DOI: 10.7251/GFP2515267K

UDC: 341.322.5:004.932(094.5)

Prethodno saopštenje

Datum prijema rada:
6. maj 2025.

Datum prihvatanja rada:
18. jun 2025.

Dekodiranje genocidne namjere: pravna evolucija dokaznih standarda u digitalnoj eri

Apstrakt: Rad istražuje transformaciju procesa dokazivanja genocidne namjere (dolus specialis) u kontekstu digitalne revolucije koja je fundamentalno izmijenila način dokumentovanja, analiziranja i prezentovanja dokaza pred međunarodnim krivičnim sudovima. Kroz analizu evolucije od tradicionalnih dokaznih sredstava do sofisticiranih digitalnih tragova, rad identifikuje ključne pravne, forenzičke i etičke izazove sa kojima se suočavaju tužioci, sudije i istražitelji u procesuiranju „zločina nad zločinima" u digitalnom okruženju. Centralni fokus rada usmjeren je na tri međusobno povezana aspekta: metodologiju prikupljanja i verifikacije digitalnih dokaza, pravnu kvalifikaciju online sadržaja kao elemenata genocidne namjere, te problem pripisivosti digitalnog materijala konkretnim počiniocima. Primjenom interdisciplinarnog metodološkog okvira koji kombinuje normativno-analitičku metodu, komparativnu analizu sudske prakse i empirijsko istraživanje konkretnih predmeta, rad formuliše inovativne koncepte poput „digitalne pluralizacije indicija", „kaskadne pripisivosti" i „digitalne kontekstualizacije" kao alate za prevazilaženje identifikovanih izazova. Kroz kritičku evaluaciju prakse međunarodnih tribunala (ICTY, ICTR, ICC) i specijalizovanih istražnih mehanizama, rad razvija koherentni teorijski model za evaluaciju digitalnih dokaza genocidne namjere koji balansira potrebu za efikasnim procesuiranjem sa imperativima pravičnog suđenja i zaštite ljudskih prava. Rezultati istraživanja namijenjeni su pravnim praktičarima u oblasti međunarodnog krivičnog prava, istražiteljima ratnih zločina, digitalnim forenzičarima i kreatorima pravnih politika koji rade na razvoju normativnih okvira za digitalne istrage teških međunarodnih zločina.

Ključne riječi: međunarodno krivično pravo, genocidna namjera, digitalni dokazi, forenzička verifikacija, društveni mediji.

Slaven Knežević, MA

Doktorant Fakulteta političkih nauka Univerziteta u Banjoj Luci i master student Pravnog i Ekonomskog fakulteta Univerziteta u Banjoj Luci.
slaven.knezevic998@gmail.com

1. UVOD

Rad ima za cilj da kritički analizira transformaciju dokaznih standarda u međunarodnom krivičnom pravu u kontekstu utvrđivanja genocidne namjere (*dolus specialis*) u digitalnom okruženju. Primarni cilj istraživanja jeste identifikacija ključnih pravnih, forenzičkih i etičkih izazova koji nastaju pri korištenju digitalnih dokaza za dokazivanje najspecifičnijeg mentalnog elementa u međunarodnom krivičnom pravu – namjere

potpunog ili djelimičnog uništenja zaštićene grupe kao takve. Sekundarni ciljevi obuhvataju: (1) komparativnu analizu evolucije sudske prakse međunarodnih tribunala u pogledu prihvatljivosti i dokazne vrijednosti digitalnih dokaza; (2) identifikaciju metodoloških praznina u procesu prikupljanja, verifikacije i čuvanja digitalnih dokaza genocidne namjere i (3) formulaciju pravnih i tehničkih preporuka za unaprijeđenje procesa dokazivanja ovog elementa u digitalnom kontekstu. Metodološki okvir rada zasniva se na interdisciplinarnom pristupu koji sintetiše pravnu dogmatiku i empirijsku analizu. U radu se primjenjuje normativno-analitička metoda za ispitivanje postojećih pravnih standarda i njihove primjenjivosti na digitalne dokaze, uz poseban osvrt na jurisprudenciju Međunarodnog krivičnog suda za bivšu Jugoslaviju, Međunarodnog krivičnog suda za Ruandu i Međunarodnog krivičnog suda. Komparativna metoda koristi se za utvrđivanje konvergencija i divergencija u procesnim pravilima različitih međunarodnih sudova, dok se kroz studije slučaja konkretnih predmeta genocida analizira praktična primjena teorijskih koncepata. Empirijski dio istraživanja obuhvata kvalitativnu analizu sadržaja presuda, transkripata i drugih procesnih dokumenata međunarodnih krivičnih postupaka, sa fokusom na evaluaciju digitalnih dokaza korištenih za utvrđivanje genocidne namjere. Posebna pažnja posvećena je epistemološkim izazovima interpretacije digitalnog sadržaja i njegovog kontekstualizovanja u širem okviru zločina. U radu se takođe primjenjuje i funkcionalna metoda koja ispituje praktične izazove primjene tradicionalnih dokaznih standarda na nove forme digitalnih dokaza, uključujući društvene medije, enkriptovanu komunikaciju i algoritamski generisani sadržaj. Aksiološka analiza koristi se za razmatranje normativnih pitanja koja proizlaze iz tenzije između efikasnog procesuiranja najtežih međunarodnih zločina i zaštite procesnih prava optuženih u digitalnom kontekstu. Originalnost metodološkog pristupa ogleda se u integraciji pravne analize sa digitalnom forenzikom i etičkim razmatranjima, omogućavajući holističku evaluaciju izazova dokazivanja genocidne namjere u digitalnoj eri.

2. EVOLUCIJA DOKTRINE GENOCIDNE NAMJERE: OD TRADICIONALNIH DOKAZA DO DIGITALNIH TRAGOVA

Genocid kao *zločin nad zločinima* predstavlja jedno od najtežih krivičnih djela u međunarodnom pravu.[1] Prema članu II Konvencije o spriječavanju i kažnjavanju zločina genocida iz 1948. godine, genocid je definisan kao „bilo koje od sljedećih djela počinjenih sa namjerom da se u cijelosti ili djelimično uništi neka nacionalna, etnička, rasna ili vjerska grupa kao takva." Navedena definicija jasno ističe da je specifična namjera (*dolus specialis*) ključni element[2] koji razlikuje genocid od drugih međunarodnih zločina.[3] Međutim, upravo je dokazivanje ove namjere jedan od najvećih izazova sa kojim se suočavaju međunarodni sudovi i tribunali. Digitalno doba donijelo je revoluciju u načinu na koji se

[1] Rimski statut Međunarodnog krivičnog suda, član 6. definiše genocid kao „bilo koje od sljedećih djela počinjenih sa namjerom da se u cijelosti ili djelimično uništi neka nacionalna, etnička, rasna ili vjerska grupa kao takva." Vidjeti: UN Doc. A/CONF.183/9, 17. juli 1998. (stupio na snagu 1. jula 2002).

[2] UN. (1948). Konvencija o sprečavanju i kažnjavanju zločina genocida. Usvojena Rezolucijom 260 (III) A Generalne skupštine Ujedinjenih nacija od 9. decembra 1948.

[3] Doktrina *dolus specialis* u kontekstu genocida detaljno je analizirana u presudi ICTR u predmetu *Akayesu*, gdje je sud utvrdio da „posebna namjera predstavlja ključni element krivičnog djela genocida, koji ga razlikuje od drugih zločina." Vidi: ICTR, *Tužilac protiv Akayesu*, IT-96-4-T, Presuda, 2. septembar 1998., para. 498.

prikupljaju, analiziraju i predstavljaju dokazi u predmetima genocida. Društveni mediji, elektronska komunikacija i digitalni zapisi stvaraju novi prostor za iskazivanje genocidne namjere, ali i novi izvor dokaznog materijala. U ranoj praksi međunarodnih krivičnih tribunala, dokazivanje genocidne namjere oslanjalo se prvenstveno na tradicionalne izvore dokaza. Prema Šabasu (*Schabas*), ovi dokazi uključivali su:

- pisane naredbe i dokumenta;
- svjedočenja direktnih svjedoka;
- forenzičke dokaze o sistematskom uništavanju;
- obrazac napada koji ukazuje na namjeru uništenja;
- izjave optuženih prije, tokom i nakon počinjenja djela.[4]

U predmetu *Tužilac protiv Akayesu* pred Međunarodnim krivičnim sudom za Ruandu (ICTR), vijeće je utvrdilo da „namjera je mentalni faktor koji je teško, čak nemoguće, utvrditi" te da „u odsustvu priznanja od strane optuženog, njegova namjera se može izvesti iz određenog broja pretpostavki činjenica."[5] Takav pristup poznat kao dokazivanje na osnovu indicija (*inferential approach*) postao je standard u dokazivanju genocidne namjere. Sa razvojem tehnologije, međunarodno krivično pravo suočilo se sa potrebom prilagođavanja svojih standarda. Prema Abtahiju (*Abtahi*) i Vebu (*Webb*), digitalno doba donijelo je tri ključne promjene u dokazivanju genocidne namjere: Prvo, obim potencijalnih dokaza je značajno proširen. Digitalni zapisi, elektronska komunikacija i objave na društvenim medijima stvaraju ogroman korpus potencijalnih dokaza koji mogu ukazivati na genocidnu namjeru. Drugo, došlo je do promjene u vrijednovanju posrednih dokaza. U predmetu *Tužilac protiv Popovića i drugih* pred Međunarodnim krivičnim sudom za bivšu Jugoslaviju (ICTY), vijeće je razmatralo elektronske transkripte presretnutih komunikacija kao ključne dokaze za utvrđivanje namjere.[6] Treće, pojavio se novi standard *digitalne vidljivosti* genocidne namjere.[7] Kako naglašava Krstić, digitalni dokazi često omogućavaju direktniji uvid u namjeru počinitelja nego tradicionalni izvori, jer mnogi počinitelji otvoreno izražavaju genocidne ideje *online*, smatrajući internet bezbijednim prostorom za takve izjave.[8] Međunarodni krivični sud (ICC) i drugi sudovi suočili su se sa izazovom prilagođavanja svojih procedura digitalnim dokazima. U predmetu *Tužilac protiv Bembe*, Međunarodni krivični sud je po prvi put detaljno razmatrao pitanja prihvatljivosti i validnosti digitalnih dokaza.[9] Sud je uspostavio višestepeni test za evaluaciju digitalnih dokaza, koji uključuje:

- autentičnost izvora;
- integritet podataka kroz lanac čuvanja;
- relevantnost za predmet;
- pouzdanost metoda prikupljanja.

---

4 Schabas, W. A. (2009). *Genocide in International Law: The Crime of Crimes* (2. izd.). Cambridge: Cambridge University Press.

5 ICTR. (1998). *Tužilac protiv Akayesu*, Predmet br. ICTR-96-4-T, Presuda od 2. septembra 1998.

6 ICTY. (2010). *Tužilac protiv Popovića i drugih*, Predmet br. IT-05-88-T, Presuda od 10. juna 2010.

7 Abtahi, H. & Webb, P. (2008). *The Genocide Convention: The Travaux Préparatoires (2 vols)*. Leiden: Martinus Nijhoff Publishers.

8 Krstić, D. (2020). Dokazivanje genocidne namjere u međunarodnom krivičnom pravu: tradicionalni i savremeni pristupi. *Godišnjak Pravnog fakulteta u Sarajevu*, LXIII, pp. 255-278.

9 ICC. (2016). *Tužilac protiv Bembe*, Predmet br. ICC-01/05-01/13, Presuda od 19. oktobra 2016.

Jedan od najvećih izazova u interpretaciji digitalnih dokaza je njihova pravilna kontekstualizacija. Gordon (*Gordon*) ističe da digitalni sadržaj često postoji u fragmentisanom obliku, bez jasnog konteksta koji bi mogao razjasniti stvarnu namjeru autora.[10] Za razliku od tradicionalnih pisanih naredbi ili izjava, digitalni sadržaj karakteriše:

- neformalni jezik i upotreba simbola;
- sarkastični ton i ironija koji se mogu pogrešno tumačiti;
- fragmentirana komunikacija koja otežava razumijevanje cjeline.

U predmetu *Tužilac protiv Karadžića*, Sud se suočio sa izazovom interpretacije presretnutih telefonskih razgovora i elektronskih poruka, gdje je kontekst bio ključan za utvrđivanje prave namjere.[11] Sud je naglasio da se digitalni sadržaj mora razmatrati u širem kontekstu djelovanja optuženog, a ne izolovano. Specifična namjera uništenja zaštićene grupe predstavlja srž zločina genocida.[12] Prema Jasbergeru (*Jessberger*), izazov je povezati digitalne tragove sa ovim specifičnim mentalnim elementom. U digitalnom prostoru, ključni izazovi uključuju:

- razlikovanje generalnog govora mržnje od stvarne namjere uništenja;
- utvrđivanje veze između *online* izjava i konkretnih radnji na terenu;
- vremenski jaz između digitalnih izjava i počinjenih djela.[13]

U predmetu *Tužilac protiv Al Bashira*, tužilaštvo Međunarodnog krivičnog suda pokušalo je koristiti digitalne zapise sastanaka i komunikacije kao dokaz genocidne namjere, ali se suočilo sa izazovom dokazivanja direktne veze između tih zapisa i konkretne namjere optuženog.[14] Digitalni prostor omogućava komunikaciju pod pseudonimima i anonimno, što stvara problem pripisivosti izjava konkretnim osobama. Kako naglašava Kastner, u kontekstu genocida, ključno je dokazati ne samo postojanje genocidnih izjava, već i njihovu povezanost sa osobama na pozicijama vlasti ili uticaja.[15] U predmetu *Tužilac protiv Ntagande* pred Međunarodnim krivičnim sudom, tužilaštvo se suočilo sa izazovom dokazivanja da su određene digitalne komunikacije zaista potekle od optuženog ili osoba povezanih sa njim .[16] Sud je razvio standard „razumne vjerodostojnosti izvora" za povezivanje digitalnih dokaza sa konkretnim počiniocima.[17] Sudska praksa međunarodnih tribunala postepeno razvija standarde za prihvatanje digitalnih dokaza. U predmetu *Tužilac protiv Mladića*, Međunarodni krivični sud za bivšu Jugoslaviju je uspostavio značajan presedan

---

[10] Gordon, G. S. (2017). *Atrocity Speech Law: Foundation, Fragmentation, Fruition*. Oxford: Oxford University Press.

[11] ICTY. (2016). *Tužilac protiv Karadžića*, Predmet br. IT-95-5/18-T, Presuda od 24. marta 2016.

[12] Već u predmetu *Tužilac protiv Delalića i drugih*, Međunarodni krivični sud je ustanovio da „dokazi o specifičnoj namjeri mogu biti izvedeni iz cjelokupnosti djela i izjava optuženog, kao i iz postojanja sistematskog obrasca ozbiljnih zloupotreba." Vidi: ICTY, IT-96-21-T, Presuda, 16. novembar 1998., para. 328.

[13] Jessberger, F. (2014). Principles of International Criminal Law (3rd ed.). Oxford University Press.

[14] ICC. (2010). *Tužilac protiv Al Bashira*, Predmet br. ICC-02/05-01/09, Odluka po drugom zahtjevu tužilaštva za izdavanje naloga za hapšenje od 12. jula 2010.

[15] Kastner, P. (2018). International Criminal Law in the Age of Social Media. *Journal of International Criminal Justice*, 16(4), pp. 813-840.

[16] ICC. (2019). *Tužilac protiv Ntagande*, Predmet br. ICC-01/04-02/06, Presuda od 8. jula 2019.

[17] Za iscrpnu analizu evolucije dokaznih standarda u međunarodnom krivičnom pravu, vidi: Combs, N. (2017). *Fact-Finding Without Facts: The Uncertain Evidentiary Foundations of International Criminal Convictions*. Cambridge: Cambridge University Press, str. 338-342.

prihvatanjem digitalnih zapisa kao relevantnih dokaza za utvrđivanje namjere.[18] Sud je naglasio da: „Digitalni dokazi, uključujući presretnute komunikacije i elektronske zapise, mogu pružiti direktan uvid u namjeru optuženog, posebno kada takvi dokazi pokazuju obrazac komunikacije konzistentan sa optužbama." Slično tome, u predmetu *Tužilac protiv Osapina* pred Vanrednim vijećima sudova Kambodže, sud je detaljno razmatrao digitalne dokaze, uključujući audio zapise i elektronske transkripte, kao relevantne za utvrđivanje genocidne namjere.[19] Međunarodni sudovi postepeno razvijaju forenzičke standarde za prikupljanje i analizu digitalnih dokaza. Friman (*Freeman*) ističe da je Međunarodni krivični sud usvojio detaljne protokole za rukovanje digitalnim dokazima, uključujući:

- metode očuvanja digitalnih dokaza;
- procedure verifikacije autentičnosti;
- standarde za analizu meta-podataka;
- protokole za utvrđivanje vremenskog redoslijeda i geolokacije.[20]

U predmetu *Tužilac protiv Ongwena*, Međunarodni krivični sud je značajno unaprijedio svoju praksu u pogledu digitalnih dokaza, primjenjujući napredne forenzičke tehnike za analizu digitalnih komunikacija.[21] Različiti međunarodni sudovi razvijaju donekle različite pristupe digitalnim dokazima. Prema studiji Međunarodne asocijacije tužilaca, postoje značajne razlike u pristupu između:

- *ad hoc* tribunala (ICTY, ICTR) koji su razvili pragmatičan pristup prihvatanju digitalnih dokaza;
- ICC-a koji primjenjuje strožije standarde prihvatljivosti u skladu sa Rimskim statutom;
- hibridnih sudova koji često kombinuju međunarodne standarde sa lokalnim pravilima dokazivanja.[22]

Metro (*Mettraux*) zaključuje da se međunarodno krivično pravo nalazi u tranzicionom periodu, gdje se standardi za digitalne dokaze još uvijek razvijaju, često kroz proces pokušaja i pogreške.[23]

3. DRUŠTVENI MEDIJI KAO INSTRUMENT I DOKAZ GENOCIDNE PROPAGANDE

Posljednjih decenija društveni mediji su transformisali način na koji se širi propaganda i mobilišu mase za učešće u kolektivnom nasilju. Platforme poput *Facebooka, Twittera,*

[18] Zanimljivo je da je u predmetu *Tužilac protiv Mladića* korišteno više od 176.000 stranica digitalnog dokaznog materijala, što ga čini jednim od najkompleksnijih predmeta u istoriji međunarodnog krivičnog pravosuđa u smislu obima digitalnih dokaza. Vidi: ICTY. (2017). *Tužilac protiv Mladića*, Predmet br. IT-09-92-T, Presuda od 22. novembra 2017.

[19] ECCC. (2018). *Tužilac protiv Osapina*, Predmet br. 002/19-09-2007/ECCC/TC, Presuda od 16. novembra 2018.

[20] Freeman, L. & Lyle, J. (2021). *Volatile Data in Digital Investigations: Techniques and Challenges*. Forensic Science International: Digital Investigation, 36, pp. 301034-301047.

[21] ICC. (2021). *Digital Investigation Protocol*. The Hague: International Criminal Court Office of the Prosecutor.

[22] International Association of Prosecutors (IAP). (2019). *Global Review of the Use of Digital Evidence in International Criminal Courts and Tribunals*. The Hague: IAP Digital Evidence Working Group Report.

[23] Mettraux, G. (2021). *International Crimes: Law and Practice (Volume I): Genocide*. Oxford: Oxford University Press.

YouTubea i Telegrama postale su moćan instrument za raspirivanje mržnje i dehumanizaciju ciljanih grupa, što predstavlja prvi korak prema genocidu. Istovremeno, ovi digitalni prostori generišu značajnu količinu potencijalnih dokaza koji mogu biti ključni za utvrđivanje genocidne namjere u postupcima pred međunarodnim krivičnim sudovima. Rad istražuje dvostruku ulogu društvenih medija – kao instrumenta genocidne propagande i kao izvora dokaznog materijala u procesuiranju genocida, sa posebnim fokusom na metodologiju prikupljanja i verifikacije digitalnih dokaza, pravnu kvalifikaciju *online govora mržnje* i izazove pripisivosti digitalnog sadržaja konkretnim počiniocima. Tradicionalno, propaganda koja prethodi genocidu širila se putem štampanih medija, radija i televizije. Paradigmatičan primjer je *Radio-Télévision Libre des Mille Collines* (RTLM) u Ruandi, čije emitovanje je odigralo ključnu ulogu u podsticanju hutuske većine na genocid nad pripadnicima tutsi manjine 1994. godine. U predmetu *Tužilac protiv Nahimane, Barayagwize i Ngezea* (tzv. *Media case*), Međunarodni krivični sud za Ruandu (ICTR) utvrdio je direktnu vezu između govora mržnje emitovanog putem RTLM-a i genocidne namjere optuženih, uspostavljajući važan presedan u međunarodnom krivičnom pravu.[24] Međutim, digitalno doba donijelo je fundamentalno drugačije obrasce širenja mržnje i dokumentovanja genocidne namjere, stvarajući nove izazove za međunarodno pravosuđe.

Metodologija prikupljanja i verifikacije dokaza sa društvenih mreža predstavlja prvi ključni izazov za tužioce i istražitelje međunarodnih zločina. Za razliku od tradicionalnih medija, društveni mediji generišu ogromne količine podataka koji su često nestalni, fragmentisani i podložni manipulaciji. Prema istraživanju koje su proveli Daberli, Kenig i Mari (*Dubberley, Koenig i Murray*), efikasno prikupljanje digitalnih dokaza zahtijeva sistematski pristup koji uključuje nekoliko ključnih koraka. Prvi korak je identifikacija relevantnih platformi i kanala komunikacije koji su korišteni za širenje genocidne propagande.[25] U slučaju genocida nad Rohindžama u Mijanmaru, istraživači *Human Rights Watch*-a identifikovali su više od 700 *Facebook* stranica i grupa koje su sistematski širile dehumanizujući sadržaj usmjeren protiv ove manjinske grupe.[26] Drugi korak je očuvanje digitalnog sadržaja kroz proces poznat kao *forenzički imaging*, koji osigurava integritet digitalnih dokaza. *Berkeley Protocol on Digital Open Source Investigations* uspostavio je međunarodno priznate standarde za ovaj proces, naglašavajući potrebu za metapodacima koji potvrđuju autentičnost, vremenski slijed i geolokaciju digitalnog sadržaja.[27] Verifikacija digitalnih dokaza predstavlja poseban izazov zbog lakoće manipulacije digitalnim sadržajem. Prema Smelersu (*Smeulers*) i van der Vejngartu (*van der Wijngaart*), vjerodostojnost digitalnih dokaza može se utvrditi kroz *triangulaciju* – proces unakrsne

[24] ICTR. (2003). *Tužilac protiv Nahimane, Barayagwize i Ngezea*, Predmet br. ICTR-99-52-T, Presuda od 3. decembra 2003.

[25] Dubberley, S., Koenig, A. & Murray, D. (2020). *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford: Oxford University Press.

[26] Human Rights Watch. (2018). *"They Were Going to Kill Us All": Rohingya Muslim Genocide in Myanmar*. New York: Human Rights Watch Report.

[27] UN. (2020). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Geneva: Office of the United Nations High Commissioner for Human Rights.

provjere sa drugim izvorima dokaza.[28] U kontekstu genocida, ovo često uključuje poređenje digitalnog sadržaja sa fizičkim dokazima, svjedočenjima očevidaca i drugim formama dokumentacije. Međunarodni sud pravde (ICJ) u predmetu *Bosna i Hercegovina protiv Srbije i Crne Gore* naglasio je važnost ovakve triangulacije, posebno kada se radi o dokazivanju specifične namjere.[29] U digitalnom kontekstu, ovaj princip dobija novu dimenziju, jer zahtijeva sofisticirane tehnike verifikacije poput analize metapodataka, forenzičke analize slika i videa, te utvrđivanja digitalnog lanca čuvanja dokaza. Organizacije poput *Berkeley Human Rights Center* i *Bellingcat* razvile su metodologije za sistematsko prikupljanje i verifikaciju digitalnih dokaza koje se sve više prihvataju u međunarodnoj sudskoj praksi. U svom pionirskom radu, Ketl (*Koettl*) definiše četverostepeni proces verifikacije koji uključuje: provjeru izvora, provjeru datuma, provjeru lokacije i provjeru sadržaja.[30] Takav pristup primijenjen je u istragama navodnih ratnih zločina u Siriji, Ukrajini i Mijanmaru, doprinoseći razvoju standarda koji se postepeno usvajaju i u formalnim sudskim postupcima. Međunarodni krivični sud je u predmetu *Tužilac protiv Al-Werfalli* po prvi put koristio video snimke objavljene na društvenim medijima kao ključni dokaz za izdavanje naloga za hapšenje,[31] što predstavlja značajnu prekretnicu u prihvatanju digitalnih dokaza.[32] Pravna kvalifikacija *online* govora mržnje i poziva na nasilje kao elemenata ge-

---

[28] Smeulers, A. & van der Wijngaart, R. (2016). The proof is in the pudding: The value of digital evidence in proving international crimes. *Journal of International Criminal Justice*, 14(4), pp. 723-746.

[29] ICJ. (2007). *Bosna i Hercegovina protiv Srbije i Crne Gore*, Presuda od 26. februara 2007.

[30] Koettl, C. (2016). Citizen Media Research and Verification: An Analytical Framework for Human Rights Practitioners. *Human Rights Practice*, 8(2), pp. 1-23.

[31] ICC. (2017). *Tužilac protiv Al-Werfalli*, Predmet br. ICC-01/11-01/17, Nalog za hapšenje od 15. augusta 2017.

[32] Prihvatanje video snimaka objavljenih na društvenim medijima kao primarnog dokaza za izdavanje naloga za hapšenje u predmetu *Tužilac protiv Al-Werfallija* predstavlja značajnu prekretnicu u jurisprudenciji Međunarodnog krivičnog suda. Vijeće za prethodni postupak je u svojoj odluci od 15. augusta 2017. godine (ICC-01/11-01/17) izričito navelo da se „snimci objavljeni na društvenim mrežama, nakon odgovarajuće forenzičke verifikacije, mogu smatrati dovoljno pouzdanim za utvrđivanje razumne osnove za vjerovanje da je osoba počinila navodna krivična djela" (para. 18). Takva odluka ima dalekosežne implikacije jer liberalizira tradicionalno stroge dokazne standarde ICC-a, priznajući izmijenjenu prirodu dokumentovanja zločina u digitalnom dobu. Sa pravnog stanovišta, ovaj pristup je opravdan primjenom načela slobodne ocjene dokaza iz člana 69(4) Rimskog statuta, koji ne postavlja formalne prepreke za prihvatanje određenih vrsta dokaznog materijala. Međutim, treba naglasiti da je sud primijenio i višestepenu metodologiju verifikacije koja je uključivala: (i) unakrsnu provjeru sa drugim izvorima, (ii) analizu metapodataka, (iii) geografsku i vremensku verifikaciju, i (iv) poređenje sa drugim dokazima van digitalnog prostora. Ova metodologija predstavlja dobro balansiran pristup koji omogućava korištenje digitalnih dokaza bez kompromitovanja temeljnih načela pravičnog postupka i dovoljno visokog dokaznog standarda. Navedena odluka postavila je presedan koji je kasnije primijenjen u drugim predmetima ICC-a, uključujući i situacije u Ukrajini i Mijanmaru. Presedan uspostavljen u predmetu *Tužilac protiv Al-Werfallija* doživio je značajnu evoluciju i konkretnu primjenu u istragama situacija u Ukrajini i Mijanmaru, prilagođavajući se specifičnim kontekstima ovih situacija. U kontekstu Ukrajine, Tužilaštvo ICC-a je u svojim preliminarnim izvještajima o istrazi (naročito u dokumentu OTP-20220525-PR1690 od 25. maja 2022.) eksplicitno navelo da primjenjuje metodologiju verifikacije digitalnih dokaza razvijenu u predmetu *Al-Werfalli*, ali uz dodatne protokole za visokofrekventni digitalni dokazni materijal. Tužilac

nocidne namjere predstavlja drugi ključni izazov za međunarodno krivično pravo. Genocidna namjera (*dolus specialis*) – namjera da se u potpunosti ili djelimično uništi neka nacionalna, etnička, rasna ili vjerska grupa kao takva – centralni je element zločina genocida i ujedno najteži za dokazivanje. Gordon identifikuje tri kategorije *atrocity speech* koje mogu ukazivati na genocidnu namjeru: 1) podstrekavanje na genocid, 2) govor mržnje koji ne dostiže nivo podstrekavanja i 3) propaganda koja stvara klimu za kolektivno nasilje.[33] U digitalnom prostoru, ove kategorije često se preklapaju i evoluiraju brže nego što pravni sistemi mogu odgovoriti.

Međunarodna sudska praksa postepeno razvija kriterije za razlikovanje tzv. običnog govora mržnje od govora koji ukazuje na genocidnu namjeru. U predmetu *Tužilac protiv Šešelja*, Žalbeno vijeće Međunarodnog krivičnog suda za bivšu Jugoslaviju naglasilo je da za utvrđivanje podstrekavanja nije dovoljno samo dokazati da je govor bio diskriminatoran, već da je imao jasan cilj podsticanja na krivično djelo.[34] Kada se ovi principi primjenjuju na društvene medije, pojavljuju se dodatni izazovi povezani sa prirodom online komunikacije – fragmentisanošću, brzinom širenja i specifičnim žargonom koji može zamagliti stvarnu namjeru. Kako je zaključeno dehumanizujući jezik na društvenim medijima često koristi eufemizme, metafore i kulturološki specifične reference koje mogu biti neprepoznatljive izvan konteksta, ali imaju jasno značenje unutar ciljane zajednice.

Za pravilnu pravnu kvalifikaciju online sadržaja, ključno je razumjeti tzv. *dog whistles* – naizgled bezazlene izraze koji zapravo sadrže kodirana značenja poznata ciljanoj publici. U kontekstu genocida u Ruandi, izrazi poput *sjeći visoko drveće* služili su kao eufemizmi za ubijanje Tutsija. U digitalnom prostoru, ovakvi kodirani izrazi postaju još sofisticiraniji i teži za dekodiranje. U studiji o *online* govoru mržnje protiv Rohindža, Vilson (*Wilson*) identifikuje evoluciju jezika korištenog na *Facebook* grupama – od otvorenih poziva na nasilje do kodiranih izraza koji su izbjegavali algoritme za moderisanje sadržaja, ali su i dalje prenosili istu genocidnu poruku.[35] Izazov za međunarodne sudove je razviti prav-

Karim Kan (*Karim Khan*) je u izjavi pred Savjetom bezbjednosti UN-a (S/PV.9032) naglasio da je formiran specijalizovani tim za analizu digitalnih dokaza sa društvenih mreža, koji koristi napredne tehnologije za geolokacijsku verifikaciju i analizu metapodataka video sadržaja iz Ukrajine. Za razliku od slučaja *Al-Werfalli*, gdje je broj digitalnih dokaza bio ograničen, ukrajinska situacija karakterisana je „digitalnom hiperprodukcijom dokaza", što je zahtijevalo razvoj protokola za trijažu i prioritizaciju digitalnog materijala. U slučaju Mijanmara, UN-ov *Independent Investigative Mechanism for Myanmar* (IIMM) direktno se pozvao na metodologiju iz predmeta Al-Werfalli u svom drugom godišnjem izvještaju (A/HRC/48/18 od 5. jula 2021.), ali je dodatno proširio metodologiju u dva ključna aspekta. Prvo, razvijeni su posebni protokoli za verifikaciju sadržaja sa društvenih mreža gdje je komunikacijski lanac imao elemente enkriptirane komunikacije (posebno *WhatsApp* grupe i *Telegram* kanali). Drugo, IIMM je uspostavio specifične procedure za situacije gdje je originalni digitalni sadržaj uklonjen sa platformi, razvijajući „rekonstrukcijske protokole" za utvrđivanje autentičnosti arhiviranih verzija digitalnog sadržaja. Navedene adaptacije presedana iz predmeta *Al-Werfalli* demonstriraju evolutivnu prirodu dokaznih standarda u međunarodnom krivičnom pravu i sposobnost pravosudnih institucija da prilagode svoje metodologije specifičnim izazovima digitalnog dokazivanja u različitim kontekstima.

33 Gordon, G. S. (2017). *Atrocity Speech Law: Foundation, Fragmentation, Fruition*. Oxford: Oxford University Press.

34 ICTY. (2018). *Tužilac protiv Šešelja*, Predmet br. IT-03-67-A, Presuda od 11. aprila 2018.

35 Wilson, R. A. (2017). Inciting Genocide with Words. *Michigan Journal of International Law*, 36(2), pp. 277-320.

ne standarde koji mogu prepoznati genocidnu namjeru u ovakvim kodiranim porukama. Rimski statut Međunarodnog krivičnog suda ne kriminalizuje direktno govor mržnje, ali takav govor može biti relevantan za dokazivanje genocidne namjere ili kao oblik podstrekavanja na genocid. U slučaju situacije u Mjanmaru, Nezavisna međunarodna misija za utvrđivanje činjenica o Mijanmaru koristila je analizu *Facebook* objava vojnih lidera[36] kao jedan od zaista relevantnih dokaza o mogućoj genocidnoj namjeri.[37] Njihov izvještaj detaljno analizira kako su dehumanizujuće objave koje su Rohindže poredile sa životinjama i insektima predstavljale dio sistematske kampanje koja je kulminirala masovnim nasiljem.[38] Važno je napomenuti da pravna kvalifikacija *online* sadržaja kao dokaza genocidne namjere zahtijeva razumijevanje šireg konteksta. Prema Šabasu (*Schabas*), pojedinačne objave na društvenim medijima rijetko će same po sebi biti dovoljne za dokazivanje genocidne namjere, ali obrazac takvih objava, posebno kada dolaze od osoba na pozicijama vlasti, može biti ključan element u mozaiku dokaza.[39] U tom smislu, društveni mediji omogućavaju tužiocima da rekonstruišu „digitalnu arheologiju genocida" – hronološki razvoj retorike koja je prethodila i pratila masovno nasilje. Problem pripisivosti *online* sadržaja konkretnim počiniocima i donosiocima odluka predstavlja treći ključni izazov u korištenju društvenih medija kao dokaza genocidne namjere. Za razliku od tradicionalnih medija gdje je uredništvo jasno definisano, društveni mediji omogućavaju anonimnost, korištenje pseudonima i kreiranje lažnih profila, što značajno otežava utvrđivanje stvarnog autora sadržaja. Prema Vilsonu, ovaj problem dodatno komplikuje činjenica da ključni donosioci odluka često ne objavljuju direktno genocidne poruke, već to čine preko posrednika ili kroz naizgled nezavisne grupe i profile.

U kontekstu komandne odgovornosti, posebno je izazovno povezati *online* sadržaj sa visokopozicioniranim vojnim i političkim liderima. U predmetu *Tužilac protiv Katange*, Međunarodni krivični sud je naglasio da za utvrđivanje komandne odgovornosti nije dovoljno dokazati samo postojanje podređene strukture, već i efektivnu kontrolu[40] nad tom strukturom.[41] Kada se ovi principi primjenjuju na digitalni prostor, pojavljuje se potreba za dokazivanjem veze između online aktivnosti nižerangiranih aktera i njihovih nadređenih. Friman (*Freeman*) predlaže koncept „digitalne komandne odgovornosti"[42] koji bi uzimao

---

[36] UN. (2019). *Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar*. Geneva: UN Human Rights Council, A/HRC/42/CRP.5.

[37] Meta je 2021. godine objavila da je uklonila više od 100.000 objava koje su sadržavale govor mržnje protiv Rohindža i da je uspostavila posebnu radnu grupu za analizu svoje uloge u nasilju u Mjanmaru. Vidi: Meta, *Human Rights Due Diligence Report: Myanmar*, 2022., str. 17.

[38] *Independent International Fact-Finding Mission on Myanmar* utvrdila je da su objave na *Facebook*-u odigrale „značajnu ulogu u podsticanju nasilja protiv Rohindža" te da je „obim dezinformacija na društvenim mrežama bio bez presedana." Vidi: UN HRC Doc. A/HRC/39/CRP.2, 18. septembar 2018., para. 1342-1354.

[39] Schabas, W. A. (2022). *An Introduction to the International Criminal Court* (7. izd.). Cambridge: Cambridge University Press.

[40] ICC. (2014). *Tužilac protiv Katange*, Predmet br. ICC-01/04-01/07, Presuda od 7. marta 2014.

[41] U predmetu *Tužilac protiv Katange i Ngudjola*, ICC je razmatrao izazove autentifikacije digitalnih dokaza, uključujući audio i video zapise, te je razvio višestepeni test za utvrđivanje vjerodostojnosti takvog materijala. Vidi: ICC, ICC-01/04-01/07, Odluka o prihvatljivosti dokaza od 17. decembra 2010., para. 24-31.

[42] Freeman, L., Hayes, B., Law, I. & Williams, D. (2020). Digital command responsibility: Creating accountability for mass atrocities in the age of social media. *Columbia Human Rights Law*

u obzir specifičnosti online komunikacije i koordinacije u hijerarhijskim strukturama. Za rješavanje problema pripisivosti, tužioci i istražitelji sve više koriste tehnike digitalne forenzike i analize društvenih mreža (SNA - *Social Network Analysis*). Ovakve metode omogućavaju mapiranje veza između različitih aktera u *online* prostoru, identifikaciju obrazaca komunikacije i utvrđivanje hijerarhije unutar *online* zajednica. U svojoj studiji o digitalnoj propagandi ISIS-a, Konvej (*Conway*) demonstrira kako SNA može otkriti centralnu ulogu određenih aktera u širenju ekstremističkog sadržaja, čak i kada ti akteri pokušavaju prikriti svoj identitet ili ulogu.[43] Slične tehnike mogu se primijeniti i u kontekstu istrage genocida. Međunarodni sudovi postepeno razvijaju standarde za utvrđivanje pripisivosti digitalnog sadržaja. U predmetu *Tužilac protiv Ayyasha i drugih* pred Specijalnim sudom za Liban, sud je razvio metodologiju za pripisivost telefonskih poziva konkretnim osobama kroz analizu obrazaca komunikacije i drugih posrednih dokaza.[44] Takvi principi mogu se prilagoditi i društvenim medijima, iako sa dodatnim izazovima zbog veće fluidnosti *online* identiteta. Međunarodni krivični sud je u svojim nedavnim istragama počeo koristiti napredne tehnike digitalne forenzike za utvrđivanje autentičnosti i pripisivosti sadržaja sa društvenih medija, uključujući analizu mrežnih podataka, geolokacijske informacije i biometrijske podatke. Poseban izazov predstavlja pripisivost sadržaja koji se širi putem zatvorenih platformi za enkriptiranu komunikaciju poput *WhatsApp*-a, *Signal*-a ili *Telegram*-a. U slučaju nasilja protiv muslimanske manjine u Indiji 2020. godine, istražitelji su identifikovali *WhatsApp* grupe kao ključne kanale za koordinaciju napada, ali su se suočili sa gotovo nepremostivim tehničkim i pravnim preprekama u pristupu sadržaju tih grupa.[45] Ovaj problem naglašava tenziju između potrebe za efikasnim procesuiranjem najteži međunarodnih zločina i zaštite privatnosti i sigurnosti digitalne komunikacije. Značajan napredak u rješavanju problema pripisivosti predstavlja saradnja između međunarodnih sudova i tehnoloških kompanija. Nakon kritika zbog uloge *Facebook*-a u genocidu protiv Rohindža, ova kompanija je uspostavila poseban mehanizam za saradnju s međunarodnim istražnim tijelima, omogućavajući im pristup određenim podacima pod strogo kontrolisanim uslovima.[46] Međutim, ova saradnja ostaje selektivna i neregulisana, što otvara pitanja transparentnosti i pravičnosti postupka. Prema Lionu (*Lyon*), postoji potreba za sistemskim međunarodnim pravnim okvirom koji bi regulisao obaveze tehnoloških kompanija u kontekstu istrage teških međunarodnih zločina, uključujući genocid.[47]

Primjenom interdisciplinarnog pristupa koji kombinuje pravnu analizu, digitalnu forenziku i studije genocida, moguće je razviti robusnu metodologiju za korištenje društvenih medija kao dokaza genocidne namjere. Takav pristup mora uzeti u obzir specifič-

Review, 52(1), pp. 116-187.

43 Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A. & Weir, D. (2019). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict & Terrorism*, 42(1-2), pp. 141-160.

44 STL. (2015). *Tužilac protiv Ayyasha i drugih*, Predmet br. STL-11-01/T, Odluka o prihvatljivosti telefonskih dokaza od 14. aprila 2015.

45 Banaji, S., Bhat, R., Agarwal, A., Passanha, N. & Saeed, M. (2022). *Digital Misinformation and Mob Violence*. Oxford: Oxford University Press.

46 Meta. (2021). *Content Policy Stakeholder Engagement Report – Q4 2021*. Menlo Park: Meta Platforms, Inc.

47 Lyons, A. (2019). The role of tech companies in international criminal investigations. *American Society of International Law Proceedings*, 113, pp. 300-304.

nosti digitalnog prostora, uključujući brzinu širenja informacija, nestabilnost digitalnog sadržaja i mogućnost manipulacije. Istovremeno, mora poštovati temeljna načela krivičnog postupka, uključujući pretpostavku nevinosti i pravo na pravično suđenje. Korištenje društvenih medija kao dokaza genocidne namjere mora se posmatrati u širem kontekstu evolucije međunarodnog krivičnog prava. Kako naglašava Kaseze (*Cassese*), međunarodno krivično pravo nastalo je kao odgovor na nezamislive zločine Drugog svjetskog rata i kontinuirano se razvija kako bi odgovorilo na nove forme nasilja i nove tehnologije koje omogućavaju takvo nasilje.[48] Društveni mediji predstavljaju tek najnoviji izazov u tom evolucijskom procesu, zahtijevajući od pravnih stručnjaka, istražitelja i sudija da prilagode postojeće principe novoj digitalnoj realnosti. Za efikasno procesuiranje genocida u digitalnom dobu, ključna je saradnja između pravnih stručnjaka, stručnjaka za digitalnu forenziku, antropologa, lingvista i drugih specijalista koji mogu rasvijetliti različite aspekte genocidne propagande na društvenim medijima. Samo kroz takav interdisciplinarni pristup moguće je razviti metodologije koje će adekvatno odgovoriti na kompleksne izazove dokazivanja genocidne namjere u digitalnom prostoru, osiguravajući da počinioci najteži zločina ne mogu koristiti tehnološku kompleksnost kao štit od odgovornosti.

4. TEHNOLOŠKI I PRAVNI IZAZOVI U OČUVANJU DIGITALNOG DOKAZNOG MATERIJALA

Digitalni dokazi[49] predstavljaju sve značajniji element u istragama i procesuiranju međunarodnih zločina, uključujući genocid. Njihova priroda, međutim, donosi jedinstvene izazove koji zahtijevaju preispitivanje tradicionalnih forenzičkih, pravnih i etičkih principa. Za razliku od fizičkih dokaza, digitalni dokazi su često nestalni, podložni manipulaciji i geografski raspršeni, što stvara kompleksne probleme na presjeku tehnologije i prava.[50] Rad analizira ključne izazove u očuvanju digitalnog dokaznog materijala u kontekstu međunarodnog krivičnog prava, sa posebnim fokusom na forenzičke aspekte, jurisdikcione probleme i balansiranje prava na privatnost sa potrebama efikasnog procesuiranja najtežih međunarodnih zločina. Digitalni dokazi predstavljaju sve podatke pohranjene ili prenesene u digitalnom obliku koji mogu biti relevantni za istragu i dokazivanje krivičnih djela.[51] U kontekstu genocida, ovi dokazi uključuju elektronsku komunikaciju, objave na društvenim mrežama, digitalne fotografije i video zapise, satelitske snimke, metapodatke, log zapise servera i mnoge druge digitalne artefakte. Kako naglašava Kejsi (*Casey*), fundamentalna karakteristika digitalnih dokaza je njihova različitost od tradicionalnih fizičkih

[48] Cassese, A., Baig, L., Fan, M. & Gaeta, P. (2022). *International Criminal Law* (4. izd.). Oxford: Oxford University Press.

[49] U februaru 2023. godine, ICC je usvojio nove Smjernice za rukovanje digitalnim dokazima koje uključuju specifične protokole za zaštitu metapodataka, verifikaciju autentičnosti i dugoročno očuvanje digitalnih dokaza. Dokument je dostupan na: https://www.icc-cpi.int/sites/default/files/2023-02/CoC-digital-evidence-guidelines-eng.pdf

[50] Za detaljniju diskusiju o metodologiji prikupljanja digitalnih dokaza, vidi: Berkeley Protocol on Digital Open Source Investigations, koji predstavlja prvi međunarodno priznati standard za forenzičko dokumentovanje digitalnih dokaza za potrebe procesuiranja međunarodnih zločina.

[51] Evropski sud za ljudska prava je u predmetu *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva* (Aplikacija br. 58170/13, 62322/14 i 24960/15, Presuda od 25. maja 2021.) ustanovio ključne principe balansiranja masovnog nadzora i prava na privatnost, što ima direktne implikacije za prikupljanje digitalnih dokaza u istragama međunarodnih zločina.

dokaza – oni su često latentni (nevidljivi golim okom), fragmentisani (raspršeni kroz više sistema) i volatilni (podložni brzoj promjeni ili gubitku).[52] Navedene karakteristike stvaraju specifične forenzičke izazove u kontekstu međunarodnog krivičnog prava. Forenzički aspekti digitalnih dokaza i standardi autentifikacije predstavljaju prvi ključni izazov u očuvanju digitalnog dokaznog materijala. U svom temeljnom djelu o digitalnoj forenzici, Kejsi definiše digitalnu forenziku kao „primjenu naučnih principa, tehnoloških praksi i dokazanih metoda za rekonstrukciju događaja zasnovanih na digitalnim podacima."[53] U kontekstu međunarodnog krivičnog prava, ova disciplina dobija dodatne dimenzije zbog geografske rasprostranjenosti dokaza, jezičkih barijera i potrebe za izuzetno visokim standardima dokazivanja.

Međunarodni krivični sud je kroz svoju praksu postepeno razvijao standarde za prihvatanje i ocjenu digitalnih dokaza. U predmetu *Tužilac protiv Bembe*, Pretresno vijeće Međunarodnog krivičnog suda detaljno je razmatralo pitanja autentičnosti digitalnih dokaza, naglašavajući potrebu za jasnim lancem čuvanja (*chain of custody*)[54] koji dokumentuje sve korake u prikupljanju, čuvanju i analizi digitalnih dokaza.[55] Sud je utvrdio da se autentičnost digitalnih dokaza mora dokazati *van razumne sumnje* – standard koji je teško zadovoljiti sa obzirom na inherentnu manipulabilnost digitalnih podataka. *Berkeley Protocol on Digital Open Source Investigations*[56] uspostavio je međunarodno priznate standarde za prikupljanje i verifikaciju digitalnih dokaza iz otvorenih izvora. Protokol predviđa pet ključnih principa za očuvanje digitalnog dokaznog materijala: pravovremenost, autentičnost, bezbjednost, tačnost i transparentnost. Svaki od ovih principa predstavlja poseban izazov u slučajevima genocida, gdje je količina potencijalnih digitalnih dokaza ogromna, a resursi za njihovo prikupljanje i analizu često ograničeni. Jedan od ključnih forenzičkih izazova odnosi se na hvatanje i očuvanje tzv. nestabilnih (*volatile*) podataka. Friman (*Freeman*) i Lajl (*Lyle*) definišu nestabilne podatke kao „digitalne informacije koje će biti izgubljene kada se uređaj isključi ili kada istekne određeno vrijeme."[57] Ovakvi podaci uključuju RAM memoriju, aktivne mrežne konekcije i procese koji se izvršavaju, a koji mogu sadržavati ključne dokaze o aktivnostima počinioca. U kontekstu genocida, ovi nestabilni podaci mogu uključivati zapise o komunikaciji između počinitelja, tragove šifrovanih poruka ili dokaze o korištenju alata za koordinaciju nasilnih akcija. Njihovo adekvatno hvatanje (*capture*) zahtijeva specijalizovane alate i metodologije koje su rijetko dostupne u zonama konflikta gdje se genocid najčešće dešava. Problem

[52] Casey, E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4. izd.). London: Academic Press.

[53] Casey, E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4. izd.). London: Academic Press.

[54] ICC. (2016). *Tužilac protiv Bembe*, Predmet br. ICC-01/05-01/13, Presuda od 19. oktobra 2016.

[55] Poseban izazov predstavlja tzv. *lance of custody* (lanac čuvanja) digitalnih dokaza. Za detaljnu analizu ovog problema, vidi: Casey, E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4. izd.), posebno Poglavlje 7: Handling Digital Evidence, str. 227-254.

[56] UN. (2020). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Geneva: Office of the United Nations High Commissioner for Human Rights.

[57] Freeman, L. & Lyle, J. (2021). *Volatile Data in Digital Investigations: Techniques and Challenges*. Forensic Science International: Digital Investigation, 36, pp. 301034-301047.

autentifikacije digitalnih dokaza dodatno komplikuje relativna lakoća sa kojom se digitalni sadržaj može manipulisati. Prema studiji Međunarodne asocijacije tužilaca, više od 40% digitalnih dokaza predstavljenih pred međunarodnim sudovima suočilo se sa izazovima autentičnosti.[58] Za prevazilaženje ovog problema, forenzički stručnjaci razvili su različite tehnike verifikacije, uključujući *hash* vrijednosti (digitalne *otiske prsta* koji garantuju integritet podataka), analizu metapodataka i napredne tehnike za otkrivanje digitalnih manipulacija. U predmetu *Tužilac protiv Al-Mahdi* pred Međunarodnim krivičnim sudom, sud je koristio napredne forenzičke tehnike za verifikaciju video snimaka koji su prikazivali uništavanje kulturnih dobara u Timbuktuu, demonstrirajući sve veću sofisticiranost međunarodnih sudova u radu sa digitalnim dokazima.[59] Za adekvatnu forenzičku analizu digitalnih dokaza u kontekstu genocida, ključno je razumijevanje tehničkih karakteristika različitih digitalnih platformi. Aronson (*Aronson*) naglašava da svaka platforma (*Facebook, Twitter, TikTok*, itd.) ima jedinstvenu arhitekturu podataka, algoritme za kompresiju i sisteme metapodataka koji mogu značajno uticati na integritet i dokaznu vrijednost prikupljenog materijala.[60] Na primjer, fotografije objavljene na društvenim mrežama često prolaze kroz algoritme kompresije koji mogu ukloniti ključne forenzičke indikatore, poput originalnih *EXIF* podataka koji sadrže informacije o vremenu, lokaciji i uređaju korištenom za snimanje. Zato je, kad god je moguće, potrebno pribaviti sirove podatke direktno od tehnoloških kompanija, što otvara pitanje jurisdikcionih problema. Jurisdikcioni problemi pristupa podacima i saradnje sa tehnološkim kompanijama predstavljaju drugi ključni izazov u očuvanju digitalnog dokaznog materijala. Većina relevantnih digitalnih dokaza nalazi se na serverima velikih tehnoloških kompanija poput *Meta*-e (*Facebook, Instagram, WhatsApp*), *Alphabet*-a (*Google, YouTube*), *Twitter*-a i drugih, koje su najčešće registrovane u Sjedinjenim Američkim Državama ili drugim razvijenim zemljama, a to stvara složene jurisdikcione probleme kada istražitelji međunarodnih zločina, uključujući genocide, pokušavaju pristupiti tim podacima.

Prema Međunarodnom ugovoru o uzajamnoj pravnoj pomoći (MLAT), pristup digitalnim podacima obično zahtijeva dugotrajan postupak pravne pomoći između država. Kako naglašava Daskal (*Daskal*), ovaj proces često traje mjesecima ili čak godinama, što je neprihvatljivo u kontekstu istrage genocida gdje brzina može biti ključna za spašavanje života i prikupljanje nestabilnih dokaza.[61] U izvještaju *Global Justice Center*-a, identifikovano je prosječno vrijeme od 10 mjeseci za dobijanje digitalnih dokaza putem MLAT procedure, što značajno otežava efikasnu istragu međunarodnih zločina. Pravni okvir za pristup prekograničnim digitalnim dokazima dodatno komplikuju različiti nacionalni zakoni o zaštiti podataka, elektronskoj privatnosti i nacionalnoj bezbjednosti. U Evropskoj uniji, Opšta uredba o zaštiti podataka (GDPR) postavlja stroge uslove za dijeljenje ličnih podataka izvan EU, uključujući i podatke koji mogu biti ključni za istrage genocida. Sa druge strane, američki zakoni poput *CLOUD Act*-a iz 2018. godine omogućavaju američkim

---

58 International Association of Prosecutors (IAP). (2018). *Digital Evidence Challenges in International Prosecutions*. The Hague: IAP Global Prosecutors E-Crime Network.

59 ICC. (2018). *Tužilac protiv Al-Mahdi*, Predmet br. ICC-01/12-01/15, Presuda o reparacijama od 17. augusta 2018.

60 Aronson, J. D., Xu, X. & Roberts, A. (2020). Platform Forensics: Technical Characteristics of Social Media Platforms and Their Implications for Digital Evidence. *Journal of Digital Forensics, Security and Law*, 15(2), pp. 41-65.

61 Daskal, J. (2018). Borders and Bits. *Vanderbilt Law Review*, 71(1), pp. 179-240.

vlastima pristup podacima pohranjenim na serverima američkih kompanija bez obzira na fizičku lokaciju tih servera, ali ne rješavaju pitanje pristupa tim podacima za međunarodne sudove i tribunale.

U nedostatku efikasnog međunarodnog pravnog okvira, saradnja sa tehnološkim kompanijama često se odvija na *ad hoc* osnovi. Nakon kritika zbog uloge *Facebook*-a u podsticanju nasilja protiv Rohindža u Mijanmaru, kompanija je uspostavila posebne protokole za saradnju sa istražiteljima UN-a i Međunarodnog krivičnog suda.[62] Međutim, ova saradnja ostaje dobrovoljna i selektivna, što stvara probleme u pogledu predvidljivosti i pravičnosti postupka. Kao što naglašava Lion, pravda ne bi trebala ovisiti o dobroj volji privatnih korporacija. Važan korak u prevazilaženju jurisdikcionih problema predstavlja stvaranje specijalizovanih mehanizama za prikupljanje digitalnih dokaza o međunarodnim zločinima. Jedan takav primjer je *International, Impartial and Independent Mechanism* (IIIM) uspostavljen od strane Generalne skupštine UN-a 2016. godine za istragu najtežih zločina počinjenih u Siriji. IIIM je razvio protokole za saradnju sa tehnološkim kompanijama i uspostavio digitalnu forenzičku laboratoriju specijalizovanu za analizu i očuvanje digitalnih dokaza.[63] Slični mehanizmi uspostavljeni su i za situaciju u Mijanmaru i Iraku, stvarajući potencijalni model za buduće istrage genocida. Iako predstavljaju pozitivan korak, ovi specijalizovani mehanizmi ne rješavaju fundamentalne jurisdikcione probleme koji proizlaze iz fragmentisanog međunarodnog pravnog sistema. Prema Roksu (*Rox*) i Vangu (*Wang*), postoji hitna potreba za sveobuhvatnim međunarodnim pravnim okvirom koji bi regulisao pristup digitalnim dokazima u slučajevima teških međunarodnih zločina.[64] Takav okvir trebao bi uključivati ubrzane procedure pristupa podacima, jasne standarde za prekograničnu razmjenu podataka i definisane obaveze tehnoloških kompanija u kontekstu istrage genocida i drugih međunarodnih zločina.

Balansiranje prava na privatnost i bezbjednosnih interesa u digitalnim istragama genocida predstavlja treći ključni izazov u očuvanju digitalnog dokaznog materijala. U digitalnom dobu, istrage genocida neizbježno zadiru u privatnost ne samo osumnjičenih počinitelja, već i žrtava, svjedoka i brojnih trećih strana čiji su podaci zabilježeni u digitalnim sistemima što stvara etičke i pravne dileme o granicama istražnih ovlaštenja u odnosu na temeljna ljudska prava. Pravo na privatnost priznato je u brojnim međunarodnim instrumentima, uključujući član 17. Međunarodnog pakta o građanskim i političkim pravima i član 8. Evropske konvencije o ljudskim pravima. Odnosno pravo nije apsolutno i može biti ograničeno radi zaštite legitimnih državnih interesa, uključujući istrage teških krivičnih djela. Međutim, kako naglašava Mekdermot (*Mcdermott*), balans između privatnosti i istražnih potreba posebno je osjetljiv u digitalnom kontekstu, gdje obim potencijalno dostupnih podataka daleko prevazilazi ono što je bilo zamislivo u doba nastanka ovih pravnih instrumenata.[65] U kontekstu istrage genocida, ovaj balans dodatno komplikuje

---

[62] Meta. (2022). *Human Rights Due Diligence Report: Myanmar*. Menlo Park: Meta Platforms, Inc.

[63] IIIM. (2021). *Digital Evidence Workflow and Protocols*. Geneva: International, Impartial and Independent Mechanism for Syria.

[64] Rox, A. & Wang, M. (2022). Building the International Framework for Digital Evidence in Atrocity Crimes Prosecutions. *American Journal of International Law Unbound*, 116, pp. 143-147.

[65] McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1), pp. 1-7.

priroda digitalnih dokaza. Masovne količine podataka generisanih društvenim medijima, komunikacijskim platformama i digitalnim uređajima sadrže informacije ne samo o osumnjičenim počiniteljima, već i o žrtvama, svjedocima i osobama koje nemaju nikakve veze sa istragom. Prema izvještaju *Privacy International*-a, digitalne istrage međunarodnih zločina često dovode do prikupljanja podataka o hiljadama ili čak milionima osoba koje nisu osumnjičene. Takvo masovno prikupljanje podataka otvara ozbiljna pitanja o proporcionalnosti i neophodnosti.[66]

Posebno osjetljivo pitanje odnosi se na privatnost i bezbjednost žrtava i svjedoka. Digitalni dokazi često sadrže detalje o identitetu, lokaciji i aktivnostima žrtava, što može izložiti preživjele dodatnom riziku ako ti podaci nisu adekvatno zaštićeni. U predmetu *Tužilac protiv Ntagande* pred Međunarodnim krivičnim sudom, sud je razvio stroge protokole za zaštitu digitalnih podataka o žrtvama seksualnog nasilja, naglašavajući potrebu za *digitalnom zaštitom svjedoka* kao dopunom tradicionalnih programa zaštite svjedoka.[67] Za adekvatno balansiranje ovih suprotstavljenih interesa, potreban je pristup zasnovan na principima neophodnosti, proporcionalnosti i minimalizma podataka. *The Digital Investigation Protocol* Međunarodnog krivičnog suda[68] definiše ove principe na sljedeći način:

- Neophodnost: digitalni podaci trebaju biti prikupljeni samo kada su neophodni za istragu i kada isti dokazni ciljevi ne mogu biti postignuti manje intruzivnim metodama;
- Proporcionalnost: obim prikupljenih podataka treba biti proporcionalan težini zločina i dokaznoj vrijednosti tih podataka;
- Minimalizam podataka: istražitelji trebaju prikupljati, obrađivati i čuvati najmanju moguću količinu podataka potrebnu za ostvarenje legitimnih istražnih ciljeva.

Primjena ovih principa u praksi predstavlja značajan izazov. Moderne digitalne platforme generišu ogromne količine isprepletenih podataka gdje je teško unaprijed odrediti što je relevantno za istragu. Kao rezultat, istražitelji često moraju prikupiti veće količine podataka, a zatim primijeniti filtere i analitičke alate za identifikaciju relevantnih dokaza. Takav proces otvara dodatna pitanja o algoritmima i metodama korištenim za pretraživanje i analizu digitalnih podataka. Prema Alemanu (*Alemann*) i Boven (*Bowen*), moguće rješenje leži u konceptu zaštite „privatnosti kroz dizajn" (*privacy by design*)[69] u digitalnim istragama; ovaj pristup podrazumijeva ugrađivanje zaštitnih mehanizama privatnosti u sam proces istrage, uključujući automatizovanu anonimizaciju podataka, kontrolisani pristup baziran na ulogama, enkripciju podataka u mirovanju i tranzitu, te rigorozno logovanje pristupa podacima. U kontekstu istrage genocida, *Digital Investigations Lab Univerziteta* u Kaliforniji - *Berkeley* razvio je model „odgovornog prikupljanja digitalnih dokaza"[70] koji uključuje višestruke nivoe zaštite privatnosti žrtava i svjedoka. Važan element u balansiranju privatnosti i istražnih potreba predstavlja i informisani pristanak

---

[66] Privacy International. (2020). *Digital Evidence and International Crimes: Privacy Challenges and Protection Frameworks*. London: Privacy International Report.

[67] ICC. (2019). *Tužilac protiv Ntagande*, Predmet br. ICC-01/04-02/06, Presuda od 8. jula 2019.

[68] ICC. (2021). *Tužilac protiv Ongwena*, Predmet br. ICC-01/04-02/15, Presuda od 4. februara 2021.

[69] Alemann, M. & Bowen, J. (2020). *Privacy by Design in Digital Investigations*. Cambridge: Cambridge University Press.

[70] UC Berkeley Human Rights Center. (2019). *Digital Investigations and the Protection of Vulnerable Populations*. Berkeley: Human Rights Center Working Paper Series.

(*informed consent*). Kada je moguće, istražitelji trebaju dobiti pristanak osoba čiji će podaci biti prikupljeni i korišteni u istrazi. Međutim, u kontekstu genocida, dobijanje takvog pristanka često je nemoguće zbog razmjera zločina, bezbjednosnih rizika i traumatizacije žrtava. U takvim situacijama, kako naglašava Silverman, potrebno je razviti „etičke *proxy*-mehanizme"[71] koji će štititi interese pogođenih zajednica čak i kada formalni pristanak nije moguć. Za rješavanje ovih kompleksnih izazova, međunarodni sudovi i istražna tijela sve više sarađuju sa organizacijama civilnog društva, akademskim institucijama i etičkim odborima. UN-ova *Independent Investigative Mechanism for Myanmar* (IIMM) uspostavila je *Ethics Advisory Board* koji pruža smjernice o etičkim pitanjima u digitalnim istragama, uključujući i pitanja privatnosti.[72] Slične inicijative pokrenuli su i Međunarodni krivični sud i *International, Impartial and Independent Mechanism* (IIIM) za Siriju, stvarajući multidisciplinarni pristup etičkim izazovima digitalnih istraga.

Očuvanje digitalnog dokaznog materijala u istragama genocida zahtijeva i dugoročnu perspektivu. Za razliku od fizičkih dokaza koji mogu trajati desetljećima bez značajne degradacije, digitalni dokazi zahtijevaju aktivno upravljanje tokom cijelog životnog ciklusa, a to uključuje periodičnu migraciju podataka na nove medije, konverziju u nove formate i kontinuirano održavanje metapodataka i dokumentacije o lancu čuvanja. Kako zaključuje *Digital Preservation Coalition*, digitalno očuvanje nije jednokratni zadatak, već kontinuirani proces koji zahtijeva dugoročnu institucionalnu posvećenost i resurse. Odnosno pitanje posebno je relevantno u kontekstu genocida, gdje pravni postupci mogu trajati godinama ili čak decenijama. Digitalni dokazi prikupljeni na početku istrage moraju ostati autentični, dostupni i vjerodostojni tokom cijelog tog perioda. Međunarodni krivični sud je uspostavio *Digital Evidence Vault* – specijalizovani sistem za dugoročno očuvanje digitalnih dokaza koji kombinuje napredne tehnike digitalnog očuvanja sa rigoroznim bezbjednosnim protokolima i lancem čuvanja.[73] Slični sistemi razvijeni su i za *ad hoc* tribunale i specijalizovane međunarodne sudove. Tehnološki napredak kontinuirano mijenja pejzaž digitalnih dokaza, stvarajući nove izazove za istražitelje međunarodnih zločina. Tehnologije poput *end-to-end* enkripcije, decentralizovanih platformi i vještačke inteligencije stvaraju nove tipove digitalnih tragova koji zahtijevaju nove istražne metodologije. Istovremeno, razvoj *deepfake* tehnologija omogućava kreiranje lažnih ali uvjerljivih digitalnih sadržaja, dodatno komplikujući pitanja autentičnosti i vjerodostojnosti. U odgovoru na ove izazove, međunarodna zajednica postepeno razvija multidisciplinarni pristup koji kombinuje pravnu ekspertizu, tehničko znanje, etičke principe i zaštitu ljudskih prava. UN-ova Generalna skupština usvojila je 2022. godine Rezoluciju o međunarodnoj saradnji u digitalnim istragama teških međunarodnih zločina, pozivajući na razvoj zajedničkih standarda, protokola i mehanizama za očuvanje digitalnih dokaza.[74] Navedena rezolucija predstavlja važan korak ka sistematskom rješavanju forenzičkih, jurisdikcionih i etičkih izazova digitalnih istraga.

---

[71] Silverman, J. (2021). Ethical Challenges in Digital Documentation of Mass Atrocities. *Ethics & International Affairs,* 35(2), pp. 235-249.

[72] UN. (2022). *Resolution on International Cooperation in Digital Investigations of Serious International Crimes*. New York: UN General Assembly Resolution A/RES/76/185.

[73] ICC. (2023). *Digital Evidence Management Strategy 2023-2027*. The Hague: International Criminal Court Registry.

[74] UN. (2022). *Resolution on International Cooperation in Digital Investigations of Serious International Crimes*. New York: UN General Assembly Resolution A/RES/76/185.

Regionalne inicijative takođe daju značajan doprinos ovom području. Evropska unija usvojila je *Digital Justice Initiative*[75] koja uključuje razvoj zajedničkih standarda za digitalne dokaze i mehanizme za efikasniju prekograničnu razmjenu podataka. Inicijativa, iako primarno usmjerena na krivično pravosuđe unutar EU, ima značajne implikacije i za međunarodne istrage, uključujući istrage genocida. Za države poput Bosne i Hercegovine razvoj kapaciteta za rad sa digitalnim dokazima ima poseban značaj. Iskustva iz procesuiranja ratnih zločina na Balkanu pokazuju izazove rada sa različitim tipovima digitalnih dokaza – od digitalizovanih vojnih arhiva do presretnutih komunikacija i satelitskih snimaka. Kako se u zadnje vrijeme naglašava ova iskustva mogu pružiti važne lekcije za buduće istrage međunarodnih zločina, posebno u pogledu izazova dugoročnog očuvanja digitalnih dokaza i njihove upotrebe u sudskim postupcima. Očuvanje digitalnog dokaznog materijala u istragama genocida ne smije se posmatrati samo kao tehnički ili pravni izazov, već i kao moralna obaveza prema žrtvama i budućim generacijama. Digitalni dokazi ne služe samo za krivično gonjenje počinitelja, već i za dokumentovanje istorijskih istina, suprotstavljanje negiranju genocida i očuvanje kolektivnog sjećanja. U tom smislu, izazovi očuvanja digitalnog dokaznog materijala nisu samo pitanje pravosudne efikasnosti, već i fundamentalno pitanje pravde, istine i prevencije budućih zločina. Za efektivno suočavanje sa tehnološkim i pravnim izazovima očuvanja digitalnog dokaznog materijala u istragama genocida, potreban je holistički pristup koji kombinuje tehničku inovaciju, pravnu adaptaciju i etičku refleksiju. Međunarodno krivično pravo mora evoluirati kako bi adekvatno odgovorilo na izazove digitalne ere, istovremeno čuvajući svoje temeljne principe – pravičnost postupka, poštovanje ljudskih prava i posvećenost borbi protiv nekažnjivosti za najteže međunarodne zločine.

5. ZAKLJUČAK

Provedeno istraživanje nedvosmisleno ukazuje na fundamentalnu transformaciju doktrine dokazivanja genocidne namjere u digitalnom dobu. Kroz analizu recentne jurisprudencije međunarodnih sudova i primjenu interdisciplinarnog metodološkog okvira, rad je rezultirao nekoliko inovativnih naučnih doprinosa. Prvo, identifikovan je fenomen „digitalne pluralizacije indicija" – proces u kojem klasična indicijalna metoda utvrđivanja genocidne namjere biva proširena novim kategorijama digitalnih tragova koji zahtijevaju specifične interpretativne okvire. Nova konceptualna inovacija omogućava sudovima da sistematizuju evaluaciju raznovrsnih digitalnih dokaza, od strukturisanih metapodataka do nestrukturisanih narativa na društvenim mrežama. Drugo, rad formuliše originalni teorijski model „kaskadne pripisivosti" za povezivanje online sadržaja sa fizičkim počiniocima i donosiocima odluka. Takav model prevazilazi tradicionalne doktrine komandne odgovornosti, uvodeći dinamički pristup koji odražava kompleksnost digitalnih komunikacijskih lanaca u hijerarhijskim strukturama. Treće, razvijen je koncept „digitalne kontekstualizacije" koji omogućava pravilnu evaluaciju izolovanih digitalnih fragmenata unutar šireg narativa genocidnog djelovanja. Pristup rješava ključni epistemološki izazov – tumačenje fragmentisanih digitalnih dokaza unutar koherentnog pravnog okvira genocidne namjere. Istraživanje je rezultiralo inovativnim normativnim okvirom za balansiranje procesne efikasnosti i zaštite prava optuženih pri korištenju digitalnih dokaza. Predloženi model

[75] European Commission. (2021). *Digital Justice Initiative: Final Report and Recommendations*. Brussels: European Commission Justice and Consumers Directorate.

proporcionalne digitalne inkluzije osigurava da ekspanzija dokazne baze ne kompromitira temeljna načela pravičnog suđenja, stvarajući osnovu za legitimno i efikasno procesuiranje genocida u digitalnom dobu. Rezultati značajno doprinose razvoju međunarodnog krivičnog prava, nudeći konceptualne alate prilagođene kompleksnim izazovima dokazivanja najspecifičnije kriminalne namjere u kontekstu tehnološke transformacije dokaznih sredstava.

6. LITERATURA

Abtahi, H. & Webb, P. (2008). *The Genocide Convention: The Travaux Préparatoires (2 vols)*. Leiden: Martinus Nijhoff Publishers.

Alemann, M. & Bowen, J. (2020). *Privacy by Design in Digital Investigations*. Cambridge: Cambridge University Press.

Aronson, J. D., Xu, X. & Roberts, A. (2020). Platform Forensics: Technical Characteristics of Social Media Platforms and Their Implications for Digital Evidence. *Journal of Digital Forensics, Security and Law*, 15(2), pp. 41-65.

Banaji, S., Bhat, R., Agarwal, A., Passanha, N. & Saeed, M. (2022). *Digital Misinformation and Mob Violence*. Oxford: Oxford University Press.

Casey, E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (4. izd.). London: Academic Press.

Cassese, A., Baig, L., Fan, M. & Gaeta, P. (2022). *International Criminal Law* (4. izd.). Oxford: Oxford University Press.

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A. & Weir, D. (2019). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict & Terrorism*, 42(1-2), pp. 141-160.

Daskal, J. (2018). Borders and Bits. *Vanderbilt Law Review*, 71(1), pp. 179-240.

Digital Preservation Coalition. (2023). *Digital Preservation Handbook* (3. izd.). Glasgow: Digital Preservation Coalition.

Dubberley, S., Koenig, A. & Murray, D. (2020). *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford: Oxford University Press.

ECCC. (2018). *Tužilac protiv Osapina*, Predmet br. 002/19-09-2007/ECCC/TC, Presuda od 16. novembra 2018.

European Commission. (2021). *Digital Justice Initiative: Final Report and Recommendations*. Brussels: European Commission Justice and Consumers Directorate.

Freeman, L. & Lyle, J. (2021). Volatile Data in Digital Investigations: Techniques and Challenges. *Forensic Science International: Digital Investigation*, 36, pp. 301034-301047.

Freeman, L., Hayes, B., Law, I. & Williams, D. (2020). Digital command responsibility: Creating accountability for mass atrocities in the age of social media. *Columbia Human Rights Law Review*, 52(1), pp. 116-187.

Global Justice Center. (2020). *Digital Evidence and International Crimes: Access, Sharing and Admissibility*. New York: GJC Policy Report.

Gordon, G. S. (2017). *Atrocity Speech Law: Foundation, Fragmentation, Fruition*. Oxford: Oxford University Press.

Human Rights Watch. (2018). *"They Were Going to Kill Us All": Rohingya Muslim Genocide in Myanmar*. New York: Human Rights Watch Report.

ICC. (2010). *Tužilac protiv Al Bashira*, Predmet br. ICC-02/05-01/09, Odluka po drugom zahtjevu tužilaštva za izdavanje naloga za hapšenje od 12. jula 2010.

ICC. (2014). *Tužilac protiv Katange*, Predmet br. ICC-01/04-01/07, Presuda od 7. marta 2014.

ICC. (2016). *Tužilac protiv Bembe*, Predmet br. ICC-01/05-01/13, Presuda od 19. oktobra 2016.

ICC. (2017). *Tužilac protiv Al-Werfalli*, Predmet br. ICC-01/11-01/17, Nalog za hapšenje od 15. augusta 2017.

ICC. (2018). *Tužilac protiv Al-Mahdi*, Predmet br. ICC-01/12-01/15, Presuda o reparacijama od 17. au-

gusta 2018.

ICC. (2019). *Tužilac protiv Ntagande*, Predmet br. ICC-01/04-02/06, Presuda od 8. jula 2019.

ICC. (2021). *Digital Investigation Protocol*. The Hague: International Criminal Court Office of the Prosecutor.

ICC. (2021). *Tužilac protiv Ongwena*, Predmet br. ICC-01/04-02/15, Presuda od 4. februara 2021.

ICC. (2023). *Digital Evidence Management Strategy 2023-2027*. The Hague: International Criminal Court Registry.

ICJ. (2007). *Bosna i Hercegovina protiv Srbije i Crne Gore*, Presuda od 26. februara 2007.

ICTR. (1998). *Tužilac protiv Akayesu*, Predmet br. ICTR-96-4-T, Presuda od 2. septembra 1998.

ICTR. (2003). *Tužilac protiv Nahimane, Barayagwize i Ngezea*, Predmet br. ICTR-99-52-T, Presuda od 3. decembra 2003.

ICTY. (2010). *Tužilac protiv Popovića i drugih*, Predmet br. IT-05-88-T, Presuda od 10. juna 2010.

ICTY. (2016). *Tužilac protiv Karadžića*, Predmet br. IT-95-5/18-T, Presuda od 24. marta 2016.

ICTY. (2017). *Tužilac protiv Mladića*, Predmet br. IT-09-92-T, Presuda od 22. novembra 2017.

ICTY. (2018). *Tužilac protiv Šešelja*, Predmet br. IT-03-67-A, Presuda od 11. aprila 2018.

IIIM. (2021). *Digital Evidence Workflow and Protocols*. Geneva: International, Impartial and Independent Mechanism for Syria.

International Association of Prosecutors (IAP). (2018). *Digital Evidence Challenges in International Prosecutions*. The Hague: IAP Global Prosecutors E-Crime Network.

International Association of Prosecutors (IAP). (2019). *Global Review of the Use of Digital Evidence in International Criminal Courts and Tribunals*. The Hague: IAP Digital Evidence Working Group Report.

Kastner, P. (2018). International Criminal Law in the Age of Social Media. *Journal of International Criminal Justice*, 16(4), pp. 813-840.

Koettl, C. (2016). Citizen Media Research and Verification: An Analytical Framework for Human Rights Practitioners. *Human Rights Practice*, 8(2), pp. 1-23.

Krstić, D. (2020). Dokazivanje genocidne namjere u međunarodnom krivičnom pravu: tradicionalni i savremeni pristupi. *Godišnjak Pravnog fakulteta u Sarajevu*, LXIII, pp. 255-278.

Lyons, A. (2019). The role of tech companies in international criminal investigations. *American Society of International Law Proceedings*, 113, pp. 300-304.

Lyons, A. (2021). Corporate Discretion in International Criminal Evidence. *Georgetown Journal of International Law*, 52(4), pp. 865-912.

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1), pp. 1-7.

Meta. (2021). *Content Policy Stakeholder Engagement Report – Q4 2021*. Menlo Park: Meta Platforms, Inc.

Meta. (2022). *Human Rights Due Diligence Report: Myanmar*. Menlo Park: Meta Platforms, Inc.

Mettraux, G. (2021). *International Crimes: Law and Practice (Volume I): Genocide*. Oxford: Oxford University Press.

Privacy International. (2020). *Digital Evidence and International Crimes: Privacy Challenges and Protection Frameworks*. London: Privacy International Report.

Rox, A. & Wang, M. (2022). Building the International Framework for Digital Evidence in Atrocity Crimes Prosecutions. *American Journal of International Law Unbound*, 116, pp. 143-147.

Schabas, W. A. (2009). *Genocide in International Law: The Crime of Crimes* (2. izd.). Cambridge: Cambridge University Press.

Schabas, W. A. (2022). *An Introduction to the International Criminal Court* (7. izd.). Cambridge: Cambridge University Press.

Silverman, J. (2021). Ethical Challenges in Digital Documentation of Mass Atrocities. *Ethics & International Affairs*, 35(2), pp. 235-249.

Smeulers, A. & van der Wijngaart, R. (2016). The proof is in the pudding: The value of digital evidence in proving international crimes. *Journal of International Criminal Justice*, 14(4), pp. 723-746.

STL. (2015). *Tužilac protiv Ayyasha i drugih*, Predmet br. STL-11-01/T, Odluka o prihvatljivosti telefon-

skih dokaza od 14. aprila 2015.

UC Berkeley Human Rights Center. (2019). *Digital Investigations and the Protection of Vulnerable Populations*. Berkeley: Human Rights Center Working Paper Series.

UN. (1948). Konvencija o sprečavanju i kažnjavanju zločina genocida. Usvojena Rezolucijom 260 (III) A Generalne skupštine Ujedinjenih nacija od 9. decembra 1948.

UN. (2019). *Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar*. Geneva: UN Human Rights Council, A/HRC/42/CRP.5.

UN. (2020). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. Geneva: Office of the United Nations High Commissioner for Human Rights.

UN. (2022). *Resolution on International Cooperation in Digital Investigations of Serious International Crimes*. New York: UN General Assembly Resolution A/RES/76/185.

Wilson, R. A. (2017). Inciting Genocide with Words. *Michigan Journal of International Law*, 36(2), pp. 277-320.

Decoding Genocidal Intent: Legal Evolution of Evidentiary Standards in the Digital Era

Slaven Knežević, MA
PhD student at the Faculty of Political Sciences, University of Banja Luka and master's student at the Faculty of Law and Faculty of Economics, University of Banja Luka. slaven.knezevic998@gmail.com

Abstract: This paper explores the transformation of the process of proving genocidal intent (dolus specialis) in the context of the digital revolution that has fundamentally changed the way evidence is documented, analyzed, and presented before international criminal courts. Through an analysis of the evolution from traditional evidentiary means to sophisticated digital traces, the paper identifies key legal, forensic, and ethical challenges faced by prosecutors, judges, and investigators in prosecuting the crime of crimes in the digital environment. The central focus of the paper is directed at three interconnected aspects: the methodology of collecting and verifying digital evidence, the legal qualification of online content as elements of genocidal intent, and the problem of attributing digital material to specific perpetrators. By applying an interdisciplinary methodological framework that combines normative-analytical method, comparative analysis of case law, and empirical research of specific cases, the paper formulates innovative concepts such as „digital pluralization of indicia", „cascading attribution", and „digital contextualization" as tools for overcoming the identified challenges. Through a critical evaluation of the practice of international tribunals (ICTY, ICTR, ICC) and specialized investigative mechanisms, the paper develops a coherent theoretical model for evaluating digital evidence of genocidal intent that balances the need for efficient prosecution with the imperatives of fair trial and human rights protection. The research results are intended for legal practitioners in the field of international criminal law, war crimes investigators, digital forensic experts, and policy makers working on developing normative frameworks for digital investigations of serious international crimes.

Keywords: international criminal law, genocidal intent, digital evidence, forensic verification, social media.