866—880

Digitálne dôkazy v medzinárodnom trestnom práve

Michal Klenka*

Abstrakt: Článok sa venuje digitálnym dôkazom, ktoré začínajú prevládať, čo predstavuje nielen právne výzvy pre medzinárodné trestné súdnictvo. Cieľom predmetného článku je analyzovať existujúci právny rámec upravujúci dôkazy v medzinárodnom trestnom práve v kontexte použitia digitálnych dôkazov. Východiskom je primárne právna úprava Medzinárodného trestného súdu, ale neopomenuli sme ani ostatné medzinárodné trestné tribunály. Článok sa nielenže venuje samotnej definícii pojmu „digitálny dôkaz", ale zaoberá sa aj pravidlami prípustnosti a vylúčenia dôkazov pred Medzinárodným trestným súdom (hlavne čl. 69 ods. 4 a ods. 7 Rímskeho štatútu), ako aj otázkami relevantnosti a prípustnosti dôkazov vo všeobecnosti. Rovnako predmetom skúmania je aj autentifikácia a spoľahlivosť digitálneho dôkazu, jeho dôkazná hodnota, a v neposlednom rade systém kontroly pôvodu digitálnych dôkazov. V závere nechýbajú ani určité úvahy o budúcnosti využívania digitálnych dôkazov a možným rizík, ktoré ich pripustenie a použitie v konaní pred súdom prináša.

Kľúčové slová: digitálny dôkaz, medzinárodné trestné právo, prípustnosť a vylúčenie dôkazov, autentifikácia digitálneho dôkazu, spoľahlivosť digitálneho dôkazu, systém kontroly pôvodu digitálneho dôkazu

Úvod

Vzhľadom na osobitnú povahu medzinárodných trestných konaní a jedinečné dôkazné výzvy, ktoré predstavujú, by nemalo byť prekvapením, že sa vyvinul unikátny systém na riadenie nakladania s dôkazmi na medzinárodných trestných súdoch. Vyšetrovanie vojnových zločinov je náročné a nebezpečné, nakoľko môže byť vyšetrovateľom zakázané zhromažďovať dôkazy z dôvodu prebiehajúceho násilia alebo nemožnosti prístupu na miesto činu. Rovnako aj fakt, že medzinárodné trestné tribunály trestne stíhajú mocných jednotlivcov vrátane hláv štátov a vedúcich predstaviteľov ozbrojených síl, ktorých osobné zdroje môžu výrazne prekročiť ročný prevádzkový rozpočet vyšetrovacieho tribunálu. Ďalším dôvodom je často aj skutočnosť, že svedkovia môžu váhať s vystúpením a častokrát majú strach z odplaty voči nim alebo ich rodinám. Nie je ani prekvapujúce, keď svedkovia obžaloby odvolávajú svoje výpovede alebo odmietajú vypovedať, nakoľko môžu skončiť nezvestní alebo zabití. Na súde, rovnako ako vo vojne, znášajú riziká svedkovia. Zatiaľ čo súd platí finančné náklady na vyšetrovanie, svedkovia nasadili svoje životy. Žiadna iná forma dôkazu nie je taká hodnotná. Napriek týmto prekážkam môžu vyšetrovatelia často získať dôkazy z radu digitálnych zariadení, vrátane pevných diskov počítača, mobilných telefónov, fotografií a videí, ako aj z informácií zverejnených na internete. Takéto digitálne informácie môžu odhaliť vzorce organizovaného násilia a v niektorých prípadoch poskytnúť dôkazy spájajúce obvineného s miestom činu, napr. vyšetrovatelia môžu z mobilných zariadení získať e-maily, telefónne hovory, fotografie, satelitné snímky, videá, bankové informácie a údaje GPS, ktoré im môžu pomôcť zdokumentovať trestné

* JUDr. Michal Klenka, PhD. Asistent súdkyně Najvyššieho súdu Slovenskej republiky. E-mail: michalklenka@gmail.com. ORCID: https://orcid.org/0000-0002-3210-6884. Názory vyjadrené v tomto článku sú výhradne názormi autora a nemožno ich považovať za oficiálnu pozíciu alebo stanoviská Najvyššieho súdu Slovenskej republiky.

činy a prepojiť vysoko postavených páchateľov s konkrétnymi udalosťami, ako sú masakre, nútené vysídlenia a mučenie. Spoliehanie sa na technológie, ktoré okrem svedectiev svedkov a obetí poskytujú dôkazy pri spáchaných medzinárodných zločinov, nie je v medzinárodnom trestnom súdnictve novinkou. Digitálne dôkazy môžu mať aj formu sociálnych médií, ako sú fotografie, video a zvukové záznamy, blogy a weby sociálnych sietí (napr. Facebook, Twitter a YouTube). Digitálne dôkazy môžu taktiež poskytnúť informácie o čase a mieste udalosti, obmedziť odhalenie zraniteľných svedkov alebo oslobodiť neprávom obvinených.[1]

Medzinárodné trestné súdy a tribunály stále častejšie používajú digitálne dôkazy pri stíhaní páchateľov medzinárodných zločinov. V konfliktných situáciách zahŕňajúcich spáchanie vojnových zločinov, zločinov proti ľudskosti a genocídy je potrebné veľké množstvo a rozmanitosť dôkazov na vysvetlenie kontextu konfliktu a na preukázanie potrebných prvkov zločinov a spôsobov zodpovednosti. Pokročilé digitálne nástroje (vrátane leteckých fotografií, mobilných zariadení, videa, rádiových zachytávačov) zachytávajú nové a obrovské množstvo údajov, ktoré môžu k existujúcim dôkazom pridať doplňujúce a podporné údaje, napr. zatiaľ čo očitý svedok môže poskytnúť relevantné informácie týkajúce sa udalosti, satelitná snímka môže odhaliť informácie, ktoré by inak boli nedostupné. Telefónne a počítačové záznamy môžu navyše poskytovať údaje relevantné pri činnosti jednotlivca alebo video môže byť geolokalizované, v dôsledku čoho vyšetrovateľom umožní vidieť podrobnosti o životnom prostredí, na ktoré svedok mohol zabudnúť. V závislosti od pravosti údajov môžu digitálne dôkazy poskytovať aj informácie o čase, mieste a spôsobe udalosti na doplnenie ústnych svedectiev. Digitálne dôkazy sa šíria tak rýchlo, ako sa technológie menia a rozširujú. Aj keď digitálne dôkazy umožňujú nové príležitosti k hľadaniu zodpovednosti, medzinárodné trestné súdy sa musia vyrovnať s výzvami, ktoré ich používanie prináša. V tejto súvislosti je potrebné poznamenať a zdôrazniť, že nato aby mohli byť digitálne dôkazy po zbere a zhromaždení následne katalogizované a využívané, rovnako, aby sa predišlo ich zbytočnému nahromadeniu, mali by v konečnom dôsledku vyšetrovatelia dodržiavať určité štandardy, aby zabezpečili, že napr. snímky, pri získaní ktorých aktivisti v prvej línii a preživší riskujú svoje životy, boli na súde využité. Ďalšou výzvou je, že digitálne dôkazy možno zmeniť (zmanipulovať) alebo znehodnotiť; rovnako je potrebné uviesť, že sú navyše oddelené od ich zdroja, napr. fotografia zachytáva iba jednu perspektívu miesta v konkrétnom čase a podobne, e-mail nezachytáva správanie alebo tón hlasu autora. Súdy si musia byť predovšetkým vedomé problémov týkajúcich sa zhromažďovania, pravosti, spoľahlivosti a prípustnosti. Napriek tomu z dôvodu nedostatku medzinárodných právnych usmernení vrátane definície digitálnych dôkazov a od nich následne odvodených dôkazov na medzinárodnej úrovni je súčasný

1 AMOURY COMBS, Nancy. Evidence. In: SCHABAS, William A. – BERNAZ, Nadia (eds). *Routledge Handbook of International Criminal Law*. Abingdon: Routledge, 2011, s. 323; HIATT, Keith. Open Source Evidence on Trial. *The Yale Law Journal Forum*. 2015–2016, Vol. 125 [cit. 2021-12-22]. Dostupné z: <http://www.yalelawjournal.org/forum/open-source-evidence-on-trial>, s. 323; KOENIG, Alexa – STOVER, Eric – CRITTENDEN, Camille – CODY, Stephen. Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court. *UC Berkeley: Human Rights Center*. 2014 [cit.], s. 3–4. Dostupné z: <https://humanrights.berkeley.edu/sites/default/files/publications/digital-fingerprints.pdf>; STAVROU, Konstantina. Open-Source Digital Evidence in International Criminal Cases: A Way Forward in Ensuring Accountability for Core Crimes? In: *Opinio Juris* [online]. 26. 1. 2021 [cit. 2021-12-22]. Dostupné z: <https://opiniojuris.org/2021/01/26/open-source-digital-evidence-in-international-criminal-cases-a-way-forward-in-ensuring-accountability-for-core-crimes/>.

právny rámec o digitálnych dôkazoch naplnený právnymi problémami, ktoré je potrebné riešiť, aby sa odstránili všetky medzery v zodpovednosti. Každá nová forma dôkazu, aj táto si vyžaduje dodatočné odborné znalosti, aby sa s ňou účinne a náležite vysporiadalo v rámci súdneho konania.[2]

Na pochopenie tejto novej a rozsiahlej kategórie dôkazov je dôležité poznať pojem „digitálny dôkaz" a pravidlá dokazovania, ktoré ho obklopujú a ktoré sú kľúčové v medzinárodnom trestnom konaní.

1. Definícia digitálnych dôkazov

Podľa Lindsey Freeman digitálnymi dôkazmi sú *„informácie a údaje cenné pre vyšetrovanie, ktoré sú uložené, prijaté alebo prenášané elektronickým zariadením"*. Väčšina digitálnych dôkazov sa považuje za listinné alebo forenzné dôkazy v závislosti od toho, či bola na preskúmanie alebo overenie predmetného dôkazu použitá akákoľvek analýza alebo vedecký postup. Digitálne fotografie, letecké a satelitné snímky, digitálne zvukové a video záznamy, záznamy hovorov, e-maily a iná elektronická komunikácia alebo elektronické dokumenty sa považujú za listinný dôkaz, a preto sa hodnotia na základe rovnakých kritérií ako papierové dokumenty. Ak boli na digitálne informácie aplikované forenzné postupy (napr. vylepšenie zvuku alebo zväčšenie fotografie) alebo bola zostavená analytická správa alebo znalecký posudok s použitím nespracovaných digitálnych údajov (napr. geolokalizovanie fotografie alebo tabuľka sekvencií hovorov), je možné, že bude potrebné predložiť dôkaz prostredníctvom znaleckého posudku, ktorý by si vyžadoval splnenie ďalších podmienok. Predmetné analytické výstupy, ktoré sú predložené ako dôkaz, by sa mali odlišovať od demonštračných dôkazov, ako sú vizuálne znázornenia alebo modely, ktoré technicky vôbec nie sú dôkazom.[3]

Medzinárodná advokátska komora diferencuje *„digitálne a technologicky odvodené dôkazy, čo znamená dôkazy prevzaté a vytvorené digitálnymi zariadeniami a prostredníctvom technológií, ako sú fotoaparáty, satelity a ďalšie technológie diaľkového prieskumu zeme […]. Rozlišujeme digitálne dôkazy vytvárané digitálnymi technológiami a samotné záznamy alebo stopy určitých aktov alebo udalosti použitých na účely konania, digitalizované dokumenty a záznamy za účelom uchovávania, organizovania a predkladania dôkazov."* Podľa Centra pre ľudské práva na Kalifornskej univerzite v Berkeley, ako aj Stephena Mansona *„digitálne dôkazy sú údaje, ktoré sú vytvárané, manipulované, uchovávané alebo komunikované akýmkoľvek zariadením, počítačom alebo počítačovým systémom alebo prenášané prostredníctvom komunikačného systému, ktoré sú relevantné pre konanie"*.[4]

---

2 *Report on Digitally Derived Evidence in International Criminal Law*. Leiden University. June 2019, s. 7. Dostupné z: <http://kalshovengieskesforum.com/wp-content/uploads/2020/11/2021_Legal-Framework-and-Practice-in-International-Courts-and-Tribunals-for-Launch-Event_for-publication.pdf>; ASHOURI Aida – BOWERS, Caleb – WARDEN, Cherrie. An Overview of the Use of Digital Evidence in International Criminal Courts. *Digital Evidence and Electronic Signature Law Review*. 2014, Vol. 11, s. 115. Dostupné z: <https://journals.sas.ac.uk/deeslr/article/view/2130/2060>; MEHANDRU, Nikita – KOENIG, Alexa. Icts, Social Media, & the Future of Human Rights. *Duke Law & Technology Review*. 2019, Vol. 17, No. 1, s. 144–145. Dostupné z: <https://scholarship.law.duke.edu/dltr/vol17/iss1/5/>.

3 FREEMAN, Lindsay. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. *Forham International Law Journal*. 2018, Vol. 41, Iss. 2, s. 297–298. Dostupné z: <https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1>.

4 *Report on Digitally Derived Evidence in International Criminal Law*, s. 9; MASON, Stephen (ed.). *International Electronic Evidence*. London: British Institute of International and Comparative Law, 2008, s. xxxv.

Môžu to byť fotografie, letecké snímky, záznamy (audio a video), forenzné dôkazy, balistické správy, DNA atď. S nástupom technológie je v súčasnosti možné ako dôkaz použiť akékoľvek digitálne/elektronické zariadenie, či už je to mobilný telefón, prenosný počítač alebo fotoaparát. Aj keď je pravda, že príbeh očitého svedka je v podstate osobnou interpretáciou spomienky na tento incident, nemusí byť taký komplexný ako elektronické zariadenie. Satelitná snímka môže byť napríklad schopná určiť neprístupné miesto a záznamy mobilných hovorov môžu poskytnúť presnú komunikáciu, čo môže zase pomôcť pri identifikácii aktivít páchateľa. Tieto informácie môžu súdom potenciálne pomôcť pri zisťovaní pravdy o incidente a ďalej môžu poskytnúť potrebnú podporu pri riadnom výkone vyšetrovania a jeho vhodnom rozhodovaní.[5]

2. Právny rámec prípustnosti dôkazov v medzinárodnom trestnom súdnictve

Vo všeobecnosti musia byť dôkazy relevantné a potrebné, aby boli pripustené a použité v konaní pred Medzinárodným trestným súdom. Akékoľvek posúdenie relevantnosti a dôkaznej hodnoty musí zahŕňať určité posúdenie spoľahlivosti dôkazov, čo znamená, že musia byť *prima facie* vierohodné. Dôkazy, ktoré nie sú dostatočne spoľahlivé, nemožno považovať za relevantné, ani za preukazujúce spornú skutočnosť.[6]

V medzinárodnom trestnom práve neexistujú žiadne výslovné dôkazné pravidlá, ktoré by upravovali prípustnosť a dôkaznú hodnotu/váhu digitálnych dôkazov. Rovnako ako všetky ostatné dôkazy, všetky digitálne dôkazy predložené medzinárodným trestným súdom sa hodnotia podľa všeobecných pravidiel dokazovania konkrétneho súdu. Tieto všeobecné pravidlá dokazovania je navyše možné doplniť tým, ako sa digitálne dôkazy v praxi pripúšťajú alebo vylučujú. Podľa pravidla 89 (C) Pravidiel súdneho konania a vykonávania dôkazov Medzinárodného trestného tribunálu pre bývalú Juhosláviu a Medzinárodného trestného tribunálu pre Rwandu môže senát pripustiť akékoľvek relevantné dôkazy, ktoré považuje za dôkazy majúce dôkaznou váhou. Pravidlo 89 (D) Pravidiel súdneho konania a vykonávania dôkazov Medzinárodného trestného tribunálu pre bývalú Juhosláviu ďalej stanovuje, že senát môže vylúčiť dôkaz, ak jeho dôkazná hodnota je podstatne prevážená potrebou zabezpečiť spravodlivý proces. Pravidla súdneho konania a vykonávania dôkazov Medzinárodného trestného tribunálu pre Rwandu neobsahujú žiadne také ustanovenie, ale rovnaký princíp sa v praxi uplatňoval.[7] Pravidlo 95 Pravidiel súdneho konania a vykonávania dôkazov Medzinárodného trestného tribunálu pre bývalú Juhosláviu a Medzinárodného trestného tribunálu pre Rwandu a článok 69 ods. 7 Rímskeho štatútu Medzinárodného trestného súdu (ďalej len „Rímsky štatút“) vyjadrujú podobný prístup vyvážením rôznych záujmov, ak sa rozlišuje medzi menšími priestup-

---

5 NARAYANAN, Aparajitha. Evidentiary Challenges of New Technologies in International Criminal Trials. *The Responsibility to Protect Student Journal*. 2020, Vol. 5, Iss. 1, s. 61.

6 SCHABAS, William A. *Introduction to the International Criminal Court*. 4th edition. Cambridge: Cambridge University Press, 2011, s. 312–313.

7 *Report on Digitally Derived Evidence in International Criminal Law*, s. 22; International Criminal Tribunal for the former Yugoslavia. Rules of Procedure and Evidence. 8 July 2015 [cit. 2021-12-27], s. 91. Dostupné z: <https://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev50_en.pdf>; International Criminal Tribunal for Rwanda. Rules of Procedure and Evidence. 13 May 2015 [cit. 2021-12-27], s. 102. Dostupné z: < https://unictr.irmct.org/sites/unictr.org/files/legal-library/150513-rpe-en-fr.pdf>.

kami a inými závažnými porušovaniami práv obžalovaného; príkladom toho druhého by mohli byť vyjadrenia získané mučením (viac nižšie).[8]

Rímsky štatút v čl. 69 obsahuje iba základné princípy, ktorými upravuje problematiku dôkazov, a ďalšie podrobnosti, sekundárne a subsidiárne pravidlá sú ďalej rozpracované v Pravidlách súdneho konania a vykonávania dôkazov (pravidla 63–75) a prostredníctvom výkladu a súdnych rozhodnutí. Požiadavka na osobnú výpoveď svedka uvedená v čl. 69 ods. 2 Rímskeho štatútu odráža želanie, aby bol primárny zdroj dôkazov dostupný na účely súdneho konania. Rovnako to dáva stranám najlepšiu príležitosť vypočuť svedka a súdu klásť otázky a hodnotiť správanie a dôveryhodnosť svedka. Pravidlo 67 Pravidiel súdneho konania a vykonávania dôkazov umožňuje svedkom vypovedať prostredníctvom audio alebo video spojenia. Je dôležité poznamenať, že predpis 26 ods. 4 Nariadení súdu uvádza, že v konaní pred súdom sa iné dôkazy ako živé svedectvá predkladajú v elektronickej forme vždy, ak je to možné, avšak pôvodná podoba je hodnoverná. Súd tiež potvrdil, že jedným z relevantných kritérií na to, či osoba (ne)môže vypovedať naživo prostredníctvom audio alebo video spojenia, je blaho svedka a osobné okolnosti.[9]

Článok 69 ods. 4 Rímskeho štatútu umožňuje súdu *„rozhodnúť o relevantnosti alebo prípustnosti všetkých dôkazov“* pred zvážením otázky ich dôkaznej váhy. Súd môže buď: i) najprv rozhodnúť, či dôkazy majú dostatočnú relevanciu na odôvodnenie ich prípustnosti, berúc do úvahy množstvo faktorov uvedených v čl. 69 ods. 4 a následne vyhodnotiť váhu akýchkoľvek prijatých dôkazov ako súčasť procesu hodnotenia; alebo namiesto toho ii) pripustiť dôkazy a spoločne zvážiť relevantnosť, prípustnosť a váhu ako súčasť hodnotenia pripustených dôkazov, pričom zohľadní rovnaké faktory. Ak by sa súd rozhodol postupovať jednou alebo druhou analytickou metódou, bolo by to ovplyvnené, okrem iného potrebou zabezpečiť ochranu iných hodnôt v rozhodovacom procese, akými sú napr. práva obvineného, právo na spravodlivý proces, spravodlivé hodnotenie svedeckej výpovede a práva obetí. V niektorých situáciách by ochrane týchto hodnôt najlepšie poslúžilo vylúčenie alebo neprípustnosť dôkazov, a nie ich pripustenie a následné priznanie malej alebo žiadnej dôkaznej váhy. V každom prípade pravidlo 64 objasňuje, že otázky týkajúce sa relevantnosti alebo prípustnosti by mali byť vznesené pri predkladaní dôkazov, pričom senát musí zdôvodniť akékoľvek rozhodnutia o dôkazných záležitostiach.[10]

Článok 69 ods. 4 Rímskeho štatútu vymenúva trojbodový test, na základe ktorého senát prípravného konania Medzinárodného trestného súdu preskúma nasledujúce prvky dôkazu: i) relevantnosť (či súvisí s okolnosťami prípadu), ii) dôkaznú hodnotu (či prispieva k dokazovaniu spornej skutočnosti) a iii) relevantnosť prevážiť nad akýmkoľvek potenciálnym škodlivým účinkom, ktorý môže byť spôsobený jeho prijatím. Je dôležité mať na pamäti, že vyššie uvedené podmienky musia byť splnené aj pri predkladaní digitálnych dôkazov.[11]

---

8 KLAMBERG Mark. Evidentiary Matters in the Context of Investigating and Prosecuting International Crimes in Sweden: Admissibility, Digital Evidence and Judicial Notice. *Scandinavian Studies in Law*. 2020, Vol. 66, s. 372. Dostupné z: <https://ssrn.com/abstract/=3705908>; International Criminal Tribunal for the former Yugoslavia. Rules of Procedure and Evidence. 8 July 2015, s. 101; International Criminal Tribunal for Rwanda. Rules of Procedure and Evidence. 13 May 2015, s. 114.

9 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*. 3rd edition. München – Oxford – Baden Baden: C. H. Beck – Hart – Nomos, 2016, s. 1722, 1723–1724; International Criminal Court. Regulations of the Court. 2018 [cit. 2021-12-27], s. 11. Dostupné z: <https://www.icc-cpi.int/Publications/Regulations-of-the-Court.pdf>.

10 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*, s. 1735.

Relevantnosť a prípustnosť sú súvisiace, ale dva odlišné pojmy. Relevantnosť nie je absolútny pojem, ale je to vzťah alebo súvislosť, ktorá je odvodená od ponúkaného dôkazu a spornej skutočnosti alebo tvrdenia, ktoré sa má dokázať alebo vyvrátiť. Je to vzťah, ktorého existencia spôsobuje, že je viac pravdepodobné ako nepravdepodobné, že skutočnosť alebo tvrdenie existuje alebo neexistuje. Existencia dôkazu má tendenciu zvyšovať alebo znižovať pravdepodobnosť existencie predmetnej skutočnosti. Toto sa často označuje ako racionálna preukázateľnosť dôkazov (*rational probativeness of the evidence*), t. j. otázkou je, či dôkaz racionálne preukazuje predmetnú skutočnosť.

Existujú dva aspekty relevantnosti, ktoré môžu spôsobiť, že dôkazy sú irelevantné. V prvom prípade dôkazy nemajú tendenciu dokázať alebo vyvrátiť predmetnú skutočnosť, t. j. neexistuje racionálna súvislosť ani dôkazná hodnota či vzťah. V druhom aspekte rovnako nemusí existovať žiadna racionálna súvislosť alebo dôkazná hodnota, ak v danom prípade nejde o konkrétnu spornú skutočnosť, o ktorej by dôkazy mohli svedčiť. V takýchto situáciách sú dôkazy irelevantné a neprípustné.

Samotná skutočnosť, že dôkazy sú striktne relevantné v logickom zmysle, však nezaručuje ich prípustnosť. Relevantnosť je často otázkou stupňa preukázateľnosti a niekedy, hoci má určitú dôkaznú hodnotu, nie je dostatočne preukázateľná na to, aby odôvodňovala pripustenie dôkazu na základe iných úvah. Tieto úvahy môžu zahŕňať situácie, keď konkrétna predmetná skutočnosť je príliš vedľajšia alebo vzdialená na to, aby bola dôkazom sporných skutočností, ktoré sa majú dokázať alebo vyvrátiť. Alebo konkrétna predmetná skutočnosť nie je v skutočnosti v kontexte prípadu sporná z dôvodu prevažujúcej dôkaznej hodnoty iných dôkazov, ktoré majú tendenciu dokázať alebo vyvrátiť predmetnú skutočnosť. Môže zahŕňať aj situácie, keď dôkazy o predchádzajúcom správaní (sexuálnom, kriminálnom alebo inom), ktoré racionálne nesúvisia s konaním, ktoré je predmetom trestného konania, môžu mať tendenciu ukázať, že daná osoba je nemorálna alebo má zlý charakter (čo je hodnotový úsudok založený na vlastných životných skúsenostiach a hodnotách posudzovateľa) alebo, že mala sklony ku kriminalite, ale bez racionálnejšej súvislosti s prípadom by takáto miera preukázateľnosti nemusela odôvodňovať pripustenie dôkazov. Takto predpojatá dôkazná hodnota zakrýva skutočnú dôkaznú váhu dôkazu, ktorá môže byť skutočne minimálna alebo neexistujúca. Pripustenie takéhoto dôkazu môže preto poškodiť spravodlivý súdny proces alebo spravodlivé hodnotenie svedeckej výpovede. Niekedy, aj keď sú dôkazy dostatočne relevantné (t. j. majú dostatočnú dôkaznú váhu), iné politické hľadiská prevážia ich pripustenie, napr. ak dôkazy podliehajú zákonom upravenej povinnosti mlčanlivosti alebo ak je ich vylúčenie nevyhnutné na ochranu národnobezpečnostných záujmov alebo svedka pred ujmou.[12]

Používanie digitálnych dôkazov na medzinárodných trestných súdoch je potrebné chápať vo svetle všeobecného prístupu k rozhodovaniu o pripustení dôkazov v konaní pred súdom. Pravidlo 69 ods. 4 nariaďuje sudcom pripustiť dôkazy *„berúc do úvahy okrem iného dôkaznú hodnotu dôkazov a akékoľvek predsudky, ktoré môžu tieto dôkazy spôsobiť pre spravodlivý proces alebo pre spravodlivé vyhodnotenie výpovede svedka“*. V súlade s pravidlom 63 ods. 2 určujú dôkazovú hodnotu a „primeranú váhu“ pripustených dôkazov na

11 NARAYANAN, Aparajitha. *Evidentiary Challenges of New Technologies in International Criminal Trials*, s. 60–61; ASHOURI, Aida – BOWERS, Caleb – WARDEN, Cherrie. *An Overview of the Use of Digital Evidence in International Criminal Courts*, s. 116–117.

12 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*, s. 1735–1736.

konci prípadu, keď posudzujú dôkazy ako celok. Existujú iba dve situácie, v ktorých je konkrétna povinnosť sudcov rozhodnúť o neprípustnosti dôkazov. Jediné výnimky z tohto širokého štandardu sú uvedené v článku 69 ods. 7 Rímskeho štatútu a pravidlo 71 Pravidiel súdneho konania a vykonávania dôkazov.

Rímsky štatút v čl. 69 ods. 7 k vylúčeniu prípustnosti uvádza, že *„dôkazy, ktoré boli získané porušením tohto štatútu alebo medzinárodne uznávaných ľudských práv, nie sú prípustné, ak a) porušenie vrhá vážne pochybnosti na spoľahlivosť dôkazov alebo b) pripustenie dôkazu by bolo v rozpore s bezúhonnosťou konania a mohlo by ju vážne ohroziť“*. Aj keď sa zdá, že to vyžaduje povinné vylúčenie dôkazov, v praxi majú sudcovia široký priestor na to, ako sa toto ustanovenie uplatňuje, keďže je na nich, aby určili požadovanú mieru kauzality. Podľa senátu pre prípravné konanie *„sudcovia majú právo uváženia hľadať v každom konkrétnom prípade primeranú rovnováhu medzi základnými hodnotami štatútu“*.[13]

Porušenie Rímskeho štatútu je pomerne jednoduchý pojem, ktorý by mohol zahŕňať porušenie niektorého z práv obvineného [čl. 55, 57 a 64 ods. 2, ods. 6 písm. e)] alebo poškodených alebo svedkov [čl. 57, 68 a 64 ods. 2, ods. 6 písm. e)] alebo iných hmotnoprávnych alebo procesnoprávnych ustanovení (čl. 56, 57, a deviata časť Rímskeho štatútu) za predpokladu, že porušenie je v príčinnej súvislosti so zhromažďovaním napadnutých dôkazov.

Pojem „medzinárodne uznávané ľudské práva“ bol určený tak, aby zahŕňal aj nezmluvné normy, aby bol širší ako samotné medzinárodné právo (napr. obsahoval uznávané normy a štandardy vypracované OSN v oblasti trestného súdnictva).[14] Jediným doposiaľ medzinárodne uznávaným ľudským právom definovaným v judikatúre Medzinárodného trestného súdu je medzinárodne uznávané právo na súkromie.

Podľa čl. 69 ods. 7 písm. a) ak sa dôkazy získavajú v rozpore s Rímskym štatútom alebo medzinárodne uznávanými ľudskými právami, môže to nepriaznivo ovplyvniť ich spoľahlivosť a môže to byť základom na ich vylúčenie. Niektoré formy nezákonnosti alebo porušovania ľudských práv vytvárajú nebezpečenstvo, že dôkazy (napr. priznanie získané od osoby počas výsluchu) nemusia byť pravdivé alebo spoľahlivé, pretože mohli byť ponúknuté v dôsledku nátlaku vyplývajúceho z okolností porušenia. Iné formy dôkazov si vyžadujú uchovávanie alebo zhromažďovanie spôsobom, ktorý zabezpečí ich integritu a spoľahlivosť pred manipuláciou, poškodením alebo znehodnotením. Predmetné ustanovenie vyžaduje, aby účinok porušenia bol takej miery, že „vyvoláva podstatnú pochybnosť“ o spoľahlivosti dôkazov. Základ vylúčenia podľa čl. 69 ods. 7 písm. b) zahŕňa, ale je širší ako otázky súvisiace so spoľahlivosťou dôkazov. Napriek porušeniu Rímskeho štatútu alebo medzinárodne uznávaných ľudských práv môžu byť dôkazy spoľahlivé alebo o ich spoľahlivosti nemusia byť zásadné pochybnosti. Škodlivý účinok predmetného ustanovenia je vyvolaný „prijatím“ dôkazov, a nie „porušením“ Rímskeho štatútu alebo medzinárodne uznávaných ľudských práv. Porušenie musí existovať ako predpoklad, ako to vyžaduje návetie odseku 7. Avšak práve pripustenie týchto dôkazov by vzhľadom na porušenie bolo v rozpore s bezúhonnosťou konania alebo by ju poškodilo. Zmyslom tohto odseku je, že by bolo v rozpore s cieľmi a integritou súdu, ktorý bol vytvorený na nápravu závažných porušení medzinárodného humanitárneho práva, pripúšťať a používať dôkazy,

---

13 *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Decision on the Confirmation of Charges, 84 (Feb. 7, 2007), [cit. 2021-12-22]. Dostupné z: <https://www.icc-cpi.int/pages/record.aspx?uri=266175>.

14 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*, s. 1745–1746.

ktoré boli získané porušením jeho vlastného štatútu alebo medzinárodne uznávaných ľudských práv. Pripustenie a použitie takýchto dôkazov súdom by v podstate poškodilo účel a integritu jeho vlastných konaní, ktorých cieľom je presadzovanie právneho štátu a ľudských práv vo svete (alebo slovami preambuly Rímskeho štatútu *„zaručiť trvalý rešpekt a vykonávanie medzinárodnej spravodlivosti“* a *„mier, bezpečnosť a blahobyt na svete“*).

Predmetný dvojitý test v rámci ods. 7 (t. j. požiadavka na porušenie a škodlivý účinok) spolu s inherentnou diskrečnou právomocou súdu pri určovaní existencie týchto podmienok vyvolal kritiku, že predmetný odsek pripúšťa porušenie niektorých ustanovení Rímskeho štatútu alebo ľudských práv, pokiaľ toto porušenie nie je takého rozsahu, aby malo škodlivé účinky uvedené v písm. a) alebo b). Do určitej miery je to opodstatnená kritika, ale ods. 7 je výsledkom dosiahnutia konsenzu a kompromisu. Ide o rovnováhu navzájom si konkurujúcich koncepcií, pokiaľ ide o základ pre pravidlo vylúčenia, ako aj o mechanizmus na vyriešenie aplikácie protichodných základných hodnôt Rímskeho štatútu v konkrétnom kontexte určovania prípustnosti dôkazov v konkrétnom prípade, ktorý je síce preukázateľný, ale bol zhromaždený spôsobom, ktorý porušuje iné hodnoty.[15]

Pravidlo 71 zakazuje pripustenie dôkazov o predchádzajúcom alebo následnom sexuálnom správaní obete alebo svedka. Tieto vyššie uvedené ustanovenia sú navrhnuté zúžene a nezabezpečujú automatické vylúčenie dôkazov. Dôkazy, ktoré majú byť prijaté, musia spĺňať *„minimálne štandardy relevantnosti a spoľahlivosti“*. Keďže latka prípustnosti je nízka, pripustenie dôkazov samo osebe neznamená, že sú dôkazy presné; sudcovia hodnotia ich váhu oddelene. Pri posudzovaní dôkazov sa *ad hoc* súdy nezameriavajú na to, či sú dôkazy prípustné, ale skôr na to, akú majú dôkaznú váhu.[16] Dôkazná váha každého digitálneho dôkazu nie je v rozhodnutiach uvedená a zdôvodnenie, ktoré za tým stojí, sa môže líšiť od prípadu k prípadu. Je preto dôležité vykonať kumulatívnu analýzu, aby sa vytvorilo usmernenie pre vyšetrovanie. Užitočnosť by mohla byť ešte väčšia, ak by bolo možné podrobne analyzovať typ digitálneho dôkazu. Medzinárodný trestný súd, ktorý v rámci svojej dvadsať ročnej existencie, zatiaľ nezhromaždil dostatok prípadov, prinajmenšom na pokrytie hlavných typov digitálnych dôkazov. V dôsledku čoho sa nedá vyhnúť tomu, že digitálne dôkazy sa v určitom rozsahu predkladajú pred súdom s určitou neistotou o ich stave.[17]

Z vyššie uvedeného možno konštatovať, že vznikol určitý všeobecný štandard prípustnosti dôkazov, ktorý je spoločný pre všetky medzinárodné trestné súdy a tribunály: i) relevantnosť (dôkazy sú *prima facie* relevantné pre konanie); ii) dôkazná hodnota samotného dôkazu; iii) potenciálny škodlivý účinok (ak je to relevantné, je potrebné zvážiť dôkazovú hodnotu voči akémukoľvek potenciálnemu škodlivému účinku dôkazu pre konanie). Tento trojdielny test vyplývajúci z čl. 69 ods. 4 Rímskeho štatútu používajú sudcovia na vyhodnotenie prípustnosti dôkazov. Pokiaľ ide o digitálne dôkazy, prax ukazuje, že otázka dôkaznej hodnoty je najkontroverznejším a najdiskutovanejším kritériom prípustnosti. Podľa judikatúry je spravidla jedným z hlavných faktorov posudzovania dôkaznej hodnoty

15 Ibidem, s. 1747–1749.

16 FREEMAN, Lindsay. *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, s. 294–295; ASHOURI, Aida – BOWERS, Caleb – WARDEN, Cherrie. *An Overview of the Use of Digital Evidence in International Criminal Courts*, s. 116–117.

17 HONG, Ilyoung. International Digital Forensic Investigation at the ICC. In: BIASIOTTI, Maria Angela – MIFSUD BONNICI, Jeanne Pia – CANNATACI, Joe – TURCHI, Fabrizio (eds). *Handling and Exchanging Electronic Evidence Across Europe*. Cham: Springer, 2018, s. 135.

spoľahlivosť dôkazov, ktorá závisí od mnohých okolností, ako je pôvod, obsah, potvrdenie, pravdivosť, dobrovoľnosť a dôveryhodnosť dôkazu. Okrem toho hodnotenie spoľahlivosti je blízke hodnoteniu dôveryhodnosti, ako aj otázke autentifikácie.[18] Hoci norma prípustnosti používaná na medzinárodných trestných súdoch vyžaduje, aby dôkazy boli relevantné a mali preukázanú dôkaznú váhu, ako už bolo vyššie uvedené, tento prah je dosť nízky. Rovnako možno konštatovať, že dôkazné pravidlá sú obzvlášť flexibilné a permisívne, čím predmetný právny rámec umožňuje Medzinárodnému trestnému súdu hodnotiť dôkazy získané z nových technológií a zariadení.[19]

3. Právne otázky pri digitálnych dôkazoch

Všeobecné pravidlá a zásady dokazovania sa uplatňujú na všetky dôkazy, vrátane tých digitálnych. Napriek jedinečným vlastnostiam digitálnych dôkazov, doposiaľ neexistuje žiadny konkrétny článok alebo ustanovenie, ktoré by bolo výslovne ustanovené pre digitálne dôkazy. To znamená, že dôkazy, ktoré majú byť pripustené, musia spĺňať minimálne štandardy relevantnosti a spoľahlivosti. Neustále sa zväčšujúce množstvo digitálnych informácií v 21. storočí a potenciálnych dôkazov použiteľných v trestnom konaní prináša príležitosti a výzvy. Jednou z kľúčových otázok je, či je možné dôkazy overiť. Pokiaľ nie je možné sudcom zaistiť pravosť digitálnych dôkazov, ich potenciálna hodnota pre vyšetrovanie trestných činov sa nevyužije. Táto obava, ktorá bude ďalej len rásť so vznikom tzv. *„deepfake"* (falošných) videí, ktoré sú dostatočne sofistikované na to, aby oklamali väčšinu divákov. Ďalšiu veľkú výzvu predstavuje samotný zber, ako aj následná analýza digitálnych dôkazov, ktoré musia byť preskúmané a overené, musí sa zriadiť určitý systém kontroly pôvodu dôkazu (*chain of custody – provenance*), keďže internetové stránky (napr. YouTube) odstraňujú metadáta, čo častokrát sťažuje stanovenie dôkaznej hodnoty samotného dôkazu. Metadáta môžu pomôcť určiť čas a dátum vytvorenia súboru, informácie o priradenom účte a zariadení, na ktorom bol súbor vytvorený, a všetky úpravy súboru. V ideálnom prípade sú k dispozícii metadáta, ktoré pomáhajú preskúmať a overiť potenciálne dôkazy. Elektronické dokumenty, ako napríklad dokumenty Word, často obsahujú metadáta, ktoré môžu pomôcť pri overovaní obsahu. Údaje sú automaticky vytvárané softvérom a môže ich doplniť autor dokumentu. Keďže metadáta sú generované automaticky, často bez vedomia alebo pomoci používateľa, je menej pravdepodobné, že budú manipulované alebo odstránené ako iný obsah. V prípade videozáznamov môžu vyšetrovatelia použiť metadáta na určenie polohy miesta vo videu a jeho autora, ktoré je potom možné extrapolovať na preskúmanie vybraných udalostí. Interpretácia metadát však vyžaduje súbor základných predpokladov, napr. musíme predpokladať, že časové pásmo na zariadení správne odráža jeho okolité prostredie v čase vytvárania informácií a že nikto neprepísal a ani nezmanipuloval metadáta.[20]

---

18 *Report on Digitally Derived Evidence in International Criminal Law*, s. 22–23.

19 AMOURY COMBS, Nancy. Evidence. In: SCHABAS, William A. – BERNAZ, Nadia (eds). *Routledge Handbook of International Criminal Law*, s. 326; TREVISAN, Stefano. Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol. In: *Giurisprudenza Penale Web* [online]. 30. 4. 2021 [cit. 2021-12-27], s. 7. Dostupné z: <https://www.giurisprudenzapenale.com/wp-content/uploads/2021/04/Trevisan_gp_2021_4.pdf>.

20 HONG, Ilyoung. International Digital Forensic Investigation at the ICC. In: BIASIOTTI, Maria Angela – MIFSUD BONNICI, Jeanne Pia – CANNATACI, Joe – TURCHI, Fabrizio (eds). *Handling and Exchanging Electronic Evidence Across Europe*, s. 127; HAMILTON, Rebecca J. Social Media Platforms in International Criminal Investigations. *Case Western Reserve*

3.1 Autentifikácia digitálneho dôkazu

Dôkazy sa považujú za autentické, ak sú pravé a nie sú sfalšované. „Overenie" je technický termín pre proces stanovenia spoľahlivosti alebo pravdivosti informácií. „Autentifikácia" odkazuje na právny koncept, ktorý podporuje integritu súdneho konania zaistením predložených dôkazov, ktoré určujú, čo chcú dokázať. Súdy sú predovšetkým znepokojené s autentifikáciou digitálnych dôkazov, pretože, ako už bolo viackrát uvedené, je ich možné ľahko manipulovať. Videozáznamy môžu byť napríklad zmenené alebo môžu byť zmenené metadáta, na zaistenie pravdivosti dôkazov je preto potrebný určitý stupeň autentifikácie. V súčasnosti v medzinárodnom trestnom práve neexistuje zavedený postup na autentifikáciu digitálnych dôkazov, ale Pravidlá súdneho konania a vykonávania dôkazov medzinárodných trestných súdov a tribunálov obsahujú ustanovenia, ktoré umožňujú súdu požiadať o autentifikáciu dôkazov. Medzinárodný trestný súd nevyžaduje, aby sudca rozhodoval o pravosti dôkazov oddelene. Ak sa strany dohodnú, že dôkazy sú autentické, alebo ak sú dôkazy spoľahlivé, sudcovia môžu s dôkazmi zaobchádzať ako s autentickými. Ak dôkaz nespĺňa *prima facie* štandard, strana môže poskytnúť dodatočné informácie na preukázanie pravosti. Navyše z judikatúry vyplýva, že strana, ktorá predkladá dôkazy, nesie bremeno preukázania jej pravosti. *Ad hoc* súdy vo všeobecnosti uprednostňujú potvrdenie digitálnych dôkazov prostredníctvom externých ukazovateľov. Ako už bolo spomenuté, autentifikácia je považovaná za základný faktor pri posudzovaní dôkazov. Autentifikácia a spoľahlivosť sú príbuzné, ale odlišné koncepty. Účelom autentifikácie je zaistiť, aby sa dôkazy neupravovali alebo sa s nimi nemanipulovalo, zatiaľ čo účelom spoľahlivosti je zistiť, či dôkaz je tým, čím údajne má byť. Na zachovanie autentickosti dôkazov je štandardnou digitálnou forenznou požiadavkou napr. použitie blokovania zápisu. Na udržiavanie, overovanie a preukazovanie autenticity digitálnych dôkazov sa používajú aj digitálne podpisy, šifrovacie a hashovacie algoritmy.[21]

3.2 Spoľahlivosť digitálneho dôkazu

Pojem „spoľahlivosť" je vlastnosťou dôveryhodnosti alebo presvedčenia. Vo svojom klasickom význame spoľahlivosť znamená spoľahlivé a konzistentné výsledky, ktoré je možné získať napodobiteľným a opakovateľným procesom. Medzinárodný trestný tribunál pre bývalú Juhosláviu opísal spoľahlivosť ako *„neviditeľnú zlatú niť, ktorá prechádza všetkými zložkami prípustnosti"*, ale prestal ju pridávať ako požiadavku, keďže nie je konkrétne uvedená v príslušnom ustanovení.[22]

Journal of International Law. 2020, Vol. 52, Iss. 1, s. 218. Dostupné z: <https://scholarlycommons.law.case.edu/jil/vol52/iss1/12>; KOENIG, Alexa – STOVER, Eric – CRITTENDEN, Camille – CODY, Stephen. *Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court*, s. 4, 6; MEHANDRU, Nikita – KOENIG, Alexa. *Icts, Social Media, & the Future of Human Rights*, s. 141–142.

21 ASHOURI Aida – BOWERS, Caleb – WARDEN, Cherrie. *An Overview of the Use of Digital Evidence in International Criminal Courts*, s. 117–118; *Report on Digitally Derived Evidence in International Criminal Law*, s. 32–33; TREVISAN, Stefano. *Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol*, s. 9–10; DUBBERLEY, Sam – KOENIG, Alexa – MURRAY, Daragh (eds). *Digital Witness. Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford University Press, 19 December 2019, s. 10.

22 TREVISAN, Stefano. *Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol*, s. 8; SCHABAS, William A. *Introduction to the International Criminal Court*, s. 312.

Spoľahlivosť sa týka dôveryhodnosti obsahu informácií obsiahnutých v digitálnom dokumente, videu alebo obrázku, ktorých vyhodnotenie sa môže líšiť v závislosti od účelu, na ktorý je dôkaz predložený. Aj o uznávaných spravodajských zdrojoch je známe, že kvôli časovému tlaku a dezinformáciám robia vážne chyby v podávaní správ. Pri menej známych zdrojoch je toto nebezpečenstvo ešte väčšie. Aj keď tradičné médiá môžu byť nápomocné pri nasmerovaní vyšetrovateľov na konkrétne udalosti, samotné príbehy majú veľmi obmedzenú dôkazovú hodnotu a akékoľvek číselné údaje, ktoré poskytujú, by mali mať vždy uvedený zdroj. Neoverené správy (*hearsay*) sú rovnako veľký problém s obsahom vytváraným používateľmi, a preto sa vyšetrovatelia musia obrátiť na používateľa a podniknúť kroky na nájdenie pôvodného zdroja informácií, aby, ak je to možné, poskytli priamy dôkaz. Na to, aby sa zaistila dôveryhodnosť informácií, vyšetrovatelia musia identifikovať objektívne overiteľné informácie a overiť ich, hľadať ďalšie dôkazy na ich potvrdenie.[23]

Podľa Ilyoung Honga, problém so spoľahlivosťou dôkazov môže nastať vtedy, ak znalosti a odbornosť osôb zapojených do zhromažďovania a uchovávania dôkazov nie sú dostatočné. Digitálne dôkazy bez náležitej dokumentácie o systéme kontroly pôvodu alebo zaručenej autentickosti nebudú počas vyšetrovania a súdneho konania považované za spoľahlivé. Aj keď sa úroveň odbornosti v oblasti digitálnej kriminalistiky celosvetovo zvyšuje, realitou je, že existuje mnoho krajín, v ktorých digitálne forenzné postupy, technológie a vyškolené ľudské zdroje ešte nie sú zavedené.[24]

Nachádzame sa v ére zvýšeného prístupu a transparentnosti a neschopnosti zabrániť virálnemu šíreniu uniknutých informácií. Pri hodnotení spoľahlivosti údajných utajovaných dokumentov, ktoré unikli, je kľúčovým faktorom dôveryhodnosť zdroja alebo úniku. Keď sú takéto dokumenty uložené na internet anonymne (napr. prostredníctvom *WikiLeaks* alebo podobných platforiem), nie je známy ich zdroj a ich dôveryhodnosť nie je možné overiť bez spoľahlivého svedka. Každý zdroj uniknutých dokumentov a samotný dokument je potrebné posudzovať od prípadu k prípadu skeptickým pohľadom, najmä ak údajný pôvodný zdroj autenticitu dokumentu popiera alebo ak dokument existuje iba v digitálnom formáte.[25]

3.3 Systém kontroly pôvodu digitálnych dôkazov

Systém kontroly pôvodu alebo proveniencie je definovaný ako pohyb a umiestnenie skutočných dôkazov, a história tých osôb, ktoré ich mali v držbe, od ich získania až do predloženia na súd. Stanovenie pôvodu si vyžaduje svedectvo o nepretržitej držbe, ako aj svedectvo o tom, že dôkaz zostal v podstate v rovnakom stave počas držby u každého jednotlivca. Tieto informácie poskytujú úplnú históriu umiestnenia a osôb, ktoré narábali s dôkazom,

---

23 FREEMAN, Lindsay. Prosecuting Atrocity Crimes with Open Source Evidence. In: DUBBERLEY, Sam – KOENIG, Alexa – MURRAY, Daragh (eds). *Digital Witness. Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, s. 66.

24 HONG, Ilyoung. International Digital Forensic Investigation at the ICC. In: BIASIOTTI, Maria Angela – MIFSUD BONNICI, Jeanne Pia – CANNATACI, Joe – TURCHI, Fabrizio (eds). *Handling and Exchanging Electronic Evidence Across Europe*, s. 132.

25 WORSTER, William Thomas. The Effect of Leaked Information on the Rules of International Law. *American University International Law Review*. 2013, Vol. 28, No. 2, s. 443–488. Dostupné z: <http://dx.doi.org/10.2139/ssrn.2012490>; FREEMAN, Lindsay. Prosecuting Atrocity Crimes with Open Source Evidence. In: DUBBERLEY, Sam – KOENIG, Alexa – MURRAY, Daragh (eds). *Digital Witness. Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, s. 65–66.

čo je dôležité pri určovaní, či bol pozmenený alebo bolo s ním manipulované, pričom jeho presnosť bude posúdená súdom. Dobre fungujúci systém kontroly pôvodu zvyšuje váhu dôkazu, podľa ktorej sudcovia pristupujú a hodnotia dôkaz. Ako príklad možno uviesť, že faktory (napr. dôkaz o autorstve), budú prirodzene nadobúdať najväčší význam pri posudzovaní váhy, ktorú má jednotlivým dôkazom pripisovať senát. Medzinárodné trestné súdy uprednostňujú ak prokuratúra poskytne výpovede živého svedka, zvyčajne autora, pred pripustením alebo prihliadnutím na digitálne dôkazy. Avšak nedostatok svedectva autora zvyčajne nevylučuje ich prijatie.[26]

Systém kontroly pôvodu je základným a kritickým problémom fyzických a offline listinných dôkazov. Napriek tomu ho aktivisti pri zabezpečovaní potenciálnych dôkazov z otvorených zdrojov často prehliadajú. Zachovanie systému kontroly pôvodu môže zvýšiť transparentnosť spôsobu, akým vyšetrovateľ informácie získal, a pomôcť zaistiť, aby so žiadnymi zhromaždenými informáciami sa nemanipulovalo. Pri používaní digitálnych dôkazov sú rizikom spôsob manipulácie a riziko ich stiahnutia, najmä pokiaľ ide o grafické alebo kontroverzné snímky. Archivácia akejkoľvek fotografie alebo videa nájdeného online pomáha zaistiť, aby bol materiál stále prístupný pre súdne účely, dokonca aj niekoľko rokov v budúcnosti. Napriek tomu, že technologické spoločnosti (Meta, Twitter a Google) ukladajú metadáta súvisiace s videami a fotografiami interne, odmietajú poskytnúť tieto informácie na účely medzinárodného trestného konania bez toho, aby prešli zmluvou o vzájomnej právnej pomoci alebo iným formálnym súdnym procesom, čiastočne, aby sa zabránilo ohrozeniu používateľov alebo narušeniu súkromia používateľov. Vyšší štandard pre dôkazy z otvorených zdrojov, ktoré sa majú použiť v konaní, v porovnaní so štandardom pre novinárske účely a/alebo obhajovanie ľudských práv, robí dokumentáciu všetkých postupov objavovania, overovania a uchovávania nevyhnutnou. Zabezpečenie toho, aby sudcovia pripúšťali dôkazy a pripisovali im dôkaznú váhu, môže do značnej miery závisieť od množstva zozbieraných metadát, uchovania systému kontroly pôvodu a kvality overovania a autentifikácie.[27]

4. Čo prinesie budúcnosť?

Lindsay Freeman naznačuje, že digitálne technológie zásadným spôsobom menia medzinárodné vyšetrovanie a stíhanie obvinených z najzávažnejších trestných činov medzinárodného záujmu dvoma spôsobmi: i) údaje a digitálne informácie vytvárané používaním digitálnych zariadení vytvorili nový a plodný súbor potenciálnych dôkazov; a ii) nové technológie menia spôsob samotnej prezentácie dôkazov. Pri pohľade na budúce prípady je zrejmé, že sa bude stále viac spoliehať na digitálne dôkazy, čo znamená, že je potrebné pripraviť prokurátorov, vyšetrovateľov, obhajcov a sudcov. Existuje niekoľko situácií z predbežných preskúmaní alebo vyšetrovaní Medzinárodným trestným súdom (napr. konflikty na Ukrajine, v Sýrii, Iraku a Afganistane), pri ktorých by bolo možné využiť potenciál digitálnych dôkazov. Vojny v Iraku a v Afganistane, ktoré sú poznačené najmä rozsiahlym používaním technológií bezpilotných lietadiel (dronov) na sledovanie a vyzbrojovanie.

---

26 ASHOURI Aida – BOWERS, Caleb – WARDEN, Cherrie. *An Overview of the Use of Digital Evidence in International Criminal Courts*, s. 121–123; TREVISAN, Stefano. *Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol*, s. 11.

27 MEHANDRU, Nikita – KOENIG, Alexa. *Icts, Social Media, & the Future of Human Rights*, s. 142–143.

Vďaka predmetnému použitiu dronov, ktoré môžu monitorovať po dlhšiu dobu ciele zhora s malým rizikom odhalenia, môžu viacerí vyšetrovatelia alebo dôstojníci v armáde sledovať rovnaký prenos a vykonávať dohľad bez zvýšenia rizika odhalenia. Ďalším argumentom pre ich používanie je skutočnosť, že drony môžu ísť tam, kam ľudia nemôžu, a teleobjektívy s vysokým rozlíšením na dronoch môžu obrázky zväčšiť, čo vyšetrovateľom umožní bližší pohľad na situáciu na zemi. Používanie dronov týmto spôsobom nielenže poskytuje živý prenos, ale sa tiež vytvára digitálny záznam záberov, ktorý je možné neskôr skontrolovať alebo dokonca použiť ako dôkaz na súde. V moderných konfliktných zónach je armáda vybavená rôznymi digitálnymi zariadeniami, ktoré poskytujú informácie o ich pohybe na zemi. Okrem toho civilisti používajú mobilné telefóny v konfliktných zónach a v ich okolí. Medzi satelitmi monitorujúcimi situáciu z vesmíru, dronmi pozorujúcimi situáciu zhora a osobami zaznamenávajúcimi situáciu na zemi je dostatok dát a záberov na zobrazenie moderných konfliktných situácií zo všetkých uhlov pohľadu a za každých okolností. Ak sudcovia potrebujú na základe informácií, ktoré majú k dispozícii, posúdiť, či niektoré činnosti vyšetrovateľov alebo dôstojníkov boli primerané, môžu namiesto spoliehania sa na svedectvá preskúmať zábery z bezpilotných lietadiel alebo mobilného telefónu.[28]

Technológia formuje ďalšiu generáciu listinných dôkazov pred súdom, ale ani takéto dôkazy nie sú bez chýb. Hoci digitálne dôkazy majú potenciál zmeniť verdikty prípadu, skepticizmus voči pravosti, stigma voči online zdrojom, nedostatok medzinárodných právnikov vyškolených v oblasti zhromažďovania a analýzy dôkazov z otvorených zdrojov, absencia etablovanej vedeckej komunity s dôveryhodnosťou na posúdenie takýchto dôkazov, bráni nevyhnutnému pokroku. Právnici a vyšetrovatelia nemusia byť reakční, ale musia sa dostať dopredu, budú sa musieť pozerať do budúcnosti a premýšľať o tom, ako môžu sami inovovať a využívať nové technológie pre svoju prácu. Kybernetická alebo digitálna forenzná analýza, podľa viacerých autorov ako doména zhromažďovania a analýzy elektronických dôkazov, sa bude naďalej transformovať a bude predstavovať výzvu; ako disciplína musí predvídať a vyvíjať sa s rýchlymi zmenami v technológii a legislatíve, ak má aj naďalej slúžiť svojmu najvyššiemu účelu, ktorým je hľadanie pravdy.[29]

Zvýšené spoliehanie sa na digitálnu technológiu v každom jednotlivom aspekte nášho života je nevyvrátiteľným faktom. Nebola by to hyperbolická predpoveď, ak by sa dalo predpokladať, že v priebehu času budeme k nej neoddeliteľne pripútaní. Žijeme v ére, ktorá je na čele technologických revolúcií, avšak na všeobecné akceptovanie neobmedzenej závislosti od digitalizácie sa treba pozerať s istou mierou obáv. Niektorí autori vyjadrujú rastúce obavy týkajúce sa negatívnych vplyvov prijímania digitálnych dôkazov. Medzinárodné spoločenstvo sa podľa nich nemôže uchýliť k svojmu „tunelovému videniu" zabezpečenia záujmov spravodlivosti spôsobom, ktorým práva obhajoby (medzi ktoré patrí aj právo na súkromie) ustupujú do úzadia. Z toho dôvodu je potrebné zaujať štruktúrovaný,

---

28 FREEMAN, Lindsay. *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, s. 329–331.

29 MEHANDRU, Nikita – KOENIG, Alexa. Open Source Evidence and the International Criminal Court. In: *Harvard Human Rights Journal* [online]. 15. 4. 2019 [cit. 2021-12-27]. Dostupné z: <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/>; FREEMAN, Lindsay. *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, s. 332–335; LOSAVIO, Michael Martin – PASTUKOV, Pavel – POLYAKOVA, Svetlana et al. The juridical sphere for digital forensics and electronic evidence in the insecure electronic world. *WIREs Forensic Science*. 2019, 1:e1337, s. 10. Dostupné z: <https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wfs2.1337>.

opatrný prístup pri presadzovaní výhod rýchleho prijatia technologických inovácií v rámci oblasti medzinárodného trestného práva.[30]

Na druhej strane názorového spektra, viacerí autori zastávajú názor, že digitálne dôkazy zvyšujú dôveryhodnosť a poskytujú viac príležitostí vyšetrovaniam, ktoré vedie Medzinárodný trestný súd. Prínosy tiež prinášajú obrovské výzvy s rôznymi vrstvami v každom kroku životného cyklu digitálnych dôkazov od fázy zberu až po ich hodnotenie súdom. Rovnako nevynímajúc ani ťažkosti s medzinárodnou spoluprácou, technologická náročnosť a neistota právnych noriem sú hlavnými problémami, ktorým čelia vyšetrovania Medzinárodného trestného súdu, ktoré je potrebné riešiť. Ako už bolo zdôraznené, takéto výzvy nie je ľahké vyriešiť bez globálneho prístupu založeného na spolupráci, ktorý si vyžaduje konsenzus o stanovení noriem, posilnenie spolupráce a organizované úsilie o nájdenie technických riešení. Najdôležitejšie je partnerstvo a angažovanosť medzi rôznymi stranami s cieľom dosiahnuť dohodu a zosúladené úsilie. Toto úsilie prispeje k výraznému zlepšeniu medzinárodnej výmeny digitálnych dôkazov a nakoniec k dosiahnutiu poslania Medzinárodného trestného súdu ukončiť beztrestnosť najzávažnejších zločinov proti ľudským právam.[31]

Záver

Používanie nových technológií v oblasti trestného stíhania najzávažnejších trestných činov týkajúce sa medzinárodného spoločenstva je rovnako na začiatku ako samotná oblasť. Zatiaľ čo nové technológie využívajú internacionalizované inštitúcie, existuje priestor na rozšírenie ich použitia tak v rámci Medzinárodného trestného súdu, ako aj mimo neho pri iných (medzi)národných súdov, ale to predstavuje proces, ktorý si vyžaduje (a mal by trvať) určitý čas. Hoci takéto nové technológie môžu mať vplyv na formovanie budúcnosti nielen medzinárodného trestného súdnictva, je potrebné si zvážiť zreteľné výhody, ktoré ponúka ich používanie.[32]

Pojem „digitálny dôkaz" možno, vzhľadom na vyššie uvedené vymedzenia, vo všeobecnosti definovať ako akékoľvek dáta, ktoré sú vytvárané, manipulované, uchovávané alebo prenášané prostredníctvom alebo akýmkoľvek digitálnym zariadením, či už počítačom alebo počítačovým systémom, alebo prostredníctvom informačno-komunikačných technológií, a ktoré sú relevantné pre súdne konanie.

Pokiaľ ide o prípustnosť digitálnych dôkazov, prístup väčšiny medzinárodných trestných súdov je zhovievavý. Vo všeobecnosti ich možno pripustiť, pokiaľ sú relevantné a majú dôkaznú hodnotu. Autentifikácia, pôvod a uchovávanie ovplyvňujú prípustnosť a dôkaznú váhu, ktorú sudcovia posudzujú podľa vlastného uváženia. Okrem toho medzinárodné trestné súdy musia zabezpečiť, aby sa s predloženými dôkazmi nemanipulovalo, ani sa neupravovali, aby sa zachovala a zistila ich autentickosť, ktorá vzhľadom na ich

30 NARAYANAN, Aparajitha. *Evidentiary Challenges of New Technologies in International Criminal Trials*, s. 71–72.

31 HONG, Ilyoung. International Digital Forensic Investigation at the ICC. In: BIASIOTTI, Maria Angela – MIFSUD BONNICI, Jeanne Pia – CANNATACI, Joe – TURCHI, Fabrizio (eds). *Handling and Exchanging Electronic Evidence Across Europe*, s. 138.

32 BERGSMO, Morten – BEKOU, Olympia – JONES, Annika. New Technologies in Criminal Justice for Core International Crimes: The ICC Legal Tools Project. *Human Rights Law Review*. 2010, Vol. 10, Iss. 4, s. 729. Dostupné z: <https://corteidh.or.cr/tablas/r26543.pdf>.

ľahkú manipuláciu je obzvlášť dôležitá. V prípadoch, keď má podporné svedectvo nízku kvalitu, môže to ovplyvniť pravosť predmetných digitálnych dôkazov natoľko, že súd nemusí považovať dôkazy za prípustné. S cieľom určiť overenie digitálneho dôkazu, medzinárodné súdy často skúmali históriu držby a úprav predmetného údaju alebo pôvod dôkazov. Preto podľa viacerých autorov je dôležité, aby (meta)dáta, ktoré môžu pomôcť overiť históriu úprav digitálnych dôkazov, boli spoľahlivo uchovávané.[33] Hoci čl. 69 ods. 4 Rímskeho štatútu ustanovuje pravidlo voľného uváženia, ods. 7 stanovuje kogentné pravidlo vylúčenia, ak sú splnené jeho podmienky. Na jednej strane ods. 4 vytvára flexibilnú rovnováhu, v ktorej možno porovnávať rôzne faktory s dôkaznou hodnotou dôkazov. Na druhej strane ods. 7 osobitne upravuje konkrétne predikatívne udalosti týkajúce sa spôsobu zhromažďovania dôkazov a škodlivých účinkov na proces, ktoré, ak sa preukážu, odôvodňujú ich vylúčenie. Určenie existencie týchto predikatívnych udalostí alebo účinkov si však vyžaduje posúdenie, a tým aj voľnú úvahu súdu.[34]

Vzhľadom na množstvo digitálnych dôkazov a rastúcu závislosť na digitálnych dôkazoch pri medzinárodnom trestnom stíhaní je podľa viacerých autorov, s ktorým názorom sa stotožňujeme, možné, že v budúcnosti môžu byť digitálne dôkazy primárnym dôkazom, na ktorom budú založené niektoré odsúdenia. S touto novou možnosťou však prichádzajú aj sprievodné riziká, s ktorými sa medzinárodné trestné súdy budú musieť v budúcnosti vysporiadať, či už priamo ustanovením upravujúcim predmetnú problematiku alebo samotnou súdnou praxou a výkladom v judikatúre. V priebehu výskumu problematiky prípustnosti digitálnych dôkazov sme narazili na otázku použitia dôkazov z otvorených zdrojov (*open source evidence*) v medzinárodnom trestnom práve, ktorej sa budeme ďalej venovať, nakoľko predmetná téma je aktuálna a neustále sa rozvíjajúca.

33 *Report on Digitally Derived Evidence in International Criminal Law*, s. 41.

34 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*, s. 1747.

Digital Evidence in the International Criminal Law

Michal Klenka (https://orcid.org/0000-0002-3210-6884)

Abstract: The article addresses the fact that digital evidence is beginning to prevail and this represents not just a legal challenge for the international criminal justice system. The aim of this article is to analyse the existing legal framework governing evidence in international criminal law in the context of the use of digital evidence. The starting point is primarily the legal regulation of the International Criminal Court, but we have not forgotten other international criminal tribunals. The article not only deals with the very definition of "digital evidence", but also deals with the rules of admissibility and exclusion of evidence before the International Criminal Court (especially Article 69 (4) and (7) of the Rome Statute), as well as issues of relevance and admissibility of evidence in general. The subject of the examination is also the authentication and reliability of digital evidence, its probative value and, last but not least, the chain of custody of digital evidence. Finally, there is also some consideration of the future use of digital evidence and the potential risks that its admission and use in court proceedings entails.

Keywords: digital evidence, international criminal law, admissibility and exclusion of evidence, authentication of digital evidence, reliability of digital evidence, chain of custody of digital evidence