508—529

Digitálne dôkazy z otvorených zdrojov

Michal Klenka*

Abstrakt: Cieľom článku je priblíženie problematiky použitia informácií získaných z digitálnych otvorených zdrojov, slúžiacich ako dôkazy v konaniach týkajúcich sa porušení medzinárodného trestného práva, ľudských práv a medzinárodného humanitárneho práva. Okrem poskytnutia základných definícií a právnych otázok, ktoré je potrebné zodpovedať pred ďalším použitím takto získaných dôkazov, článok kriticky analyzuje rôzne aspekty, ktoré predmetný druh dôkazov otvára (noví aktéri, sprostredkovanosť, objektivita a subjektivita). Napriek ich jednoznačným výhodám využívania, netreba opomínať ani určité s tým spojené problematické otázky, výzvy, najmä z dôvodu, že digitálny formát umožňuje pomerne jednoduchú manipuláciu a falšovanie, ktoré v niektorých prípadoch predstavuje neodstrániteľnú prekážku pri zisťovaní autenticity dôkazu a jeho pôvodu. Pozornosť je rovnako zameraná na zraniteľné miesta pri používaní informácií zo sociálnych médií (objem vytváraného obsahu, jeho moderácia platformami a otázka metadát), nakoľko obsah, ktorý sa na nich objavuje, odráža nielen povahu súčasného vedenia medzinárodného alebo vnútroštátneho ozbrojeného konfliktu, ale aj dezinformácií, ktoré ovplyvňujú spoločnosť. Vzhľadom na rastúce množstvo hacknutých a uniknutých informácií vo verejnej doméne, článok sa v záverečnej časti zaoberá použiteľnosťou predmetných informácií ako dôkazov v súdnom konaní a rozoberá s tým súvisiace právno-etické otázky prípustnosti.

Kľúčové slová: medzinárodné trestné právo, digitálny dôkaz z otvorených zdrojov, sociálne média, hacknuté a uniknuté informácie, verejná doména

Úvod

Skúmanie konkrétnych prípadov Medzinárodného trestného súdu a súdnych rozhodnutí v priebehu času ilustruje meniacu sa povahu informácií z otvorených zdrojov, ktoré sú k dispozícii v prípadoch vojnových zločinov, zločinov proti ľudskosti a genocídy – od novín, rozhlasového vysielania a (mimo)vládnych správ až po príspevky na sociálnych sieťach a iný digitálny obsah na internete. Zdrojmi takéhoto obsahu sú neštátni aktéri (napr. komerčné satelitné snímky), používatelia (vrátane tých, ktorí prežili, ale aj samotní páchatelia), ktorých vytváraný obsah sa kvalitatívne aj kvantitatívne líši od analógových foriem. Vyšetrovania z otvorených zdrojov sú vyšetrovania, ktoré sa pri formálnom a systematickom vyšetrovaní údajného protiprávneho konania úplne alebo čiastočne opierajú o verejne dostupné informácie.

V období pred internetom boli otvorené zdroje obmedzené a zahŕňali predovšetkým tradičné rozhlasové a printové médiá a verejné záznamy, ktoré si na získanie prístupu vyžadovali cestu do knižnice, archívu alebo na iné fyzické miesto. S príchodom internetu a rozšírením mobilných komunikačných technológií sa rozsah otvorených zdrojov, ktoré sú k dispozícii na získavanie informácií, dramaticky rozšíril, čím vznikli nové výzvy vzhľadom na obrovský objem údajov a rýchlosť, akou sa digitálne informácie môžu zdieľať. V súčasnosti existuje aj oveľa viac možností na monitorovanie udalostí, ktoré sa odohrávajú v reálnom čase. V kontexte ich zhromažďovania si predmetné informácie vyžiadali nový pohľad na ich využívanie na nielen vojenské, politické a zahraničnopolitické účely,

* JUDr. Michal Klenka, PhD. Asistent sudkyne 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.

ale aj na podporu právnej zodpovednosti. Postupne sa obsah vytvorený v konfliktných zónach začal používať ako dôkaz v prípadoch vojnových zločinov na celom svete. Keď tento obsah začal zaplavovať internet, objavili sa nové možnosti prístupu k takýmto zdrojom a ich analýzy. S rastúcou túžbou a potrebou používať online informácie z otvorených zdrojov ako dôkazy v (medzi)národných trestných konaniach sa musí vyvíjať právo, ktoré bude riešiť zložitosť autentifikácie digitálneho obsahu. V konečnom dôsledku sú informácie získané z otvorených zdrojov nedostatočne využívaným zdrojom, ktorého význam rýchlo rastie.[1]

S rozvojom technológií sa neustále zavádzajú nové nástroje, ktoré menia povahu a dostupnosť dôkazov. Rozširovanie, prepojiteľnosť a možnosti zabudovaných kamier a mobilných zariadení s pripojením na internet (napr. geografické označovanie, časové značky), ktoré zaznamenávajú oveľa viac informácií o činnostiach a komunikácii ľudí ako kedykoľvek predtým, sa stávajú rozhodujúcimi pri vytváraní dôkazného základu pre medzinárodné trestné činy a menia spôsob, akým vyšetrovatelia a prokurátori zhromažďujú, hodnotia a predkladajú dôkazy súdu. Platí to najmä v medzinárodných trestných procesoch, v ktorých prokurátori musia predložiť rozsiahly a rôznorodý súbor dôkazov na preukázanie viacerých obvinení súvisiacich so zložitými konfliktmi. Úlohou prokurátora je predložiť dôkazy spôsobom, ktorý pomôže súdu posúdiť ich význam a pochopiť, ako zapadajú do širšieho príbehu.[2] Inovatívne prezentačné nástroje zase umožňujú rozšíriť a posilniť dôkaznú situáciu pridaním doplňujúcich údajov a vytvorením presvedčivých vizuálnych zobrazení môžu pomôcť určiť miesto činu a ukázať zmeny konkrétneho miesta v priebehu času (napr. vizualizácie pred a po bombardovaní nemocnice).

Medzinárodný trestný súd a iné medzinárodné trestné tribunály, na potvrdenie výpovedí svedkov a vyplnenie dôkazných medzier, čoraz častejšie zapájajú do svojich vyšetrovaní obsah z otvorených zdrojov. Kým ešte pred niekoľkými rokmi mala medzinárodná právna komunita problém s nedostatkom vizuálneho obsahu, dnes bude potrebné nájsť spôsob ako rozlíšiť a nájsť potrebné relevantné dôkazy v množstve vytváraného šumu. Náročným aspektom je ako spracovať objem údajov, a ktoré zároveň poskytujú dôveryhodné a užitočné informácie pre vyšetrovanie. Vzhľadom na ich objem, mnohé organizácie experimentujú s procesmi strojového učenia, ktoré pomáhajú lokalizovať, analyzovať a uchovávať mimoriadne veľké množstvo údajov. Výzvy sú však podobne objemné, od potreby dostatočného množstva trénovaných údajov (napr. na to, aby sa stroje naučili identifikovať určité druhy zbraní vo veľkých súboroch údajov videí alebo fotografií) až po vývoj algoritmov schopných nájsť užitočný obsah. Technológia by mala dostatočne využívať už

---

1 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*. Oxford University Press, 19 December 2019, s. 48–49; KOENIG, Alexa – FREEMAN, Lindsay. Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation. *Hastings Law Journal*. 2022, Vol. 73, Iss 5, s. 1237 [cit. 2022-08-02]. Dostupné z: <https://repository.uchastings.edu/hastings_law_journal/vol73/iss5/4>; KOENIG, Alexa – MCMAHON, Felimon – MEHANDRU, Nikita – SILLIMAN BHATTACHARJEE, Shikha. Open Source Fact-Finding in Preliminary Examinations. In: BERGSMO, Morten – STAHN, Carsten (eds). *Quality Control in Preliminary Examination: Volume 2*. Brussels: Torkel Opsahl Academic EPublisher, 2018, s. 682, 684, 691, 710.

2 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. 283–284 [cit. 2021-03-27]. Dostupné z: <https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1>; MEHANDRU, Nikita – KOENIG, Alexa. Icts, Social Media, & the Future of Human Rights. *Duke Law & Technology Review*. 2019, Vol. 17, No. 1, s. 129 [cit. 2021-03-27]. Dostupné z: <https://scholarship.law.duke.edu/dltr/vol17/iss1/5/>.

zhromaždené informácie o vyšetrovaní a zároveň by pri vyhľadávaní a zhromažďovaní nemala odhaľovať žiadne dôverné informácie. Nájdenie rovnováhy bude kľúčom k úspechu. Vyšetrovatelia sa začínajú úspešne pohybovať v tomto novom teréne a uznávajú, že budúcnosť zodpovednosti bude prepojená s technologickým pokrokom; posilňujú siete na zdieľanie digitálneho obsahu, začleňujú do praxe nových aktérov (napr. programátorov a dátových vedcov) a vyvíjajú nové metódy na zisťovanie a overovanie informácií online.[3]

Od roku 2016 došlo k pozorovateľnému a výraznému nárastu používania dôkazov zo sociálnych médií na medzinárodných a vnútroštátnych súdoch. Na Medzinárodnom trestnom súde pomohli satelitné snímky, videá a geolokalizačné údaje z internetu k odsúdeniu Ahmada Al-Faqi Al-Mahdiho[4] za vojnový zločin ničenia kultúrneho majetku, ako sú mešity a mauzóleá v Timbuktu v Mali. V prípade Jean-Pierra Bembu Gomba[5] a členov jeho právneho tímu za zneužitie výkonu spravodlivosti v súvislosti s manipuláciou so svedkami, obžaloba predložila fotografie z Facebooku, aby preukázala vzťahy medzi stranami údajnej korupčnej schémy. Nasledujúci rok Medzinárodný trestný súd vydal zatykač na líbyjského veliteľa Mahmúda Al-Werfalliho[6] pre tridsaťtri obvinení z vojnových zločinov vraždy, a to najmä na základe videí z popráv nájdených na sociálnych sieťach. V Nemecku, Fínsku a Švédsku boli obvinení migranti, žiadatelia o azyl alebo vracajúci sa zahraniční bojovníci, ktorí sa zúčastnili na bojoch v Iraku alebo v Sýrii. V každom prípade sa obžaloba spoliehala na elektronicky zaznamenané snímky a videá šírené prostredníctvom sociálnych médií ako na dôkazy, ktoré zabezpečia odsúdenie. Argumentácia v týchto vnútroštátnych prípadoch síce nie je záväzná v prípadoch Medzinárodného trestného súdu, ale podľa Freeman môže napriek tomu zohrávať dôležitú úlohu pri formovaní toho, ako sudcovia Medzinárodného trestného súdu budú v budúcnosti vykladať právo a rozhodovať o prípustnosti a váhe, ktorú možno pripísať dôkazom zo sociálnych médií. V modernej dobe sa priame dôkazy o trestných činoch môžu práve nachádzať na sociálnych médiách a iných otvorených zdrojoch, čo vyvoláva otázku: Aký postup sa vyžaduje a aký proces je žiadúci na autentifikáciu a overenie tohto obsahu, aby sa naň sudcovia mohli spoliehať ako napr. na dôkaz preukazujúci vinu v trestnom konaní?[7]

Berkeley protokol o vyšetrovaní digitálnych otvorených zdrojov[8] (ďalej len „Berkeley protokol“) vypracovalo Centrum pre ľudské práva Kalifornskej univerzity v Berkeley spolu

---

3 KOENIG, Alexa. “Half the Truth is Often a Great Lie”: Deep Fakes, Open Source Information, and International Criminal Law. *American Journal of International Law. AJIL Unbound* [online]. 2019, Vol. 113, s. 251–252 [cit. 2022-05-27]. Dostupné z: <https://doi.org/10.1017/aju.2019.47>; 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. 134–135.

4 *Prosecutor v Ahmad Al-Faqi Al-Mahdi (Judgment and Sentence)* ICC- 01/ 12- 01/ 15 (25 February 2016). Dostupné z: <https://www.icc-cpi.int/court-record/icc-01/12-01/15-171>.

5 *Prosecutor v Jean-Pierre Bemba Gombo*. Dostupné z: <https://www.icc-cpi.int/car/Bemba-et-al>.

6 *Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli (Warrant for Arrest)* ICC- 01/ 11- 01/ 17 (15 August 2017). Dostupné z: <https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2017_05031.PDF>.

7 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. 52–53.

8 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS – HUMAN RIGHTS CENTER AT THE UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW. *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Advance version. New York – Geneva, 2020. Dostupné z: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>, <https://humanrights.berkeley.edu/berkeley-protocol-digital-open-source-investigations>.

s Úradom vysokého komisára OSN pre ľudské práva s cieľom poskytnúť medzinárodné normy a usmernenia pre vyšetrovateľov v oblasti medzinárodnej trestnej justície a ľudských práv. Zavedenie konzistentných a merateľných noriem na podporu tejto multidisciplinárnej oblasti je prostriedkom profesionalizácie praxe predmetného vyšetrovania. V týchto zásadách sa uvádzajú minimálne právne a etické normy na vykonávanie účinného vyšetrovania z otvorených zdrojov (identifikácia, zhromažďovanie, uchovávanie, analýza a prezentácia).[9] Aj keď normy Berkeley protokolu nemajú právne záväzný charakter, mohli by harmonizovať postupy a metodiky vyšetrovania. Správna metodika pri zhromažďovaní a uchovávaní informácií z otvorených zdrojov s väčšou pravdepodobnosťou povedie k zisteniu prípustnosti a k udeleniu dôkaznej váhy. Zabezpečenie dostatočných a presných dôkazov o spáchaní trestných činov zostáva v medzinárodnom trestnom práve výzvou. Použitie digitálnych dôkazov z otvorených zdrojov sa môže ukázať ako cenná odpoveď na patové situácie vo vyšetrovaní v mnohých prípadoch. Reagujúc na prirodzené obavy týkajúce sa digitálnych informácií z otvorených zdrojov, ako sú zaujatosť alebo skreslenie, autenticita, spoľahlivosť a dôveryhodnosť, je Berkeley protokol podľa Stavrou cenným nástrojom na podporu úsilia vyšetrovateľov a na zabezpečenie prípustnosti tohto typu dôkazov v trestnom konaní. Napriek tomu, že sa dôkazy z otvorených zdrojov zavádzajú ako spôsob posilnenia dôkaznej situácie, je potrebné ich dôkladné preskúmanie v predsúdnom a súdnom konaní, aby sa rovnako zabezpečili práva obvinených a spravodlivosť konania.[10]

1. Definícia dôkazov z otvorených zdrojov

Otvorené zdroje informácií zahŕňajú verejne dostupné informácie, ktoré môže každý člen verejnosti sledovať (pokiaľ sú tieto procesy prístupné všetkým používateľom v jurisdikciách, v ktorých je prístup legálny, a pri prístupe k nim alebo ich prezeraní sa neporušuje ochrana súkromia alebo bezpečnosť), zakúpiť (prostredníctvom platených služieb, ktoré sú dostupné všetkým členom verejnosti, ale nie služby, ktoré obmedzujú prístup pre určité skupiny, napr. príslušníkov orgánov činných v trestnom konaní) alebo o ne požiadať (a získať verejné informácie od štátnych orgánov na základe zákonov o slobode informácií alebo o prístupe k informáciám) bez toho, aby sa vyžadovalo osobitné právne postavenie alebo išlo o neoprávnený prístup.[11]

---

9 *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, s. vii, 3; MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. Mapping the Use of Open Source Research in UN Human Rights Investigations. *Journal of Human Rights Practice*. 2022, Vol. 14, Iss 2, s. 2 [cit. 2022-06-01]. Dostupné z: <https://doi.org/10.1093/jhuman/huab059>; UN HUMAN RIGHTS OFFICE. *Berkeley Protocol gives guidance on using public digital info to fight for human rights*. 1. December 2020 [cit. 2023-01-29]. Dostupné z: <https://www.ohchr.org/en/stories/2020/12/berkeley-protocol-gives-guidance-using-public-digital-info-fight-human-rights>.

10 HUBLEY, Hillary. Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations. *International Criminal Law Review*. 2022, Vol. 22, Iss 5–6, s. 15 [cit. 2022-08-02]. Dostupné z: <https://doi.org/10.1163/15718123-bja10124>; 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/>.

11 *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, s. 3.

Digitálne informácie z otvorených zdrojov sú verejne dostupné informácie v digitálnom formáte, ktoré sa spravidla získavajú z internetu. Zahŕňajú údaje vytvorené používateľom i strojom a môžu zahŕňať napr. obsah zverejnený na sociálnych sieťach, dokumenty, obrázky, videá a zvukové záznamy na webových stránkach a platformách na zdieľanie informácií, satelitné snímky a údaje zverejnené vládou. Na internete rovnako rastie objem údajov, ktoré boli zverejnené bez súhlasu ich vlastníkov, ako sú informácie, ktoré boli hacknuté, unikli, ako následok odhalených bezpečnostných zraniteľností alebo ich zverejnila tretia strana bez náležitých povolení (napr. hackerské útoky sponzorované štátom, úniky údajov spoločností, anonymné zneužitia). Hoci sú tieto informácie verejne dostupné, preto ich teoreticky možno považovať za dôkaz z otvoreného zdroja, napriek tomu môžu existovať právne a etické obmedzenia pre určité typy ich konečného použitia. Okrem toho môžu byť digitálne informácie prístupné osobám so špecializovanými technickými zručnosťami a výcvikom, ktoré môžu získať prístup do sieti a k údajom, ktoré sú pre bežného človeka nedostupné alebo je nepravdepodobné, že by sa k nim dostal.

Spravodajské informácie z otvorených zdrojov sa vzťahujú na podkategóriu informácií z otvorených zdrojov, ktoré sa zhromažďujú a používajú na konkrétny účel podpory tvorby politiky a rozhodovania, najčastejšie vo vojenskom alebo politickom kontexte. Zatiaľ čo informácie z otvorených zdrojov zahŕňajú všetky verejne dostupné informácie, ktoré môže ktokoľvek legálne získať, spravodajské informácie z otvorených zdrojov sú podmnožinou týchto informácií, ktoré sa zhromažďujú, využívajú a včas šíria vhodnému publiku na účely riešenia konkrétnej spravodajskej požiadavky.

Dôkazy z otvorených zdrojov sú informácie z otvorených zdrojov s dôkaznou hodnotou, ktoré možno pripustiť na účely zistenia alebo overenia skutočností v súdnom konaní. Hoci využívanie informácií z otvorených zdrojov pri vyšetrovaní nie je novinkou, objem a rozmanitosť otvorených zdrojov sa rozšírili v dôsledku stále častejšieho využívania internetu a iných možností na výmenu informácií vrátane rozšírenia sociálnych médií. V súčasnosti môže každý jednotlivec s inteligentným telefónom a prístupom na internet vytvárať a šíriť digitálny obsah na celom svete, aj keď v rôznej kvalite, pravdivosti a transparentnosti. Zároveň môžu tvorcovia obsahu v súčasnosti relatívne ľahko šíriť dezinformácie a manipulovať s digitálnymi údajmi. Rastúci objem údajov a rýchlosť, akou sa tieto údaje prenášajú a zdieľajú, vytvorili nové príležitosti pre vyšetrovateľov na ich zhromažďovanie a analýzu.[12]

2. Právne otázky pri dôkazoch z otvorených zdrojov

Doposiaľ neexistuje žiadny konkrétny článok alebo ustanovenie, ktoré by bolo výslovne pre digitálne dôkazy, pod ktoré dôkazy z otvorených zdrojov zaraďujeme. To znamená, že musia spĺňať minimálny všeobecný štandard prípustnosti dôkazov, ktorý vyplýva z judikatúry Medzinárodného trestného súdu, z Rímskeho štatútu Medzinárodného trestného súdu[13] (ďalej len „Rímsky štatút"), z Pravidiel súdneho konania a vykonávania dôkazov Medzinárodného trestného súdu,[14] ako aj z Jednotného technického protokolu na posky-

12 Ibidem, s. 3–4, 6–8.

13 *Rome Statute of the International Criminal Court*. Dostupné z: <https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>.

14 *Rules of Procedure and Evidence*. Dostupné z: <https://www.icc-cpi.int/sites/default/files/Publications/Rules-of-Procedure-and-Evidence.pdf>.

tovanie dôkazov, informácií o svedkoch a obetiach v elektronickej podobe:[15] i) relevantnosť (dôkazy sú *prima facie* relevantné pre konanie); ii) dôkazná hodnota samotného dôkazu; iii) absencia potenciálneho škodlivého účinku (ak je to relevantné, je potrebné zvážiť dôkazovú hodnotu voči akémukoľvek potenciálnemu škodlivému účinku dôkazu pre konanie).[16]

V praxi sa väčšina dôkazov pripúšťa a otázky ohľadom dôkazov sa týkajú skôr ich dôkaznej váhy než ich prípustnosti, keďže väčšina relevantných informácií bude prijatá. Na jednej strane flexibilný dôkazný štandard Medzinárodného trestného súdu umožňuje prijať holistický prístup k hodnoteniu dôkazov. Na druhej strane má táto flexibilita za následok zakrytie tohto štandardu, nakoľko prebieha v hlavách sudcov, nie v písomnom rozhodnutí.[17] Medzinárodný trestný súd vyžaduje, aby boli ku všetkým predloženým dokumentom pripojené metadáta, ako aj dokumentácia preukazujúca históriu držby, totožnosť zdroja, pôvodného autora a informácie o príjemcovi, prípadne príslušnej organizácii autora a príjemcu, aby bolo možné preukázať ich pôvod a integritu (napr. že neboli upravené). Kvôli poddajnosti a pominuteľnosti digitálneho materiálu sú však takéto dôkazy obzvlášť citlivé na spochybňovanie pravosti, dokazovanie ktorej komplikujú anonymné a pseudonymné zdroje, chýbajúci pôvod a rozšírené dezinformácie, ktoré zahŕňajú všetko od skreslených obrázkov až po zavádzajúce správy. Od znalcov sa často vyžaduje, aby sa vyjadrili, aké informácie dôkaz poskytuje, v porovnaní s tým, čo je len vecou špekulácie. Súdy však majú diskrečnú právomoc vylúčiť dôkazy, ktoré sú získané nezákonne, v rozpore s právami obvineného alebo inými procesnými právami (napr. podvodom, nezákonným sledovaním, krádežou alebo mučením). Dôkazy z otvorených zdrojov môžu v tejto oblasti vyvolávať značné obavy, najmä ak sú podkladové informácie zostavené takým spôsobom, že sa zdajú byť pre prípad rozhodujúce; úpravy môžu mať podstatný vplyv na zjavnú vinu spôsobom, ktorý je problematický, pretože sa môže odchyľovať od objektívnej pravdy, ktorá je základom konkrétnej udalosti. Okrem toho, keďže predmetné vyšetrovanie pozostáva z relatívne nových metód, obhajoba (a súdy) nemusia mať potrebné odborné znalosti na to, aby primerane preskúmali, ako profesionálne a/alebo nestranne boli tieto metódy použité.[18] V záujme optimalizácie potenciálneho využitia informácií z otvorených zdrojov ako dôkazov je nevyhnutné, aby sa zhromažďovali systematicky, aby sa od začiatku vyšetrovania zvažovali dôkazné a procesné otázky a aby vyšetrovatelia prijali dodatočné opatrenia na zabezpečenie ich spoľahlivosti, nakoľko digitálne dôkazy vo všeobecnosti otvárajú množstvo otázok týkajúcich sa zhromažďovania, spracovania, uchovávania a forenznej analýzy.

V niektorých prípadoch môže byť dôkaz tzv. „samooverovací" (*self-authenticating*), napr. overený dokument alebo záznam s oficiálnym (obchodným) logom. V iných prípa-

15 *Unified Technical protocol ("E-court Protocol") for the provision of evidence, witness and victims information in electronic form*. Dostupné z: <https://www.icc-cpi.int/sites/default/files/RelatedRecords/CR2019_00267.PDF>.

16 KLENKA, Michal. Digitálne dôkazy v medzinárodnom trestnom práve. *Právník*. 2022, roč. 161, č. 9, s. 869–877.

17 HIATT, Keith. Open Source Evidence on Trial. In: *The Yale Law Journal Forum*, 2015–2016, Vol. 125, s. 327–329 [online]. 3. 3. 2016 [cit. 2021-12-22]. Dostupné z: <http://www.yalelawjournal.org/forum/open-source-evidence-on-trial>.

18 MEHANDRU, Nikita – KOENIG, Alexa. Open Source Evidence and the International Criminal Court. *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/>; *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, s. v; KOENIG, Alexa – FREEMAN, Lindsay. *Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation*, s. 1243–1244.

doch možno overenie pravosti dosiahnuť viacerými spôsobmi, ktoré zvyčajne zahŕňajú identifikáciu pôvodu dôkazu. Pokiaľ ide o digitálne dôkazy, autenticitu od momentu zhromaždenia až po predloženie na súde možno zabezpečiť pridelením *hash hodnoty*, ktorá preukazuje, že položka je jedinečná a nebolo s ňou manipulované. Tento postup však nezohľadňuje možnosť manipulácie medzi časom vytvorenia a časom zhromažďovania vyšetrovateľom. Digitálny obsah sa dá ľahko sfalšovať a sociálne médiá uľahčili rozsiahle šírenie dezinformácií, nesprávne priradených informácií, falzifikátov a podvrhov. Vyšetrovatelia preto musia pochopiť, ako a prečo ľudia komunikujú prostredníctvom rôznych platforiem, aké sú možnosti falšovania, botov a manipulácie, a ako sa môže líšiť pokrytie v závislosti od faktorov, ako sú napr. geografia, sociálny status a vek používateľa. V súčasnosti musia byť vyšetrovatelia viac ako kedykoľvek predtým skeptickí a opatrní, pokiaľ ide o to, na čo sa spoliehajú a aké závery vyvodzujú z verejne dostupných informácií. Ak sa zistí, že údaj je autentický, súd posúdi dôveryhodnosť zdroja a spoľahlivosť informácií alebo tvrdení v ňom uvedených. Overovanie teda často zahŕňa dvojstupňový proces: najprv sa hodnotí zdroj informácií a potom sa overuje ich obsah.[19]

3. Aspekty používania dôkazov z otvorených zdrojov

Odborníci identifikovali niekoľko kľúčových výhod používania digitálnych informácií z otvorených zdrojov pri vyšetrovaní. Hiatt dokonca vyjadril nádej, že nové technológie by mohli priniesť lepšie, lacnejšie a bezpečnejšie trestné konanie.[20] Avšak, je potrebné poukázať na názor McDermott, Koenig a Murray, ktorí uznávajú potenciálne významné výhody spojené s využívaním informácií z otvorených zdrojov a domnievajú sa, že táto forma získavania informácií a dôkazov by mala zohrávať kľúčovú úlohu v budúcich vyšetrovaniach. V ich článku zaznieva varovanie pred prehliadaním viacerých obmedzení, skreslení a slepých miest, ktoré môžu brániť užitočnosti takto získavaných informácií pri vyšetrovaní medzinárodných zločinov. Hoci je pravda, že tieto informácie možno použiť na poukázanie na potenciálne spáchanie medzinárodných trestných činov alebo na preukázanie prepojenia medzi kľúčovými aktérmi, na preukázanie viny vedúcich predstaviteľov a/alebo existencie plánu alebo politiky. Je potrebné poznamenať, že vo väčšine prípadov budú stále potrebné svedecké výpovede (najmä tzv. *insiderov* a *whistleblowerov*[21]), ako aj triangulácia informácií získaných z viacerých zdrojov, aby sa vytvoril zrozumiteľný a komplexný obraz situácie. Informácie z otvorených zdrojov by sa nemali považovať za všeliek a neexistujú ani vo vákuu. Okrem toho, hoci predmetné informácie majú napr. jednoznačne demokratizačný potenciál, existuje riziko, že náhlenie sa za väčším prijatím výskumných metód z otvorených zdrojov pri vyšetrovaní, môže neúmyselne umlčať niektoré z najviac marginalizovaných skupín obyvateľstva. Autori tvrdia, že digitálne infor-

19 DUBBERLEY, Sam – KOENIG, Alexa – MURRAY, Daragh (eds). *Digital Witness. Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, s. 63–65.

20 HIATT, Keith. *Open Source Evidence on Trial*, s. 324.

21 *Insider* je (spolupracujúca) osoba (ktorá je súčasťou určitej skupiny), v porovnaní s ostatnou verejnosťou, disponujúca rozsiahlejšími a kvalitnejšími informáciami (prostredníctvom svojich znalostí alebo vplyvu) ohľadom páchanej nezákonnej činnosti. *Whisteblower* alebo oznamovateľ kriminality alebo inej protispoločenskej činnosti je osoba (napr. súčasný alebo bývalý zamestnanec, zmluvný partner alebo dodávateľ súkromnej alebo verejnej organizácie), ktorá odhalí a v dobrej viere bez oprávnenia zdieľa (napr. novinárom) alebo oznámi (príslušnému orgánu) súkromné alebo utajované informácie súvisiace s činnosťou organizácie, ktorá sa považuje za nezákonnú, nemorálnu, nebezpečnú, podvodnú, alebo je v rozpore s verejným záujmom, alebo ide o pochybenia a nedbanlivosť ohrozujúcu verejnosť.

mácie z otvorených zdrojov môžu byť rovnako zraniteľné voči skresleniam ako akákoľvek iná forma dôkazov.[22] Cieľom kritického pohľadu nie je brániť rastúcemu využívaniu digitálnych informácií z otvorených zdrojov, ale skôr zabezpečiť, aby sa takéto informácie používali zodpovedne a efektívne. Znižovanie latky len preto, aby sa do prípadov zaviedli chybné zistenia a vyniesli zlé rozsudky, môže výrazne poškodiť dlhodobú dôveryhodnosť týchto techník a legitimitu právneho systému.[23] V nasledujúcej časti priblížime a kriticky zanalyzujeme rôzne aspekty, ktoré vyvstávajú používaním dôkazov z otvorených zdrojov.

3.1 Demokratizačný potenciál

Veľkou uznávanou výhodou je demokratizačný potenciál digitálnych dôkazov z otvorených zdrojov, keďže umožňujú prístup k oveľa širšiemu okruhu zdrojov a hlasov, než by sa za normálnych okolností získavali tradičnými metódami zhromažďovania informácií pre medzinárodné trestné vyšetrovanie. Ako poznamenali Dyer a Ivens, vyšetrovania *„môžu sústrediť skúsenosti skupín, ktorých hlasy sú príliš často silne sprostredkované, marginalizované alebo vylúčené z bežného spravodajstva“*.[24] Okrem toho, dokumentácia občanov o porušovaní ľudských práv zohráva dôležitú úlohu v súčasných procesoch zisťovania faktov, môže tiež pomôcť čeliť dezinformáciám a tzv. „popieračskej“ propagande všetkých aktérov zapojených do konfliktu vrátane mocností.[25]

Ako je vyššie uvedené, používanie dôkazov z otvorených zdrojov môže tiež umožniť vypočuť si viac perspektív a potenciálne posilniť inak marginalizované hlasy. Vlastnosťou, ktorá sa považuje za obzvlášť užitočnú, je, že môže presunúť kontrolu nad rozprávaním z rúk ľudskoprávnych odborníkov, investigatívnych novinárov alebo iných osôb a presunúť ju do rúk tých, ktorých sa porušovanie priamo dotýka. Ako poznamenala Hamilton, *„používateľmi vytvárané dôkazy by mohli „demokratizovať“ zhromažďovanie dôkazov presunutím rovnováhy kontroly z vonkajších odborníkov na miestnych ľudí“*.[26] Land poukazuje na to, že to môže znamenať, že *„tí, ktorí boli predtým ‚subjektmi‘ vyšetrovania ľudských práv, majú teraz potenciál byť samostatnými aktérmi“*.[27] Informácie z otvorených zdrojov znamenajú, že počujete nielen to, čo hovoria ľudskoprávne organizácie, ale máte prístup k hlasom, ktoré by ste inak nepočuli. Napriek tomuto demokratizačnému účinku však môže vzniknúť alebo už existuje nová kategória tzv. „digitálnych elít“, ktoré majú neprimeraný vplyv na sociálnych médiách, najmä na medzinárodné publikum.[28]

---

22 MCDERMOTT, Yvonne – KOENIG, Alexa – MURRAY, Daragh. Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations. *Journal of International Criminal Justice*. 2021, Vol. 19, Iss. 1, s. 4 [cit. 2021-07-23]. Dostupné z: <https://doi.org/10.1093/jicj/mqab006>.

23 KOENIG, Alexa – FREEMAN, Lindsay. *Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation*, s. 1238–1241.

24 DYER, Sophie – IVENS, Gabriela. What would a feminist open source investigation look like? *Digi War*. 2020, Vol. 1, Iss. 1–3, s. 5–17. Dostupné z: <https://doi.org/10.1057/s42984-020-00008-9>.

25 MCDERMOTT, Yvonne – KOENIG, Alexa – MURRAY, Daragh. *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, s. 1–3.

26 HAMILTON, Rebecca. User-Generated Evidence. *Columbia Journal of Transnational Law*. 2018, Vol. 57, Iss. 1, s. 1–61. Dostupné z: <http://dx.doi.org/10.2139/ssrn.3124409>.

27 LAND, Molly. Democratizing Human Rights Fact-Finding. In: ALSTON, Philip – KNUCKEY, Sarah (eds). *The Transformation of Human Rights Fact-Finding*. Oxford University Press, 2016.

28 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 9.

3.2 Sprostredkovaný prístup

Digitálne dôkazy z otvorených zdrojov poskytujú určitý prístup do konfliktných zón, do ktorých nie je možné sa fyzicky dostať z bezpečnostných, diplomatických alebo logistických dôvodov. Vyšetrovatelia nemusia cestovať a na prácu im postačia zariadenia pripojené na internet, mimo fyzických prekážok a nebezpečenstiev. Skutočnosť, že tento materiál možno získať na diaľku, do určitej miery rovnako pomáha chrániť svedkov, ktorí nemusia podstupovať riziko výpovede, nakoľko skutočnosti napr. o vzťahu medzi údajnými páchateľmi alebo o zničení kultúrneho majetku alebo o údajnom spáchaní trestných činov možno preukázať prostredníctvom overiteľných verejne dostupných informácií, ktoré sú čoraz častejšie k dispozícii bez nákladov alebo s nízkymi nákladmi.[29]

Keď tí, ktorí sú na mieste činu počas páchania zločinov alebo krátko po ňom, zaznamenávajú to, čo vidia, a dôkazy, ktoré by sa inak mohli stratiť alebo zničiť, sa naopak prostredníctvom ich digitalizácie zachovajú. Ich zapojenie sa do dokumentovania krutostí prostredníctvom videí a fotografií sa môže ukázať ako dvojsečná zbraň, keďže používaním tohto obsahu môžu vyšetrovatelia upútať neželanú pozornosť na očitých svedkov a ľudí, ktorí získavajú informácie z prvej ruky (napr. používateľ, ktorý nahral usvedčujúce video alebo náhodní svedkovia na fotografii), a tým ohroziť ich rodiny, prípadne celé komunity. Preto je rozhodujúce prijať opatrenia na zabezpečenie primeranej ochrany jednotlivcov a potenciálne riziká spojené s ukladaním a zverejňovaním tohto obsahu sa musia starostlivo určiť, aby sa predišlo odhaleniu totožnosti svedka alebo tretej strany. Dôležitá dilema pri spracúvaní údajov, ktoré sa zhromažďujú pri vyšetrovaniach z otvorených zdrojov, sa týka uchovávania veľkých súborov údajov, ktoré obsahujú množstvo digitálnych osobných informácií. Tento vývoj viedol k značným obavám o súkromie a ochranu údajov, ako aj o právo na spravodlivý proces.[30] Predmetné zhromažďovanie a spracúvanie na účely cielenej prevencie a vyšetrovania trestných činov predstavuje zákonnú výnimku z noriem ochrany údajov. Hromadné alebo necielené zhromažďovanie osobných údajov však nie, požiadavky nevyhnutnosti a primeranosti platia vždy.[31] Medzi ohrozené práva v súvislosti s takouto formou vyšetrovania patria: právo na súkromie, právo na život a slobodu pred mučením, neľudským alebo ponižujúcim zaobchádzaním, právo na slobodu a bezpečnosť, a samozrejme práva detí, ktoré si vyžadujú osobitnú náležitú starostlivosť.[32] Riziká sú nielen na strane svedkov, ale aj pri samotných tvorcoch obsahu, ako aj vyšetrovateľoch, všetky tieto osoby môžu byť terčom útokov, odplaty zo strany (ne)štátnych subjektov, rôznej formy kyberšikany (napr. *doxxingu* alebo *trollovania*) zo strany podporovateľov páchateľov.

---

29 MEHANDRU, Nikita – KOENIG, Alexa. *Icts, Social Media, & the Future of Human Rights*, s. 133; MCDERMOTT, Yvonne – KOENIG, Alexa – MURRAY, Daragh. *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, s. 324–325.

30 EIJKMAN, Quirine – WEGGEMANS, Daan. Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*. 2013, Vol. 23, Iss. 4, s. 291 [cit. 2022-08-03]. Dostupné z: <https://doi.org/10.1163/18750230-99900033>.

31 DE BUSSER, Els. Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You. *Groningen Journal of International Law*. 2014, Vol. 2, No. 2, s. 113 [cit. 2022-03-18]. Dostupné z: <https://ugp.rug.nl/GROJIL/article/view/31124/28431>.

32 DUBBERLEY, Sam – IVENS, Gabriela. *Outlining a Human-Rights Based Approach to Digital Open Source Investigations: A guide for human rights organisations and open source researchers*. Project Report. University of Essex, Human Rights, Big Data and Technology Project, 2022, s. 15–22 [cit. 2022-06-01]. Dostupné z: <http://repository.essex.ac.uk/32642/1/Outlining%20a%20Human-Rights%20Based%20Approach%20to%20Digital%20Open%20Source%20Investigations.pdf>.

Okrem toho je pravdepodobnosť získania a potenciálneho použitia dezinformácií nájdených online pomerne vysoká, preto je overenie tohto obsahu kľúčové. Medzi najčastejšie nástrahy informácií z otvorených zdrojov patrí nesprávne priradenie, inscenovanie a technická manipulácia. Nesprávna atribúcia sa vyskytuje často a zahŕňa úmyselnú alebo neúmyselnú recykláciu online obsahu s nesprávnym dátumom, časom alebo miestom. Vzhľadom na obrovské množstvo spôsobov, ako možno digitálny obsah pozmeniť, treba s informáciami pochádzajúcimi z otvorených zdrojov zaobchádzať opatrne, najmä ak sa používajú na preukázanie „pravdy" o tom, čo sa odohralo. „Pozemné overovanie pravdivosti" (*ground truthing*) teda potvrdenie presnosti analýzy otvorených zdrojov osobami priamo v konfliktnej zóne, a zapojenie sa do overovacích procesov, ktoré sa zameriavajú na analýzu zdrojov aj obsahu, zostáva kritickou zložkou zabezpečenia pravdivosti obsahu z otvorených zdrojov.[33] Podľa viacerých autorov vyšetrovanie z otvorených zdrojov nemôže nikdy poskytnúť úplný obraz o porušovaní ľudských práv na konkrétnom mieste a vyšetrovatelia musia mať na pamäti slepé miesta tohto vyšetrovania.[34] Predmetná skutočnosť predstavuje obmedzenosť a neúplnosť sprostredkovaných informácií.

3.3 Objektivita a skreslenosť obsahu

Ďalšou identifikovanou výhodou využívania digitálnych informácií z otvorených zdrojov pri vyšetrovaní medzinárodných trestných činov je ich relatívna objektivita, napr. na rozdiel od svedka (a napriek technickým obmedzeniam) satelitný snímok nemôže zabudnúť na významné skutočnosti, nesprávne si zapamätať kľúčové detaily alebo byť motivovaný vlastnými záujmami či lojalitou k určitej skupine.[35] Súčasne rastúca všadeprítomnosť takýchto informácií môže formovať a ovplyvňovať rozprávanie a vnímanie svedkov, ktoré sa objavuje, niekedy spôsobom, ktorý sa výrazne odchyľuje od prežitých skúseností.[36]

Najdôležitejšie informácie sa na prvý pohľad nemusia týkať samotných trestných činov, napr. kľúčovým dôkazom nemusí byť video zabíjania, ale satelitný snímok holého miesta, ktorý naznačuje masový hrob, alebo snímka dvoch fajčiacich ľudí, ktorá spája veliteľa s páchateľom na fronte. Použitie geopriestorových údajov na lokalizáciu udalostí v priestore a čase môže tiež zohrávať dôležitú úlohu pri potvrdzovaní alebo vyvracaní výpovedí svedkov. Na preukázanie existencie konkrétnych prvkov môžu napr. satelitné snímky z otvorených zdrojov ukázať pohyb obyvateľstva, umiestnenie vojsk, masové hroby alebo zničené dediny. Informácie o pohybe obyvateľstva možno použiť na podporu obvinenia z násilného presunu alebo deportácie, zatiaľ čo sledovanie umiestnenia a pohybu vojsk môže pomôcť preukázať, že podozrivá skupina sa nachádzala v oblasti, kde boli spáchané zločiny. Snímky možno taktiež použiť na zobrazenie príslušných štruktúr, osôb, uniforiem, vozidiel a zbraní, pričom všetky tieto údaje možno použiť ako identifikačné dôkazy

33 MEHANDRU, Nikita – KOENIG, Alexa. *Icts, Social Media, & the Future of Human Rights*, s. 134–135.

34 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 11–13.

35 MCDERMOTT, Yvonne – KOENIG, Alexa – MURRAY, Daragh. *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, s. 3–4.

36 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 13–14.

na preukázanie príslušnosti priamych páchateľov k určitej vojenskej skupine.[37] Podobne ich aktuálnosť môže poskytnúť úroveň prehľadu a podrobnosti, ktorá by inak nebola možná. Preskúmaním časových značiek príslušných príspevkov na sociálnych médiách môžu vyšetrovatelia zaradiť informácie do hrubého chronologického poradia a posúdiť, či výpoveď svedka potvrdzuje informácie o incidente, ktoré možno získať z digitálnych otvorených zdrojov. Videozáznamy z rôznych uhlov môžu zachytiť rôzne perspektívy v priebehu určitého časového obdobia a tiež môžu prekonať problémy s neúplnými alebo nepresnými spomienkami svedkov.[38] Častokrát poskytujú pohľad na okolnosti udalosti a miesto, ktoré môže niekomu uniknúť.

Osobitne dôležité pri používaní predmetných dôkazov je zvážiť tri kategórie skreslení. Prístupové skreslenie (*access bias*), ktoré súvisí s tým, kto má prístup k digitálnym nástrojom a kto nie, a teda čie perspektívy a skúsenosti sú a nie sú zastúpené online. Druhou je algoritmické skreslenie (*algorithmic bias*), ktoré sa týka programovania vyhľadávača a spôsobu, akým určuje, ktoré výsledky vyhľadávania sa majú používateľom zobrazovať. Vyšetrovatelia preto musia prijať proaktívne opatrenia na maximalizáciu neutrality výsledkov vyhľadávania. Konkrétne kľúčové slová a jazyky, ktoré používajú spolu s booleovskými operátormi nasadenými na prepojenie zdrojov a kľúčových slov, môžu tiež radikálne ovplyvniť výsledky. Tretiu kategóriu tvoria kognitívne skreslenia (*cognitive biases*) vyšetrovateľa, ktoré môžu ovplyvniť nielen to, ako a kde vyšetrovateľ vyhľadáva informácie, ale aj to, ako interpretuje výsledky, čo sa rozhodne zhromažďovať a uchovávať a čo neberie do úvahy.[39]

4. Zraniteľnosti pri používaní dôkazov zo sociálnych médií

Sociálne médiá – pojem vzťahujúci sa na webové stránky a aplikácie navrhnuté tak, aby umožnili ľuďom rýchlo, účinne a v reálnom čase zdieľať obsah. Ich hlavným zmyslom je tvorba digitálneho obsahu používateľmi, slogan YouTube znie *„Vysielajte sami“* (*Broadcast Yourself*), výzvu prijali ľudia na celom svete vrátane ľudí, ktorých životy sa odohrávajú v konfliktných zónach, medzi ktorých patria aj samotní páchatelia, nielen teroristi, ktorí svoje zločiny vysielajú na propagandistické a náborové účely. Obsah vytváraný používateľmi postupom času získava na význame, keďže sa stal aj veľmi silným nástrojom na informovanie o tom, čo sa deje na mieste. Výsledkom je nepretržitý prúd videí, ktoré dokumentujú páchané zločiny na miestach (napr. Ukrajina a Sýria). V dôsledku toho sa informácie z otvorených zdrojov pochádzajúce zo sociálnych médií stávajú čoraz dôležitejšími pri medzinárodných vyšetrovaniach trestných činov a so sebou prinášajú významné právne dôsledky a nútia vyšetrovateľov rozvíjať nové technické zručnosti a právnikov prehodnotiť procesné pravidlá, ktorými sa riadia vyšetrovacie činnosti.[40]

---

37 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. 59, 61, 63.

38 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 7, 9, 11.

39 KOENIG, Alexa – FREEMAN, Lindsay. *Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation*, s. 1241–1242.

40 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, Documenta-*

Na jednej strane dôležitým aspektom sociálnych médií je skutočnosť, že predstavujú celosvetovo dostupnú platformu a s miliónmi tvorcov obsahu online sa exponenciálne zvýšil počet digitálnych informácií (každú minútu sa na YouTube nahrá viac ako 500 hodín obsahu[41]), pričom ich spoľahlivosť sa zároveň stala neistejšou. Na druhej strane je zrejmé, že sociálne médiá boli, sú a budú inštrumentálne využívané ich používateľmi aj na nenávistnú propagandu a dezinformácie, prostredníctvom zdieľania poburujúcich príspevkov, falošných správ a nenávisti, čo viedlo k praktike rozsiahleho vymývania mozgov a indoktrinácií obyvateľstva, až k ich prejavov v reálnom živote. V súlade s tým vytvárajú atmosféru nenávisti a nepriateľstva a neustále ju živia, aby mohli sledovať svoje politické ciele na úkor medzinárodného mieru a bezpečnosti.[42]

Dobre známe problémy dezinformácií, manipulácie s obsahom a s tým súvisiaca nedôvera v digitálne informácie, najmä k obsahu sociálnych médií, predstavujú riziko, že budú brániť užitočnosti dôkazov z otvorených zdrojov, a to tak pre vyšetrovania, ako aj pre procesy zodpovednosti, ktoré môžu z týchto vyšetrovaní vyplynúť.[43] Jednou z výziev je, že takto získaný obsah môže vyvolávať otázky týkajúce sa pravdivosti, keďže metadáta sú často odstránené, preto sa nedajú použiť na potvrdenie dôležitých informácií o autorovi videa a nahrávajúcom, ako aj o čase, dátume a mieste natáčania. Nedostatok štandardizovaných formátov súborov alebo schém metadát v záznamových zariadeniach, platformách digitálnych médií a operačných systémoch znamená, že rovnaké pozorovanie údajov nahraných na dve rôzne platformy môže mať úplne odlišné metadáta.[44] Preto je nevyhnutné stanoviť normy týkajúce sa potvrdzovania a overovania, ktoré pomôžu maximalizovať dôkaznú váhu informácií získaných z otvorených zdrojov. Dôležité je uviesť, že opakované zdieľanie obsahu bráni možnosti identifikovať pravdivosť incidentu tým, že potenciálne zakrýva jeho zdroj.[45] Hoci je potrebné vyriešiť otázky spoľahlivosti, informácie sa považujú za cenné, najmä v počiatočnej fáze skúmania pri nasmerovaní vyšetrovania.

Platformy sociálnych médií odstraňovaním digitálneho obsahu sa snažia moderovať svoj priestor. Nie je prekvapením, že najväčšie riziko odstránenia hrozí obsahu s potenciálnou dôkaznou hodnotou, ktorý je skutočne škodlivý a deštruktívny, ale mohol by slúžiť ako cenný dôkaz v trestnom konaní. Odstraňovanie obsahu je jednou z foriem moderovania obsahu, na ktorú sa platformy často spoliehajú, najmä pokiaľ ide o extrémistický, násilný alebo explicitný obsah. Po odstránení tohto škodlivého obsahu, pokiaľ sa nezá-

tion, and Accountability, s. 49–52; BELHADJ ALI, Chiraz. International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media. *Groningen Journal of International Law*. 2021, Vol. 9, No. 1, s. 46 [cit. 2022-03-18]. Dostupné z: <https://ugp.rug.nl/GROJIL/article/view/37950/35540>.

41 Dostupné z: <https://blog.youtube/press/>.

42 BELHADJ ALI, Chiraz. *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, s. 43–44.

43 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 16–17.

44 DEUTCH, Jeff – HABAL, Hadi. The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms. *State Crime Journal*. 2018, Vol. 7, No. 1, s. 50 [cit. 2022-03-18]. Dostupné z: <https://doi.org/10.13169/statecrime.7.1.0046>.

45 MEHANDRU, Nikita – KOENIG, Alexa. *Open Source Evidence and the International Criminal Court*; KOENIG, Alexa – MCMAHON, Felimon – MEHANDRU, Nikita – SILLIMAN BHATTACHARJEE, Shikha. Open Source Fact-Finding in Preliminary Examinations. In: BERGSMO, Morten – STAHN, Carsten (eds). *Quality Control in Preliminary Examination: Volume 2*, s. 693–695.

visle nezachová alebo úspešne ho neobnoví žiadna zo strán, nemôže byť použitý v súdnom konaní. Moderovanie obsahu ovplyvňuje mnohé aspekty vyšetrovania vrátane toho, či sú k dispozícii dôkazy s potenciálnou dôkaznou hodnotou a ako dlho. Keďže súdy začínajú prijímať poznatky z týchto vyšetrovaní ako dôkazy, všetky zainteresované strany by si mali byť vedomé možnosti ich zmiznutia bez možnosti obnovy a svojich vlastných obmedzení pri zapojení sa do tohto problému bez jeho riešenia. Problémom pri odstraňovaní obsahu je však ohrozenie jeho potenciálnej dôkaznej hodnoty. Žiaľ ako uviedla Hubley, *„spoločnosti pôsobiace v oblasti sociálnych médií môžu odstraňovať obsah a aj ho odstraňujú, pričom neberú ohľad na jeho dôkaznú hodnotu. V skutočnosti si platformy dobre uvedomujú, čo robia, ale ‚pre niekoho extrémistická propaganda je pre iného dôkazom vojnového zločinu'.“*[46] Rozsiahla a dynamická povaha internetu a značný objem informácií, ktoré sa na ňom nachádzajú, spôsobujú, že digitálne vyšetrovanie je citlivé na viaceré výzvy týkajúce sa rozhodovacieho procesu vyšetrovateľa, najmä jeho určenia toho, čo je a čo nie je relevantné a čo sa rozhodne preskúmať a zhromaždiť. To sa stáva obzvlášť kritickým v prípadoch, keď boli relevantné informácie z internetu odstránené medzi časom udalosti a začiatkom vyšetrovania, napr. z dôvodu moderovania obsahu sociálnych médií alebo keď používateľ oľutoval svoj príspevok a vymazal ho.[47]

Existuje ďalší aspekt, ktorému sa venuje menej pozornosti, hoci jeho dôsledky sú rovnako významné pre budúcnosť nielen medzinárodného vyšetrovania. Konkrétne, digitálne dôkazy neprinášajú do systému len novú formu dôkazov, ale ako už bolo vyššie uvedené aj množstvo nových aktérov. Patria k nim aj technologické spoločnosti, ako napr. Google (dcérska spoločnosť Alphabet Inc.), ktorý vlastní YouTube alebo súkromné osoby (Elonovi Muskovi patriaci Twitter[48]), tieto platformy sa stali dôležitými úložiskami dôkazov nielen o vojnových zločinoch, pričom medzinárodné trestné vyšetrovanie nie je niečo, čo by niekedy zamýšľali alebo predpokladali, že sa do neho zapoja.[49] Vzhľadom na závažnosť a dôležitý charakter takýchto informácií sa možno len zamyslieť nad z toho vyplývajúcimi právnymi dôsledkami. Vynárajú sa úvahy o možnej zodpovednosti vedenia alebo vlastníkov za napomáhanie alebo uľahčovanie spáchania trestného činu podľa čl. 25 ods. 3 písm. c) Rímskeho štatútu. Iní môžu argumentovať, že sú vinní z nečinnosti, keďže nevykonávali žiadne monitorovanie alebo filtrovanie obsahu zobrazovaného na ich platformách. Je však zrejmé, že zavinenie na takýto postup je zložité preukázať vzhľadom na to, že v praxi je ťažké dokázať súvislosť medzi trestným činom a platformou sociálnych médií. Napriek tomu ide o aktuálnu tému, ktorou by sa medzinárodné spoločenstvo malo zaoberať.[50]

---

46 HUBLEY, Hillary. *Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations*, s. 2–4, 16.

47 KOENIG, Alexa – STOVER, Eric – CRITTENDEN, Camille – CODY, Stephen. *Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court*. Human Rights Center UC Berkeley School of Law, 2014, s. 6. Dostupné z: <https://humanrights.berkeley.edu/sites/default/files/publications/digital-fingerprints.pdf>.

48 CONGER, Kate – HIRSCH, Lauren. Elon Musk Completes $44 Billion Deal to Own Twitter. In: *The New York Times* [online]. 27. 10. 2022 [cit. 2022-11-14]. Dostupné z: <https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html>.

49 HAMILTON, Rebecca. Social Media Platforms in International Criminal Investigations. *Case Western Reserve Journal of International Law*. 2020, Vol. 52, Iss. 1, s. 213–223 [cit. 2021-07-23]. Dostupné z: <https://scholarlycommons.law.case.edu/jil/vol52/iss1/12>.

50 BELHADJ ALI, Chiraz. *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, s. 55–59.

Vyššie uvedené možno ukázať na prípade občianskej vojny v Sýrii, ktorá začala v roku 2011 a o ktorej je viac hodín digitálneho obsahu vytvoreného používateľmi, ako bolo hodín samotného konfliktu.[51] Keďže však zábery sú často explicitné, algoritmus môže omylom označiť obsah týkajúci sa porušovania ľudských práv ako porušujúci pravidla YouTube. Spoločnosť Google odstraňuje obrovské množstvo online videí, odkedy v júni 2017 oznámila, že bude používať strojové učenie na odhaľovanie extrémistického obsahu. Sýrsky archív[52] môže zachovať odstránené videá z YouTube, ak sa k nim dostane ako prvý a zálohuje ich do svojej databázy.[53] Rozsah dokumentácie sýrskeho konfliktu (zo strany Sýrskeho archívu) znamená, že anotovanie a overovanie skutočností a vytváranie zodpovednosti založenej na dôkazoch bude pokračovať aj roky po skončení konfliktu.[54] Na doplnenie možno uviesť, že model Sýrskeho archívu sa rozšíril aj na ďalšie konfliktné zóny, keďže jeho materská spoločnosť Mnemonic (založená v roku 2017) začala viesť archivačné iniciatívy aj pre Sudán, Jemen a Ukrajinu.[55] Ako píšu Hamilton a Freeman, *„prípad Ukrajiny by bol jedným z prvých a určite najvýznamnejších príkladov spoliehania sa obžaloby na dôkazy vytvorené používateľmi počas súdneho procesu, kde súd vyžaduje dôkaz bez dôvodných pochybností (podstatne vyšší štandard ako štandard tzv. „rozumných dôvodov domnievať sa“, ktorý sa vyžaduje na vydanie zatykača)“*.[56] Nie je to prvýkrát, čo sa Ukrajina stala testovacím priestorom pre používanie online príspevkov ako dôkazov o vojenských zločinoch. Spoločnosť Bellingcat,[57] ktorá je priekopníkom a popularizovala verejné využívanie spravodajských informácií z otvorených zdrojov, sa do popredia dostala vďaka vyšetrovaniu letu Malaysia Airlines MH17 z Amsterdamu do Kuala Lumpur, ktorý bol zostrelený nad Ukrajinou v roku 2014.[58]

Čoraz väčšie spoliehanie sa na digitálne dôkazy zo strany súdov posúva iniciatívu občianskej spoločnosti nad rámec iba pomenovania a dáva účinok jej snahám o verejné odsúdenie. Skutočnosť, že odhalenie na sociálnych sieťach má právne dôsledky, pomaly, ale isto udeľuje týmto dôkazom status „nevyhnutnej súčasti“, nakoľko orgány prišli do bodu, v ktorom je ignorovanie takýchto digitálnych dôkazov z pohľadu spoločnosti kontroverzné. Spoločnosť by totiž mohla vnímať vylúčenie týchto dôkazov ako nespravodlivé a ako nesprávny výkon spravodlivosti. V súlade s tým je ich používanie v tomto digitálnom kontexte nevyhnutné, a dokonca nutné na vyrovnanie sa s novou realitou. Napriek

51 GREENBERG, Andy. Google's New YouTube Analysis App Crowdsources War Reporting. In: *WIRED* [online]. 20. 4. 2016 [cit. 2022-11-14]. Dostupné z: <https://www.wired.com/2016/04/googles-youtube-montage-crowdsources-war-reporting/>.

52 *Syrian Archive*. Dostupné z: <https://syrianarchive.org/>.

53 O'FLAHERTY, Kate. YouTube keeps deleting evidence of Syrian chemical weapon attacks. In: *WIRED* [online]. 26. 6. 2018 [cit. 2022-11-14]. Dostupné z: <https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video>.

54 DEUTCH, Jeff – HABAL, Hadi. *The Syrian Archive: A Methodological Case Study of Open-Source Investigation of State Crime Using Video Evidence from Social Media Platforms*, s. 49–50, 73; HUBLEY, Hillary. *Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations*, s. 24.

55 *Mnemonic*. Dostupné z: <https://mnemonic.org/>.

56 HAMILTON, Rebecca – FREEMAN, Lindsay. The Int'l Criminal Court's Ukraine Investigation: A Test Case for User-Generated Evidence. In: *JUST SECURITY* [online]. 2. 3. 2022 [cit. 2022-11-14]. Dostupné z: <https://www.justsecurity.org/80404/the-intl-criminal-courts-ukraine-investigation-a-test-case-for-user-generated-evidence/>; KINSTLER, Linda. What Russia Is Doing to Ukraine Must Be Preserved—Not Just Seen. In: *WIRED* [online]. 3. 3. 2022 [cit. 2022-11-14]. Dostupné z: <https://www.wired.com/story/russia-ukraine-war-crimes-evidence-digital-media/>.

57 *Bellingcat*. Dostupné z: <https://www.bellingcat.com/>.

58 SIMONITE, Tom. The Race to Archive Social Posts That May Prove Russian War Crimes. In: *WIRED* [online]. 11. 4. 2022 [cit. 2022-11-14]. Dostupné z: <https://www.wired.com/story/open-source-russia-war-crimes-ukraine/>.

tomu je dôležité zdôrazniť, že aj keď sa dôkazy vytvorené používateľmi zdajú byť riešením veľkých procesných problémov, vyžadujú si prísnu reguláciu vzhľadom na riziká, ktoré prinášajú. Medzinárodný trestný súd napríklad prijal elektronický protokol, v ktorom špecifikuje opatrenia, ktoré prijíma *„na zabezpečenie autenticity, presnosti, dôvernosti a uchovávania záznamov o konaní"*. Okrem toho stanovuje požiadavky na formátovanie, obrazové a dátové štandardy a osobitný režim číslovania. Rovnako dôkazy získané zo sociálnych médií musia prejsť autentifikáciou s maximálnou opatrnosťou, aby sa zabezpečila legitímnosť údajov. Ak sa teda dôkladne regulujú a dôrazne zohľadňujú, dôkazy vytvárané používateľmi zmierňujú dôkazné bremeno. Navyše právo obvinených na spravodlivý proces je ďalším dôležitým bodom v jadre výkonu spravodlivosti, ktorý stojí za diskusiu. Ochrana tohto práva sa v digitálnej ére stáva zložitejšou, najmä vo vzťahu k rovnosti zbraní. Keďže pri zhromažďovaní týchto dôkazov sa pozornosť sústreďuje skôr na usvedčujúce než na ospravedlňujúce dôkazy. V súlade s tým vo väčšine prípadov slúžia tieto dôkazy výlučne obžalobe, čo vytvára jasný nepomer medzi oboma protistranami.[59] Okrem toho dôkazy vytvárané používateľmi môžu vytvárať prirodzené kognitívne skreslenia sudcov a prokurátorov, pretože grafický materiál môže byť veľmi presvedčivý a môže niesť ťažké dôsledky týkajúce sa ich úsudku.

5. Použiteľnosť hacknutých a uniknutých digitálnych dokumentov

Hoci definícia informácií z otvorených zdrojov je jednoduchá, existuje niekoľko kategórií informácií, ktoré patria do šedej zóny medzi súkromnými a verejnými – najmä rastúce množstvo nelegálne hacknutých a uniknutých informácií na internete. Na objasnenie, hacknuté informácie sú informácie získané cudzou osobou, ktorá k nim získa neoprávnený prístup, zatiaľ čo uniknuté informácie sú informácie získané osobou, ktorá má k nim oprávnený prístup, ale zdieľa ich neoprávneným spôsobom. Úniky informácií online, či už sú výsledkom hackerského útoku alebo whistleblowingu, zodpovedajú definícii informácií z otvorených zdrojov. Napriek tomu je vo svojej podstate niečo iné, ak ide o informácie vo verejnej doméne, ktoré neboli určené na zverejnenie. Na jednej strane by sa nemal odmeňovať nezákonný spôsob ich získania a zároveň by nezákonné činy, ktoré sú v dokumentoch odhalené, nemali zostať nepotrestané. Verejný záujem môže byť obojstranný.[60]

Pokrok v informačných technológiách a možnosť prístupu k údajom, či už legálne alebo nelegálne spôsobujú, že bude nevyhnutné, aby súdy hodnotili nezákonne získané dôkazy. Žiaľ, otázka, ako by mali súdy rozhodovať, keď budú čeliť takýmto otázkam, nie je ani zďaleka jasná. Zdá sa, že prístup všeobecnej prípustnosti takýchto dôkazov nezniesol ani kontrolu v minulosti, ani neobstojí v dnešnom tempe kybernetických útokov, únikov informácií a iných zásahov do suverénnych sfér. S rozšírením WikiLeaks a podobných webových stránok došlo k výraznému nárastu počtu strán, ktoré sa snažia predložiť dôkazy, ktoré boli získané nezákonným spôsobom. Tento problém však nie je nový, keďže

59 BELHADJ ALI, Chiraz. *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, s. 48–50.

60 FREEMAN, Lindsay. Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases. *UCLA Journal of International Law and Foreign Affairs*. 2021, Vol. 25, Iss. 2, s. 45–47 [cit. 2022-03-18]. Dostupné z: <https://escholarship.org/uc/item/5b87861x>.

prvým príkladom medzinárodného súdu zaoberajúceho sa nezákonne získanými dôkazmi je prípad Korfský prieplav. Z predmetného rozhodnutia možno vyvodiť záver, že aj keď sa dôkazy získajú nezákonne, v rozpore s medzinárodným právom, takéto dôkazy sa nebudú automaticky považovať za neprípustné a súd sa o ne môže opierať.[61] Medzinárodný súdny dvor sa v predmetnom prípade nezaoberal prípustnosťou takýchto dôkazov, nestanovil ani všeobecné pravidlo o neprípustnosti. Okrem toho, hoci Medzinárodný súdny dvor mohol vo veci Diplomatický a konzulárny personál USA v Teheráne[62] naznačiť, že dôkazy získané nezákonným spôsobom by nemali byť prípustné, nikdy nevyjadril, že by sa to malo považovať za pravidlo. Medzinárodný súdny dvor sa konkrétne nezaoberal (ne)prípustnosťou dokumentov, ktoré by pravdepodobne mali byť dôkazom údajného protiprávneho konania USA vo vnútroštátnych záležitostiach Iránu, ktorý sa ich nesnažil použiť, keďže sa na súdnom konaní nezúčastnil. Zo znenia rozhodnutia však vyplýva, že súd by nepripustil dôkazy získané v rozpore s mnohými medzinárodnými dohovormi.[63]

Senát Špeciálneho tribunálu pre Libanon vo veci *Ayyash a i*.[64] priamo analyzoval otázku nezákonne získaných dôkazov. Čl. 162 Pravidiel súdneho konania a vykonávania dôkazov libanonského tribunálu výslovne povoľuje vylúčenie dôkazov získaných metódami, ktoré môžu spochybniť ich spoľahlivosť alebo poškodiť integritu konania: *„žiadny dôkaz nie je prípustný, ak bol získaný metódami, ktoré podstatne spochybňujú jeho spoľahlivosť, alebo ak by jeho prijatie bolo v rozpore s integritou konania a vážne by ju poškodilo“*, a dodáva, že najmä sa vylúčia dôkazy, ak boli získané v rozpore s medzinárodnými normami v oblasti ľudských práv vrátane zákazu mučenia (čl. 15 Dohovoru proti mučeniu). K ďalším relevantným ustanoveniam patrí čl. 149 (C), podľa ktorého môže senát prijať dôkazy, *„o ktorých sa domnieva, že majú dôkaznú hodnotu“*, čl. 149 (D), ktorý umožňuje vylúčiť dôkazy, ak *„ich dôkazná hodnota je podstatne prevážená potrebou zabezpečiť spravodlivý proces“*, a čl. 149 (E), podľa ktorého môže senát *„požiadať o overenie pravosti dôkazov získaných mimo súdu“*. Senát dospel k záveru, že dokumenty WikiLeaks *„nemajú potrebné prima facie znaky spoľahlivosti (konkrétne pravosť a presnosť) na prijatie ako dôkaz“*. Vylúčenie únikov na základe ich (nedostatočnej) dôkaznej hodnoty súdom odhaľuje potenciálnu alternatívu k vylúčeniu na základe nezákonnosti.[65]

---

61 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*. Dostupné z: <https://www.icj-cij.org/en/case/1>.

62 *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*. Dostupné z: <https://www.icj-cij.org/en/case/64>.

63 BLAIR, Cherie – VIDAK GOJKOVIĆ, Ema. WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence. *ICSID Review – Foreign Investment Law Journal*. 2018, Vol. 33, Iss. 1, s. 237, 241–242 [cit. 2022-05-31]. Dostupné z: <https://doi.org/10.1093/icsidreview/six030>; ASHFORD, Peter. The Admissibility of Illegally Obtained Evidence. *Arbitration: The International Journal of Arbitration, Mediation and Dispute Management*. 2020, Vol. 86, Iss. 4, s. 377, 384 [cit. 2022-05-31]. Dostupné z: <https://kluwerlawonline.com/journalarticle/Arbitration:+The+International+Journal+of+Arbitration,+Mediation+and+Dispute+Management/85.4/AMDM2019048>; MANSOUR FALLAH, Sara. The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals. *The Law & Practice of International Courts and Tribunals*. 2020, Vol. 19, Iss. 2, s. 148, 156–157 [cit. 2022-05-31]. Dostupné z: <https://doi.org/10.1163/15718034-12341420>.

64 Decision on the Admissibility of Documents Published on the WikiLeaks Website STL-11-01/T/TC (21 May 2015).

65 BLAIR, Cherie – VIDAK GOJKOVIĆ, Ema. *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evid*, s. 242–243; MANSOUR FALLAH, Sara. *The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals*, s. 151–154, 161–162.

Na rozdiel od libanonského tribunálu Súdny dvor Európskej únie výslovne povolil prijatie dokumentov WikiLeaks ako dôkazu, pričom zdôraznil „čisté ruky" strany, ktorá sa na takýto dôkaz odvolávala. Rozhodol v prospech žalobcu, pričom sa odvolal na vec Dalmine proti Komisii, v ktorej uviedol, že *„všeobecnou zásadou práva Spoločenstva je voľné hodnotenie dôkazov"*, a pokračoval, že *„jediným rozhodujúcim kritériom pri tomto hodnotení dôkazov je ich vierohodnosť"*.[66] Okrem toho *„predmetné dôkazy boli relatívne dôveryhodné, keďže ich pravosť vláda Spojených štátov* [amerických] *nespochybnila"*.[67] Hoci Európsky súd pre ľudské práva výslovne nerozhodol o prípustnosti príslušných dokumentov WikiLeaks, ale ani nenaznačil, že by sa takéto dôkazy mali považovať za neprípustné.[68] Napriek tomu, že ich judikatúra nie je záväzná, možno sa na ňu odvolávať v rozsudkoch Medzinárodného trestného súdu podľa čl. 21 ods. 1 písm. b) Rímskeho štatútu.[69]

V mnohých prípadoch boli informácie obsiahnuté v uniknutých dokumentoch použité v rôznych vyšetrovaniach. Najmä uniknuté informácie od vládnych predstaviteľov zohrali ústrednú úlohu pri objasňovaní skutočnosti a vyvodzovaní zodpovednosti za zneužívanie moci a porušovanie zákona, ktoré by inak zostali nepotrestané. Vládne a vojenské dokumenty tradične zohrávajú kľúčovú úlohu pri zisťovaní ťažko dokázateľných prvkov trestných činov, ako sú znalosť alebo úmysel páchateľa (napr. pri dokazovaní spojenia medzi vysokopostaveným vojenským veliteľom a činmi jeho jednotiek v teréne zohráva kľúčovú úlohu súkromná vojenská komunikácia). Interné komunikácie sú často jediným priamym dôkazom organizačného „plánu alebo politiky", čo je kontextový prvok zločinov proti ľudskosti, ktorý môže byť náročné dokázať bez dôvodných pochybností len na základe nepriamych dôkazov. Uniknuté vojnové denníky z Iraku a Afganistanu nielenže odhalili porušenia zákona (napr. neoprávnené zabíjanie civilistov príslušníkmi armády), ale odhalili aj to, že osoby na najvyšších miestach velenia o týchto porušeniach vedeli. Obsahovali dôkazy o zločinoch a dôkazy o ich krytí, sú stále dostupné na WikiLeaks a určite budú relevantné pre prípady Medzinárodného trestného súdu. Očakáva sa však, že ak sa prípad dostane pred súd, prípustnosť dôkazov z WikiLeaks bude dôrazne spochybnená.

Hoci existuje precedens, keď sa uniknuté dokumenty od whistleblowerov používajú ako dôkaz o nesprávnom postupe vlády, situácia je komplikovanejšia, keď sú fakty opačné. Hacky sponzorované štátom (pri ktorých sa súkromným subjektom ukradnú emaily a iné údaje a zverejnia sa online), úniky firemných údajov (pri ktorých sa zverejnia online osobné údaje používateľov, ktoré má tretia strana) a anonymné zneužitia (politicky alebo spoločensky motivované hacky, ktoré sa zameriavajú na konkrétne subjekty a zverejňujú ich informácie online) sa nemusia zdať bezprostredne relevantné pre medzinárodné trestné vyšetrovanie, ale určite by sa za určitých okolností mohli ukázať ako relevantné, keďže vojnoví zločinci a skorumpovaní vládni predstavitelia využívajú aj tieto služby. Obsah súborov NSA (informácie zhromaždené v rámci programov masového sledovania) alebo

---

66 *Dalmine SpA proti Komisii Európskych spoločenstiev*. Vec T-50/00 *Dalmine/Komisia*. Rozsudok Súdu prvého stupňa (druhá komora) z 8. júla 2004, bod 72. ECLI:EU:T:2004:220 [online] [cit. 2022-11-25].

67 *Persia International Bank plc proti Rade Európskej únie*. Vec T-493/10 *Persia International Bank/Rada*. Rozsudok Všeobecného súdu (štvrtá komora) zo 6. septembra 2013, bod 95. ECLI:EU:T:2013:398 [online] [cit. 2022-11-25].

68 Bližšie napr. rozsudky Európskeho súdu pre ľudské práva vo veci *El-Masri proti Severnému Macedónsku* z 13. decembra 2012 (č. 39630/09), a vo veci *Al Nashiri proti Poľsku* z 24. júla 2014 (č. 28761/11).

69 BLAIR, Cherie – VIDAK GOJKOVIĆ, Ema. *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evid*, s. 243–246; FREEMAN, Lindsay. *Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases*, s. 55–57.

Panama Papers (interná komunikácia, obchodné záznamy, zmluvy) a ďalšie môžu byť tiež relevantnými údajmi, ktoré majú vyšetrovaciu alebo dôkaznú hodnotu v medzinárodných trestných veciach vrátane tých, ktoré patria do právomoci Medzinárodného trestného súdu. Tieto uvedené príklady poukazujú aj na etické dilemy týkajúce sa toho, či a ako možno tieto informácie použiť. Uniknuté dokumenty z hackerských útokov autoritárskych vlád a spoločností, s ktorými obchodujú, môžu obsahovať užitočné informácie. Ich použitie ako dôkazov na súde by však mohlo vytvoriť zlý precedens pre použitie iných hacknutých údajov, napr. osobných údajov súkromných osôb.[70]

Dôležitou koncepčnou otázkou, ktorá sa objavuje v niektorých prípadoch, je, či je relevantné, kto získal dôkaz nezákonne a kto ho používa na súde. Prvou situáciou by bola situácia, keď informácie získala nezákonne tretia nezainteresovaná osoba („*ktorá nie je účastníkom konania a nemá z jeho výsledku žiadny prospech ani stratu*"),[71] dostali sa na verejnosť, sú verejne dostupné pred konaním a následne ich v konaní použila strana; bolo by možné argumentovať, že takýto dôkaz by sa mal považovať za *prima facie* prípustný, aj keď bol pôvodne získaný nezákonným konaním. Druhou situáciou relevantnou pre takýto druh vyšetrovania by bola situácia, keď dôkaz síce nebol verejne dostupný, ale napriek tomu ho získal niekto iný ako strana, ktorá ho použila. Umožniť účastníkovi konania opierať sa o dôkaz, ktorý tento účastník získal nezákonným spôsobom, by bolo v rozpore so zásadou *ex turpi causa non oritur actio* (právo nemôže vyplývať z protiprávneho konania).[72]

Digitálny dokument sa dá relatívne ľahko zmeniť a takéto zmeny je často ťažké odhaliť. Preto je v prípade uniknutých digitálnych dokumentov stanovenie ich pravosti náročné, keďže neexistuje jasný systém kontroly pôvodu od zdroja dokumentov až po ich zverejnenie na internete, čím vzniká priestor, počas ktorého by mohli byť zmenené. Okrem toho by uniknuté digitálne dokumenty mohli byť úplne sfalšované. Táto výzva sa so zavedením syntetických médií (digitálny obsah generovaný pomocou umelej inteligencie) len zvýši, pretože bude rýchlejšie, jednoduchšie a lacnejšie vytvárať presvedčivé falzifikáty. Pre každý digitálny dôkaz získaný z internetu, a nie z priameho zdroja, sa musí vytvoriť základ pravosti, pretože anonymita internetu a poddajnosť digitálneho média ho robia obzvlášť náchylným na falšovanie. To platí pre všetky typy digitálnych informácií z otvorených zdrojov a únikov, ktoré nemajú pôvod alebo jasný systém kontroly pôvodu. Hoci je často nemožné s absolútnou istotou určiť pravosť dokumentov bez originálov, možno použiť rôzne informácie na preukázanie neautentičnosti dokumentov alebo na spochybnenie pravosti dokumentov. Napríklad predložením ďalších dôkazov na overenie pravosti dokumentov, ako sú výpovede svedkov s priamou znalosťou alebo získanie originálnych verzií dokumentov priamo zo zdroja. Ak to nie je možné, musia sa pred ich prijatím prijať dodatočné opatrenia na získanie potvrdzujúcich informácií na určenie pravosti (napr. znalec vykonávajúci forenznú analýzu). Ďalším problémom je, keď sa v procese získavania

70 FREEMAN, Lindsay. *Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases*, s. 49–50, 53–70.

71 Case Concerning Military and Paramilitary Activities In and Against Nicaragua (*Nicaragua v United States of America*) (Merits) [1986] ICJ Rep 392 para 69.

72 MANSOUR FALLAH, Sara. *The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals*, s. 163, 176; BLAIR, Cherie – VIDAK GOJKOVIĆ, Ema. *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evid*, s. 256–258.

dôkazov poruší právo na súkromie, pričom do takéhoto práva možno zasiahnuť len „v súlade so zákonom“ a súd musí posúdiť, aký vplyv má porušenie súkromia na spoľahlivosť dôkazov alebo spravodlivosť konania.[73]

Keď hovoríme o uniknutých dokumentoch, ktoré obsahujú utajované alebo citlivé informácie, ktoré by mohli ohroziť národné bezpečnostné záujmy štátu, nemôžeme vynechať čl. 72 ods. 4 Rímskeho štatútu, podľa ktorého *„ak sa štát dozvie, že v niektorom štádiu konania sa pravdepodobne zverejnia alebo mohli by sa zverejniť informácie alebo dokumenty štátu a ich zverejnenie by podľa jeho názoru ohrozilo jeho národné bezpečnostné záujmy, tento štát má právo zasiahnuť s cieľom vyriešiť danú vec v súlade s týmto článkom“*. Uvedené znamená, že takýto riadne podaný zásah bude mať za následok zastavenie ďalšieho zverejňovania informácií, kým senát nedospeje ku konečnému rozhodnutiu vo veci.[74] Nie je však jasné, či sa štát môže dovolávať záujmu národnej bezpečnosti v prípade dokumentov, ktoré sú už teoreticky verejne dostupné. Aj keď sú hacknuté alebo uniknuté dokumenty utajované a obsahujú citlivé informácie, záujem národnej bezpečnosti vyplýva z ich zverejnenia, nie z ich použitia ako dôkazov alebo poskytnutia obhajobe, keďže obhajoba už má k informáciám prístup. V takomto prípade by štát mohol tvrdiť, že to, čo je verejné, nie je autentické a že nemôže poskytnúť skutočné dokumenty z dôvodu národnej bezpečnosti napriek svojej povinnosti spolupracovať s obžalobou (čl. 86 Rímskeho štatútu[75]).[76]

Záver

Digitálne informácie z otvorených zdrojov sa stávajú dôležitým nástrojom vyšetrovateľov, ktorí si postupne osvojujú technológiu umožňujúcu zhromažďovať dôkazy. Medzinárodné trestné súdy a tribunály sú ideálnymi platformami, ktoré môžu objasňujúcim spôsobom využívať a prezentovať pokrok v oblasti digitálnych technológií. Hoci medzinárodné spoločenstvo čoraz viac využíva potenciál digitálnych informácií z otvorených zdrojov na posilnenie zisťovania a overovania faktov, je dôležité zároveň priznať slabé miesta takýchto procesov a možnosť zaujatosti alebo skreslenia, ktorá môže ovplyvniť zber a analýzu takto získaných informácií.[77]

Ako bolo vyššie uvedené, digitálne informácie z otvorených zdrojov môžu zohrávať významnú úlohu pri vyšetrovaniach, a to nielen pri poskytovaní hlavných dôkazov a potvrdzovaní iných dôkazov, ale aj samotné poskytovanie priamych dôkazov o porušovaní, čo sa v praxi čoraz viac uznáva. Týmto spôsobom môžu pomôcť prekonať niektoré prekážky prístupu, ktoré bránili vyšetrovaniam, a majú potenciál poskytnúť hlas širšiemu okruhu ľudí a perspektív, než by sa inak mohli brať do úvahy. Digitálny priestor je to, čo dnes

73 FREEMAN, Lindsay. *Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases*, s. 80–84.

74 TRIFFTERER, Otto – AMBOS, Kai (eds). *Rome Statute of the International Criminal Court: A Commentary*. 3rd ed. München – Oxford – Baden Baden: C. H. Beck – Hart – Nomos, 2016, s. 1797.

75 *„Štáty, zmluvné strany, v súlade s ustanoveniami tohto štatútu plne spolupracujú so Súdom pri vyšetrovaní a trestnom stíhaní činov v jeho jurisdikcii.“*

76 FREEMAN, Lindsay. *Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases*, s. 86–88.

77 MCDERMOTT, Yvonne – KOENIG, Alexa – MURRAY, Daragh. *Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations*, s. 21.

využíva mnoho ľudí, preto sa práve v ňom často nachádzajú dôkazy, prílev ktorých má významný vplyv na ich zhromažďovanie. Význam dôkazov vytváraných používateľmi na sociálnych médiách viedol k pozitívnym aj negatívnym dôsledkom, je zrejmé, že tento typ dôkazov je dvojsečná zbraň. Napriek tomu tento vývoj so sebou prináša aj jedinečné právne výzvy, ktoré súvisia s otázkami spoľahlivosti, presnosti, dôveryhodnosti, autenticity a spravodlivého procesu, nakoľko existuje väčšia nespoľahlivosť a neistota v dôsledku jednoduchosti falšovania a manipulácie s digitálnym obsahom. Okrem toho má aj značné negatíva, pokiaľ ide o bezpečnosť nielen používateľov a ochranu ich práv. Prijatím prístupu založeného na dodržiavaní ľudských práv a vykonaním náležitej starostlivosti pred vyšetrovaním a počas neho, ako aj po ňom, sa vyšetrovatelia povzbudzujú k tomu, aby pochopili súvisiace riziká nielen pre seba, ale aj pre všetky osoby zapojené do procesu.

Už v minulosti boli médiá nápomocné a súčasne zneužité na podnecovanie páchania medzinárodných zločinov. Preto zosilnenie tohto javu v dnešnom kontexte nie je prekvapením, vzhľadom na rýchly rozvoj online platforiem a ich široké využívanie. Bez ohľadu na to, ktorý typ médií sa využíva, či rozhlas alebo sociálne médiá, používatelia sledujú zreteľný model šírenia nenávisti, ktorý sa zhmotňuje v hroznej brutalite mimo internetu. Dôležitým prvým krokom v tomto smere je uznanie skutočnosti, že informácie z otvorených zdrojov môžu byť rovnako otvorené skresleniam, medzerám a zraniteľnostiam ako akákoľvek iná forma informácií a môžu udržiavať marginalizáciu určitých skupín a komunít. Najlepším spôsobom, ako zabezpečiť premyslený, koherentný a starostlivý prístup k vyšetrovaniu s využitím otvorených zdrojov, je dôkladné plánovanie a investovanie do odbornej prípravy, personálu a zdrojov potrebných na úplné začlenenie metód s využitím otvorených zdrojov do vyšetrovacích tímov.[78] Vyšetrovatelia by zatiaľ mali k informáciám z otvorených zdrojov na internete pristupovať kriticky a používať systematické metódy vyšetrovania, aby sa zabezpečilo, že sa na ne bude možné spoľahnúť v súdnom konaní.

Odstraňovanie obsahu predstavuje riziko pre ľudskoprávnych aktivistov, právnikov, novinárov a všetkých, ktorí majú záujem na zachovaní kolektívnej pamäte o zverstvách. Viac obsahu znamená viac umelej inteligencie a rastúci regulačný tlak spôsobí, že platformy budú preventívne a radikálne odstraňovať obsah. Vyšetrovatelia si musia tento jav uvedomiť a uznať, že platformy, na ktoré sa spoliehajú pri zhromažďovaní dôkazov, sú dynamickí aktéri s vlastným záujmom. Ako výstižne uviedla Hamilton, *„spoliehať sa na digitálne dôkazy znamená spoliehať sa aj na platformy, ktoré ich hostia“*.[79] Ako platformy opakovane uviedli, obsahu je príliš veľa na to, aby ho bolo možné starostlivo moderovať. V skutočnosti môžu platformy ľahko obrátiť argument o slobode prejavu – neodstraňovanie obsahu je ich spôsobom podpora slobody prejavu a odstraňovanie (alebo moderovanie) obsahu je spôsob zlepšovania prejavu a uľahčovania otvorenej výmeny názorov.[80]

78 MURRAY, Daragh – MCDERMOTT, Yvonne – KOENIG, Alexa. *Mapping the Use of Open Source Research in UN Human Rights Investigations*, s. 22; DUBBERLEY, Sam – IVENS, Gabriela. *Outlining a Human-Rights Based Approach to Digital Open Source Investigations: A guide for human rights organisations and open source researchers*, s. 35–36; BELHADJ ALI, Chiraz. *International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media*, s. 59–60.

79 HAMILTON, Rebecca. *Social Media Platforms in International Criminal Investigations*, s. 223.

80 HUBLEY, Hillary. *Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations*, s. 26–27.

Dokumenty, ktoré boli získané nezákonným spôsobom, vrátane dokumentov získaných zo zdrojov ako je WikiLeaks, sa stále môžu považovať za dokumenty s obmedzenou dôkaznou hodnotou, ak je ich pravosť sporná. Libanonský tribunál nakoniec odmietol uznať dokumenty WikiLeaks ako dôkaz z dôvodu vnímanej nedostatočnej spoľahlivosti a autenticity. Na to, aby boli prípustné, musí strana, od ktorej boli dokumenty získané, uznať ich pravosť alebo ich presnosť alebo pravosť musia potvrdiť iné dôkazy.[81] Úniky informácií online, či už sú výsledkom legitímneho informovania, neoprávneného úniku alebo nezákonného hackingu, zodpovedajú definícii informácií z otvorených zdrojov, a predsa je niečo iné, keď sú informácie vo verejnej doméne, ktoré neboli určené na zverejnenie. Hacknuté a uniknuté dokumenty stiahnuté priamo z internetu by sa nemali pripustiť bez ďalšieho vyšetrovania a dodatočného overovania. Ak je možné získať dokumenty z ich pôvodného zdroja, tento krok by sa mal urobiť vždy, keď je to možné. Pokiaľ ide o predloženie uniknutých dokumentov, navrhujúca strana nesie bremeno vysvetlenia ich pôvodu a spoľahlivosti. Na overenie hacknutých a uniknutých digitálnych dokumentov by mal znalec analyzovať obsah dokumentov, zdroj dokumentov a technické aspekty dokumentu, ako je typ súboru a metadáta. Podľa Koenig a Freeman,[82] s ktorými súhlasíme, by sa digitálne informácie z otvorených zdrojov mali, podľa možnosti, podporiť fyzickými, svedeckými alebo inými listinnými dôkazmi. Výpovede svedkov a znalcov by preto mali zohrávať dôležitú úlohu pri interpretácii a overovaní pravosti uniknutých dokumentov. Preto sa odporúča, aby sudcovia uprednostňovali predkladanie tohto typu materiálov prostredníctvom svedka s jeho vysvetlením. Ak sa vyšetrovanie z otvorených zdrojov vykonáva starostlivo a profesionálne, môže mať obrovskú hodnotu pre súdne konanie. Hoci je objasnenie trestných činov pre medzinárodné súdne procesy prvoradé, rovnako dôležité je, aby tieto inštitúcie rešpektovali a chránili ľudské práva. Pripustenie uniknutých dokumentov by mohlo poškodiť práva obvinených viacerými rôznymi spôsobmi vrátane práva na konfrontáciu so svedkami obžaloby, práva na verejný proces a práva na kvalifikovanú obhajobu. Ak uniknuté dokumenty nie sú riadne overené, ich prijatie by tiež mohlo poškodiť spravodlivosť a legitímnosť súdneho konania. Prípadne by vylúčenie uniknutých dokumentov mohlo poškodiť obžalobu a odoprieť obetiam spravodlivosť.[83]

Podľa nášho názoru medzi pravdepodobne najväčšie prekážky prípustnosti a vhodnosti použitia dôkazov z otvorených zdrojov ako dôkazov v (medzi)národných trestných konaniach bude rozhodujúca schopnosť preukázať ich relevantnosť v konaní, dôkaznú hodnotu (spoľahlivosť, autentickosť a presnosť) a nevynímajúc absenciu akéhokoľvek škodlivého účinku na konanie.

V ére dezinformácií, falošných správ a alternatívnych faktov, ktorú niektorí označujú ako „éru postpravdy“, je súdne konanie poslednou možnosťou na objasnenie trestných činov. Súčasný nedostatok dôvery v politické a novinárske inštitúcie sa nemôže rozšíriť na súdne inštitúcie bez toho, aby došlo ku katastrofálnemu zlyhaniu právneho štátu. Napokon sú to podľa Freeman práve súdy, ktoré musia bojovať proti súčasnej kríze dôvery tým,

81 BLAIR, Cherie – VIDAK GOJKOVIĆ, Ema. *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evid*, s. 259.

82 KOENIG, Alexa – FREEMAN, Lindsay. *Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation*, s. 1254.

83 FREEMAN, Lindsay. *Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases*, s. 88–92.

že usilovne, rázne a dôsledne zabezpečia, aby súdne siene nikdy neboli „postpravdivé".[84] Ako uviedol Snyder, *„ak stratíme inštitúcie, ktoré vytvárajú fakty, ktoré sú pre nás relevantné, potom máme tendenciu utápať sa v príťažlivých abstrakciách a fikciách. […] Postpravda oslabuje právny štát a pozýva na režim mýtov"*.[85] Zabezpečenie riadneho zhromažďovania a uchovávania digitálnych dôkazov je účinným spôsobom ako ukázať, že páchatelia budú braní na zodpovednosť. Internet umožňuje spochybňovanie faktov a šírenie lží, ale ich aj odhaľuje. Technológia nie je ničím iným ako rozšírením a znásobením ľudských chýb a vlastností.

84 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. 66–67.

85 SNYDER, Timothy. The American Abyss. In: *New York Times Magazine* [online]. 9. 1. 2021, aktualizované 28. 12. 2021 [cit. 2022-11-14]. Dostupné z: <https://www.nytimes.com/2021/01/09/magazine/trump-coup.html>.

Open-Source Digital Evidence

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

Abstract: The aim of the article is to consider the use of information obtained from digital open sources as evidence in proceedings related to violations of international criminal law, human rights and international humanitarian law. In addition to providing basic definitions and legal questions that need to be answered before evidence obtained in this way could be further used, the article examines the different aspects that the type of evidence in question raises (new actors, mediation, objectivity and subjectivity). Despite the clear advantages, we should not overlook some of the problematic issues and challenges involved, particularly because the digital format allows for relatively easy manipulation and falsification, which in some cases poses an insurmountable obstacle to establishing the authenticity of the evidence and its provenance. The analysis also focuses on the vulnerabilities in the use of social media information (the volume of content produced, its moderation by platforms and the issue of metadata), since the content that appears on them reflects not only the nature of the current conduct of international or non-international armed conflict but also the misinformation that affects society. Given the increasing amount of hacked and leaked information in the public domain, the article concludes by examining the applicability of the information in question as evidence in legal proceedings and discusses the related legal and ethical issues of admissibility.

Keywords: international criminal law, open-source digital evidence, social media, hacked and leaked information, public domain