenému počtu osôb priamo alebo na požiadanie.

V rámci vymedzenia pojmu informácia z otvorených zdrojov *je vhodné vyhýbať sa* spájaniu týchto druhov informácií *s atribútom verejnosti*, čo môže zvádzať k interpretácií, že ide výlučne iba o verejné a hromadne prístupné informácie, čo nezodpovedá pravde, čo bude analyzované ďalej.

2 Právny rámec OSINT – od vytvorenia po zdieľanie

Keďže analýzy OSINT predstavujú otvorené vyšetrovanie, v zásade ich možno vykonávať bez akéhokoľvek predchádzajúceho súhlasu alebo príkazu justičného orgánu. Je však možné konštatovať, že vykonané analýzy OSINT môžu byť na základe žiadosti predmetom záujmu

[4] Dostupné dňa 22.05.2026 na: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence alebo NATO príručka pre OSINT, Executive summary. Dostupné dňa 20.05.2026 na: https://archive.org/stream/NATOOSINTHandbookV1.2/NATO OSINT Handbook v1.2 - Jan 2002_djvu.txt

[5] Berkeley Protocol on Digital Open Source Investigations. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 13. Dostupné dňa 20.05.2025 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[6] Open Source Evidence and the International Criminal Court, By / April 15, 2019 By Nikita Mehandra and Alexa Koenig, dostupné dňa 26.5.2026 na: https://journals.law.harvard.edu/hrj/2019/04/open-source-evidence-and-the-international-criminal-court/ - _ftn29

[7] Pozn. autora, článok sa nevenuje využívaniu OSINT analýzy pre spravodajské účely.

justičných orgánov iného (tretieho) štátu alebo členského štátu EÚ vo vlastnom trestnom stíhaní.

Medzinárodné právo poskytuje viacero nástrojov na vykonávanie analýz OSINT v trestnom konaní, a to tak v medzinárodnom konaní, ktoré vedie Úrad prokurátora Medzinárodného trestného súdu (ICC), ako aj vo vnútroštátnych vyšetrovaniach, ktoré vedú vnútroštátne orgány. Pokiaľ ide o prvý prípad, primárna pozornosť by sa mala zamerať na dokument *Rules of Procedure and Evidence of the ICC*[8] pri získavaní dôkazov prostredníctvom analýz OSINT o medzinárodných zločinoch, najmä čl. 19 a) a b) dokumentu *Rules of Procedure and Evidence*, ktoré stanovujú možnosť, aby Sekretariát Medzinárodného trestného súdu[9] (ďalej len „Sekretariát“) mal/vybudoval odborné kapacity s odborníkmi s cieľom podporiť procesné postavenie obete alebo svedkov v konaniach vedených pred ICC alebo pri prijímaní ochranných opatrení[10] alebo podporiť Sekretariát v právnych a administratívnych záležitostiach, vrátane oblastí humanitárneho a trestného práva[11], *mutatis mutandis* pre Úrad prokurátora ICC.[12] Na základe článku 93 Rímskeho štatútu môže súd v spolupráci so zmluvným štátom požiadať o odborný posudok[13] alebo uľahčiť dobrovoľnú účasť expertov v konaniach pred ICC.[14] Medzi tieto postupy možno podľa autora zaradiť i vykonávanie OSINT analýz, ktoré boli použité aj zo strany Medzinárodného trestného súdu v jednotlivých konaniach resp. rozhodnutiach.[15]

Pokiaľ ide o medzinárodnú spoluprácu v trestných veciach s tretími štátmi, ako aj o spoluprácu založenú na vzájomnom uznávaní medzi členskými štátmi EÚ, možno využiť viacero nástrojov.

---

[8] Článok 51 Oznámenie MZV SR č. 333/2002 Z. z. o podpísaní štatútu Medzinárodného trestného súdu. Rímsky štatút (ďalej len „*Rímsky štatút*“).

[9] *ICC Registry,* pozn. autora. Čl. 43 Rímskeho štatútu.

[10] Čl. 19, písm.a) dokumentu *Rules of Procedure and Evidence.* Dostupné dňa 22.05.2026 na: https://www.icc-cpi.int/publications/core-legal-texts/rules-procedure-and-evidence

[11] Čl. 19, písm.b) dokumentu *Rules of Procedure and Evidence.* Dostupné dňa 22.05.2026 na: https://www.icc-cpi.int/publications/core-legal-texts/rules-procedure-and-evidence

[12] ICC, Office of the Prosecutor, DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE, 6.3 2025, str. 26-28. Dostupné dňa 22.05.2026 na: https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf

[13] Článok 93.1, písm. b) Rímskeho štatútu.

[14] Článok 93.1, písm. e) Rímskeho štatútu.

[15] Prokurátor v. Al-Werfalli, ICC-01/11-01/17, Príkaz na zatknutie (Aug. 15, 2017), alebo prípad „Prokurátor v. Thomas Lubanga Dyilo“ Technický protokol pre poskytnutie dôkazov, materiálov a informácií o svedkoch a obetiach v elektronickej forme pre účely ich vykonania pred súdom (pozn. preklad autora), dostupné dňa 25.05.2026 na: https://www.icc-cpi.int/sites/default/files/RelatedRecords/CR2008_01599.PDF, alebo Prokurátor v. Bemba, ICC-01/05-01/08, Rozsudok podľa čl. 74 Rímskeho štatútu (Mar. 21, 2016), para 531, 616, 619.

Dohovor Organizácie Spojených národov proti počítačovej kriminalite[16], ktorý bol otvorený na podpis, poskytuje podľa článku 44 možnosť zdieľať analýzy OSINT prostredníctvom medzinárodnej justičnej spolupráce, ktorá už bola vytvorená, keďže umožňuje zverejňovať elektronické údaje uložené prostredníctvom systému informačných a komunikačných technológií umiestneného na území požiadaného zmluvného štátu.

Dohovor Rady Európy o počítačovej kriminalite (Budapeštiansky dohovor)[17] umožňuje zmluvným stranám v súlade s článkom 26 (spontánne poskytnutie) v rámci svojho vnútroštátneho práva a bez predchádzajúcej žiadosti poskytnúť inej zmluvnej strane informácie získané v rámci vnútroštátneho konania, ak sa domnievajú, že poskytnutie týchto informácií by mohlo pomôcť prijímajúcej zmluvnej strane, alebo prostredníctvom nástroja medzinárodnej spolupráce v trestných veciach stanoveného v článku 31 Budapeštianskeho dohovoru. S poukazom na článok 26 ods. 2 Budapeštianskeho dohovoru možno za určitých okolností poskytnúť inej zmluvnej strane spontánne informácie len vtedy, ak citlivé informácie zostanú utajené alebo ak bude možné stanoviť ďalšie podmienky týkajúce sa využívania týchto informácií,[18] ak by zverejnenie informácií mohlo ohroziť dôležité záujmy poskytujúceho štátu. Ak však prijímajúca strana s podmienkou súhlasí, musí ju dodržať. Predpokladá sa, že takto stanovené podmienky budú v súlade s podmienkami, ktoré by mohla stanoviť poskytujúca strana na základe žiadosti o vzájomnú pomoc zo strany prijímajúcej strany.[19]

Európske právo[20] poskytuje možnosť zdieľať dôkazy, ktoré už boli získané a sú v držbe orgánu členského štátu EÚ[21], v rámci európskeho vyšetrovacieho príkazu, oddiel H3.[22] Z hľadiska ochrany osobných

[16] Dostupné dňa 22.05.2026 na: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

[17] Oznámenie MZV SR č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite.

[18] Bod 261 Dôvodovej správy k Dohovoru o počítačovej kriminalite. Dostupné dňa 23.05.2026 na: https://rm.coe.int/16800cce5b

[19] Tamtiež.

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

[21] Rozsudok Súdneho dvora Európskej únie, C-670/22 ENCROCHAT, para: 132.2.

[22] V súčasnosti nevidíme možnosť získať prístup k analýzam OSINT vypracovaným vyšetrovacími alebo justičnými orgánmi iných členských štátov EÚ prostredníctvom európskeho príkazu na predloženie dôkazov alebo európskeho príkazu na zabezpečenie dôkazov podľa Nariadenia (EÚ) 2023/1543 Európskeho parlamentu a Rady z 12. júla 2023 o európskych príkazoch na predloženie dôkazov a európskych príkazoch na uchovanie dôkazov v trestnom konaní a na výkon trestov odňatia slobody po trestnom konaní, keďže obe

údajov sa zhromažďovanie a spracúvanie údajov v analýzach OSINT vyšetrovacími a justičnými orgánmi riadi článkami 4 a 8 Policajnej smernice.[23]

Okrem toho, v rámci jurisdikcie členských štátov EÚ, je taktiež advokát oprávnený získavať dôkazy vrátane OSINT[24], zvyčajne prostredníctvom tretej odborne zdatnej osoby. Domnievame sa, že analýzy OSINT vykonané a predložené obeťou alebo podozrivým v trestnom konaní spadajú pod výnimku GDPR[25], ak sú vykonané riadnym spôsobom, tak ako je uvedené ďalej. Tento postup je možne vidieť i v iných právnych poriadkoch.[26]

Napriek tomu stojí za zmienku aj využitie analýz OSINT mimo rámca trestného konania. Využitie analýz OSINT v týchto postupoch zvyčajne upravujú zákonníky práce pri nástupe nových kľúčových zamestnancov alebo ako súčasť kybernetickej obrany, ktorá má pôvod v NIS 2[27] alebo DORA[28].

sú adresované poskytovateľom služieb alebo ich zákonným zástupcom, ako je stanovené v článkoch 3.1 až 3.3.

[23] 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.

[24] Smernica Európskeho parlamentu a Rady (EÚ) 2016/343 z 9. marca 2016 o posilnení určitých aspektov prezumpcie neviny a práva byť prítomný na konaní pred súdom v trestnom konaní.

[25] Čl. 6.1, písm. d) a f) Nariadenia 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).

[26] UK Data Protection Act (2018). Dostupné dňa 22.05.2026 na: https://www.legislation.gov.uk/ukpga/2018/12/contents
UK GDPR. Dostupné dňa 22.05.2026 na: https://www.legislation.gov.uk/eur/2016/679/contents
US Electronic Communications Privacy Act (1986). Dostupné dňa 20.05.2026 na: https://www.congress.gov/bill/99th-congress/house-bill/4952
Canadian Personal Information Protection and Electronic Documents Act. Dostupné dňa 20.05.2026 na: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
Australian privacy act. Dostupné dňa 20.05.2026 na: https://www.legislation.gov.au/C2004A03712/asmade/text

[27] Napr. čl. 21, ods. 1 až ods. 3 Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

[28] Napr. čl. 27 ods. 7 Nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

3 Kategorizácia informácií

Analýza otvorených zdrojov v zásade pracuje s štyrmi rôznymi kategóriami informácií:[29]

- verejne ľahko dostupné,
- verejne ťažko dostupné,
- verejne dostupné na požiadanie a
- uzavreté – chránené alebo utajené.

Ide teda o využívanie voľne dostupných informačných kanálov, ktoré sú verejnosti prístupné bez poplatku alebo môžu byť prístupné za poplatok. Nesmú však byť chránené, alebo dokonca utajené. Do poslednej kategórie spadajú i súkromné alebo polosúkromné digitálne informácie ako obrázky, alebo videá, ktoré sú sprístupňované alebo posielané iba členom uzavretej skupiny, alebo pozvaným/ schváleným účastníkom.[30]

Vo väčšine právnych poriadkov a organizácií sa digitálne dôkazy riadia tromi základnými princípmi: relevantnosťou[31], spoľahlivosťou[32] a dostatočnosťou[33]. Vzhľadom na chýbajúce jednotné normy a definície je možné sa riadiť technickými normami a usmerneniami stanovenými v norme ISO 27037 – Usmernenia pre identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov[34], keďže kľúčovými zložkami, ktoré zabezpečujú dôveryhodnosť vyšetrovania, sú metodiky uplatňované počas procesu[35], bez zameriavania sa na konkrétne nástroje alebo metódy.

[29] OPEN SOURCE INVESTIGATIONS IN THE AGE OF GOOGLE / editors, Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology, 2059-1063; Vol. 4, s. 47.

[30] Open Source Evidence and the International Criminal Court, By / April 15, 2019 By Nikita Mehandra and Alexa Koenig. Dostupné dňa 20.05.2026 na: https://journals.law.harvard.edu/hrj/2019/04/open-source-evidence-and-the-international-criminal-court/ - _ftn29

[31] Relevantnosťou sa rozumie údaj o hodnote informácie pre vyšetrovanie a ktorá predstavuje dôvod na jej získanie, ako je stanovené v norme ISO-EIC 27037, s. 6.

[32] Atribút konzistentného výsledku a očakáva teľných postupov ISO EIC 27037, Pojmy a definície, 3.15.

[33] Informácie odôvodňujúce záver, že bolo zhromaždené také množstvo materiálu na vykonanie riadneho (otvoreného) vyšetrovania OSINT s odôvodnenými závermi. ISO-EIC 27037, s. 6.

[34] Publikované v 2012.

[35] ISO EIC 27037.

4 Princípy získavania informácií prostredníctvom OSINT

Pri získavaní elektronických dôkazov prostredníctvom OSINT musia byť dodržané určité negatívne ale i pozitívne princípy. Medzi negatívne princípy patrí:

- *Princíp zákazu prekonania odporu* – informácia z otvorených zdrojov nesmie byť získaná prostredníctvom neoprávneného prístupu, alebo porušením bezpečnostných opatrení napr. využitím získaných prihlasovacích údajov bez súhlasu dotknutej osoby.[36] Jednak by išlo trestný čin neoprávneného zásahu do počítačového systému podľa § 247a Tr. zák., ale taktiež je takýto postup neakceptovateľný aj podľa medzinárodných štandardov podľa čl. 2[37] alebo čl. 5[38] Dohovoru o počítačovej kriminalite resp. európskeho práva.[39]
- *Princíp zákazu infiltrácie do uzavretých skupín* – tak ako už bolo naznačené vyššie ide o informácie, ktoré sa šíria alebo tvoria v uzavretom okruhu osôb a pôvodca, resp. šíriteľ má záujem, aby tieto informácie boli zdieľane iba v uzavretom okruhu[40] týchto osôb. Prirodzeným dôsledkom je, že ak je zástupca zložky vynucujúcej právo v takejto uzavretej skupine prítomný, tak je to pod úplnou alebo čiastočnou legendou a takáto osoba už zbiera informácie o páchanej trestnej činnosti utajovaným spôsobom[41] a napĺňa procesné znaky agenta podľa § 117 Tr. por. čím sa tento postup diametrálne líši od analýzy otvorených zdrojov bez zákonom stanovenej regulácie. Možno konštatovať, že tento postup sa aplikuje i na viac početné skupiny (rádovo i v stovkách členov), ktoré už spĺňajú definíciu verejnosti podľa zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.[42] I z tohto dôvodu je vhodné nehovoriť v súvislosti s OSINT o *„verejnosti“* ale *„otvorenosti“* zdrojov informácií, pretože sa tým vystihuje podstata postupu, ktorým sa hľadajú, identifikujú,

[36] Bod 45 Dôvodovej správy k Dohovoru o počítačovej kriminalite. Dostupné dňa 20.05.2026 na: https://rm.coe.int/16800cce5b

[37] Body 44 a 45. Tamtiež

[38] Body 65 a 68. Tamtiež.

[39] Čl. 5, písm. f) Všeobecného nariadenia o ochrane osobných údajov.

[40] Pozvaných, schválených alebo odsúhlasených účastníkov.

[41] § 117 ods. 3, 4 a 10 Tr. por.

[42] Podľa § 122 ods. 2 Tr. zák. trestný čin je spáchaný verejne ak je *spáchaný obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom, alebo pred viac ako dvoma súčasne prítomnými osobami*.

získavajú a hodnotia dostupné informácie bez obmedzenia vyplývajúceho z charakteru právom chránenej informácie.

Medzi pozitívne princípy možno zaradiť:

- *Princíp nevyhnutnosti* – rozsah získavaných informácií môže byť vymedzený časovo (relevantný interval skúmania), alebo osobne a je rámcovaný získaním dôležitých informácií pre trestné konanie v nevyhnutnom rozsahu na dosiahnutie účelu analýzy.[43]
- *Princíp identifikácie* – uvádzanie presných údajov a záznamov o využití zdroja informácie ako i identifikácia osoby, ktorá tento zdroj využila.[44]
- *Princíp objektivity a absencie konfliktu záujmov*[45] – tak ako pri akomkoľvek inom vyhľadávaní dôkazov, osoba vyhľadávajúca a hodnotiaca dôkazy získané metódou OSINT (tzv. OSINT dôkazy), musí k týmto pristupovať bez zaujatosti a objektívne, bez konfliktu záujmov.[46]
- *Princíp podpornej funkcie* – OSINT analýza spravidla poskytuje kontextové informácie k predmetu analýzy, menej priame usvedčujúce alebo oslobodzujúce dôkazy.[47] V prípade, že ide

[43] BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 13. Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source K tomu porovnaj aj ISO 27037.

[44] OPEN SOURCE INVESTIGATIONS IN THE AGE OF GOOGLE / editors, Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology, 2059-1063; Vol. 4, s. 47.

[45] BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 12 – 15. Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[46] BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 12 – 15. Dostupné Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[47] BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN

o priame usvedčujúce alebo oslobodzujúce dôkazy (napr. detská pornografia, extrémistické video, video z vojenskej operácie, ktoré preukazuje vojnové zločiny apod.) súčasťou otvoreného vyšetrovania musia byť i štandardy akvizície príslušnej informácie z otvoreného zdroja.

– *Princíp bezpečnosti OSINT postupov* – ide napr. o nesprístupnia informácie o ich pripojení, nesprístupnia informácie o vlastnom zariadení, nesprístupnia informácie o ich identite a pod.[48]

Analýza a závery otvoreného vyšetrovania, ktoré je vykonané hore naznačeným, môžu byť v trestnom stíhaní využité prostredníctvom dôkazného prostriedku,[49] a to najmä (i) ústneho výsluchu osoby podľa § 133 Tr. por., alebo prostredníctvom videokonferencie podľa § 61b Tr. por, pri výsluchu je možné použiť i vizualizácie OSINT analýzy formou poznámok, (ii) písomne prostredníctvom odborného vyjadrenia podľa § 141 Tr. por., pričom súčasťou písomného odborného vyjadrenie môžu byť i vizualizácia výsledkov a postupov pri tvorbe OSINT analýzy, doplnený o prípadný výsluch osoby, ako aj (iii) čítaním listiny, ktorou bude samotná analýza a interpretácia.

Záver

Analýza otvorených zdrojov predstavuje v trestnom konaní osobitný spôsob získavania a vyhodnocovania informácií, ktorý môže za splnenia zákonných podmienok a požiadavky transparentnosti či overiteľnosti nadobudnúť dôkazný význam. Hoci slovenský právny poriadok OSINT výslovne neupravuje ako samostatný procesný inštitút, jeho využitie nemožno vylúčiť, ak je zachované rozlíšenie medzi informáciami dostupnými z otvorených zdrojov a informáciami, ktorých získanie by vyžadovalo prekonanie technickej, právnej alebo faktickej bariéry. Práve toto rozlíšenie je rozhodujúce pre zákonnosť postupu

Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 15. Dostupné Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[48] BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. *A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 39 – 41. Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[49] ANDRAŠKO, J., DRAŽOVÁ, P., KORDÍK, M., MESARČÍK, M., RAMPÁŠEK, M. a kol. *Regulácia kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality*. 1. vyd. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta UK, 2026, 638 s.

a použiteľnosť výsledkov OSINT analýzy v trestnom konaní. Pojem OSINT nemožno zužovať iba na verejne a hromadne dostupné informácie, keďže je vhodnejšie hovoriť o „otvorených zdrojoch“. OSINT analýzu je preto potrebné odlíšiť od infiltrácie, utajeného pôsobenia alebo neoprávneného prístupu do počítačových systémov, keďže takéto postupy podliehajú osobitnému právnemu režimu a nemožno ich považovať za otvorené vyšetrovanie. Minimálny rámec prípustnosti dôkazu OSINT v trestnom konaní je determinovaný dodržaním negatívnych a pozitívnych princípov. OSINT analýza má v trestnom konaní spravidla podpornú a kontextovú funkciu, pretože môže prispievať k objasneniu skutkového stavu, identifikácii súvislostí, overeniu iných dôkazov alebo k vytvoreniu analytického podkladu pre ďalšie dokazovanie. Možno teda uzavrieť, že OSINT analýza môže byť v trestnom konaní využiteľná ako dôkaz, ak okrem zásad trestného konania rešpektuje požiadavky kladené na prípustnosť elektronických dôkazov. Jeho dôkazná hodnota preto závisí nielen od obsahu získanej informácie, ale aj od kvality postupu jej identifikácie, získania, uchovania a vyhodnotenia. Preto je potrebné formulovať minimálne štandardy práce s OSINT, ktoré umožnia vnímať otvorené zdroje nielen ako operatívny nástroj, ale aj ako legitímny a procesne použiteľný zdroj poznania v dokazovaní v trestnom konaní.

Použité zdroje

1. ANDRAŠKO, J., DRAŽOVÁ, P., KORDÍK, M., MESARČÍK, M., RAMPÁŠEK, M. a kol. *Regulácia kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality*. 1. vyd. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta UK, 2026, 638 s.
2. AUSTRALIAN PRIVACY ACT. Dostupné dňa 20.05.2026 na: https://www.legislation.gov.au/C2004A03712/asmade/text
3. BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3. Dostupné dňa 20.05.2026 na: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source
4. Canadian Personal Information Protection and Electronic Documents Act. Dostupné dňa 20.05.2026 na: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

5. ČENTÉŠ, J. a kol.: *Trestné právo procesné. Všeobecná časť.* Šamorín : Heuréka, 2016.
6. ICC, Office of the Prosecutor, DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE. Dostupné dňa 22.05.2026 na: https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf
7. ISO EIC 27037.
8. ISO EIC 27042.
9. 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).
10. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.
11. Nariadenie (EÚ) 2023/1543 Európskeho parlamentu a Rady z 12. júla 2023 o európskych príkazoch na predloženie dôkazov a európskych príkazoch na uchovanie dôkazov v trestnom konaní a na výkon trestov odňatia slobody po trestnom konaní.
12. OPEN SOURCE INVESTIGATIONS IN THE AGE OF GOOGLE / editors, Henrietta Wilson, SOAS University of London, UK & King's College London, UK,Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK.Description: New Jersey : World Scientific, [2024] | Series: Security science and technology, 2059-1063; Vol. 4.
13. OPEN SOURCE EVIDENCE AND THE INTERNATIONAL CRIMINAL COURT. By / April 15, 2019 By Nikita Mehandra and Alexa Koenig. Dostupné dňa 26.05.2026 na:https://journals.law.harvard.edu/hrj/2019/04/open-source-evidence-and-the-international-criminal-court/ - _ftn29
14. Oznámenie MZV SR č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite.
15. Oznámenie MZV SR č. 333/2002 Z. z. o podpísaní štatútu Medzinárodného trestného súdu. Rímsky štatút.
16. Prokurátor v. Al-Werfalli, ICC-01/11-01/17, Príkaz na zatknutie (Aug. 15, 2017).
17. Prokurátor v. Thomas Lubanga Dyilo. Technický protokol pre poskytnutie dôkazov, materiálov a informácií o svedkoch a obetiach v elektronickej forme pre účely ich vykonania pred súdom (pozn. preklad autora). Dostupné dňa 25.05.2026 na: https://www.icc-cpi.int/sites/default/files/RelatedRecords/CR2008_01599.PDF

18. Prokurátor v. Bemba, ICC-01/05-01/08, Rozsudok podľa čl. 74 Rímskeho štatútu (Mar. 21, 2016).
19. Rozsudok Súdneho dvora EÚ vo veci C-670/22 ENCROCHAT.
20. RULES OF PROCEDURE AND EVIDENCE OF THE ICC. Dostupné dňa 22.05.2026 na: https://www.icc-cpi.int/publications/core-legal-texts/rules-procedure-and-evidence
21. Smernica Európskeho parlamentu a rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).
22. Smernica Európskeho parlamentu a Rady (EÚ) 2016/343 z 9. marca 2016 o posilnení určitých aspektov prezumpcie neviny a práva byť prítomný na konaní pred súdom v trestnom konaní.
23. 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.
24. Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.
25. UK Data Protection Act (2018). Dostupné dňa 22.05.2026 na: https://www.legislation.gov.uk/ukpga/2018/12/contents
26. UK GDPR. Dostupné dňa 22.05.2026 na: https://www.legislation.gov.uk/eur/2016/679/contents
27. US Electronic Communications Privacy Act of 1986. Dostupné dňa 20.05.2026 na: https://www.congress.gov/bill/99th-congress/house-bill/4952
28. Vládny návrh zákona o niektorých opatreniach súvisiacich s prijatím zákona o medzinárodnej justičnej spolupráci v trestných veciach a o zmene a doplnení niektorých zákonov.
29. Dôvodová správa k Dohovoru o počítačovej kriminalite. Dostupné dňa 23.05.2026 na: https://rm.coe.int/16800cce5b
30. Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.
31. Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.