Irena R. Čučilović*

Pregledni naučni članak
UDK: 343.533::004
doi: https://doi.org/10.56461/SPZ_1140
Primljeno: 15. 8. 2025.
Prihvaćeno: 2. 12. 2025.
Online First: 3. 12. 2025.

ANONIMNOST I DIGITALNE GRANICE PRAVA: IZAZOVI VISOKOTEHNOLOŠKOG KRIMINALITETA I NOVE ISTRAŽNE TEHNIKE

Sažetak

U radu se analiziraju izazovi koje anonimnost korisnika interneta, pre svega TOR mreže i *darkneta*, postavlja pred krivičnopravnu teoriju i praksu. Centralni deo rada odnosi se na studiju slučaja *Playpen*, odnosno na pravne i etičke dileme koje su se pojavile u kontekstu operacije *Playpen*, u okviru koje je FBI koristio malver za identifikaciju korisnika sajta dečje pornografije. Autorka razmatra upotrebu sofisticiranih tehničkih sredstava u kontekstu zaštite prava na privatnost, sa posebnim osvrtom na četvrti amandman Ustava SAD i praksu američkih sudova. U zaključnom delu rada, autorka iznosi stav da efikasna borba protiv visokotehnološkog kriminaliteta zahteva pažljivo normiranje novih posebnih dokaznih radnji, koje bi omogućile proporcionalnu, zakonitu i sudski kontrolisanu primenu sofisticiranih tehničkih sredstava za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata.

Ključne reči: darknet, TOR, Playpen, privatnost, posebne dokazne radnje.

* Advokat, doktor pravnih nauka, Beograd, Srbija.

E-mail: *irena@advokatskitim.rs*
ORCID: *https://orcid.org/0009-0000-5823-780X*

ANONYMITY AND THE DIGITAL BOUNDARIES OF LAW: CALLENGES OF HIGH-TECH CRIME AND NEW INVESTIGATIVE TECHNIQUES

Summary

This paper examines the challenges that user anonymity on the internet, particularly on the TOR network and darknet, poses to contemporary criminal law theory and practice. The central focus is a case study of Operation Playpen, addressing the legal and ethical dilemmas arising from the FBI's use of malware to identify users of a child pornography website. The analysis explores the deployment of sophisticated technical tools in light of the right to privacy, with particular emphasis on the Fourth Amendment to the U.S. Constitution and relevant U.S. case law. The author concludes that effectively combating high-tech crime requires the precise legislative regulation of new special investigative measures, enabling the proportionate, lawful and judicially supervised use of advanced technological tools to de-anonymize users of digital communication networks and platforms.

Keywords: Darknet, TOR, Malware, Playpen, Privacy, Special Investigative Measures.

1. Uvod

U literaturi se često kao prvi poznati slučaj izvršenja krivičnog dela putem računarske mreže navodi anegdota o *online* kupoprodaji droge između dva studenta sa Harvarda[1] početkom sedamdesetih godina prošlog veka putem platforme *ARPANET*, koja se smatra pretečom savremenog interneta (Shortis, Aldrige & Barratt, 2020, p. 357; Omar & Ibrahim, 2020, p. 111). Od sedamdesetih godina prošlog veka do danas razvoj informacionih tehnologija zabeležio je eksponencijalni rast, što je doprinelo značajnoj rasprostranjenosti visokotehnološkog kriminaliteta (Phillips *et al.*, 2022, p. 379). Ključni problem na nivou suzbijanja i sprečavanja visokotehnološkog kriminaliteta predstavlja činjenica da postojeći normativni okvir nije formulisan prema osnovnim fenomenološkim osobenostima ovog oblika kriminaliteta, što ga čini nedelotvornim u oblasti borbe protiv visokotehnološkog kriminaliteta.

[1] Prema dostupnim podacima u literaturi, u konkretnom slučaju je dogovor o kupoprodaji marihuane učinjen putem platforme *Arpanet,* dok je primopredaja izvršena fizički.

Iz dana u dan neophodnost reforme krivično-procesnog zakonodavstva postaje sve očiglednija, dok su izazovi sa kojima se pravna nauka suočava u ovom procesu sve ozbiljniji (Pisarić, 2013).

U ovom trenutku je jasno da je efikasno suzbijanje i sprečavanje visokotehnološkog kriminaliteta u direktnoj koliziji sa zahtevom za poštovanje prava na privatnost (Prlja & Reljanović, 2009, pp. 164-165). Očigledno je da su tradicionalne dokazne radnje gotovo potpuno neefikasne kada je u pitanju otkrivanje, rasvetljavanje i dokazivanje krivičnih dela visokotehnološkog kriminaliteta, dok se posebne dokazne radnje, izvorno oblikovane prema fenomenološkim karakteristikama organizovanog kriminaliteta (Škulić, 2018, pp. 539-544), suočavaju sa nepremostivim preprekama. U tom kontekstu postavlja se pitanje: da li je opravdano dalje ograničavanje ljudskih prava zarad efikasnosti krivičnog gonjenja i gde se nalazi granica između legitimne represije i zaštite osnovnih ljudskih prava u digitalnom dobu?

Autorka u ovom radu ukazuje na ključne fenomenološke karakteristike visokotehnološkog kriminaliteta, koje zahtevaju preispitivanje tradicionalnih postulata krivičnog procesnog prava i prava ljudskih prava. Uvažavajući sve potencijalne opasnosti koje prete osnovnim ljudskim pravima u digitalnoj eri, ona ističe da razvoj krivičnog procesnog prava mora pratiti razvoj informacionih tehnologija. U suprotnom ćemo se, figurativno rečeno, protiv nuklearnog oružja boriti mačem. Sa ciljem da se razumeju razlozi zbog kojih su opšte i posebne dokazne radnje nedelotvorne pri istraživanju krivičnih dela izvršenih na *darknetu*, kao i pravne i etičke dileme koje su vezane za korišćenje sofisticiranih tehničkih sredstava u krivičnim postupcima, u radu je izložena studija slučaja *Playpen,* uz analizu relevantnih sudskih odluka vezanih za operaciju *Playpen*. U radu su primenjeni normativni i uporednopravni metodi. Na osnovu analize fenomenoloških karakteristika visokotehnološkog kriminaliteta, međunarodnih dokumenata i relevantne sudske prakse, autorka ukazuje na neophodnost normiranja novih posebnih dokaznih radnji koje bi omogućile proporcionalnu, zakonitu i sudski kontrolisanu primenu sofisticiranih tehničkih alata za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata.

2. Specifičnosti visokotehnološkog kriminaliteta i *darknet*

Nagli razvoj interneta i informaciono-komunikacionih tehnologija doveo je do pojave novih krivičnih dela koja po svojoj prirodi, načinu ili sredstvu izvršenja podrazumevaju zloupotrebu računarskih sistema, mreža ili digitalnih tehnologija (Đukić, 2018, p. 130; Karović & Simović, 2022, p. 47). Osim pojave novih krivičnih

dela, razvoj informaciono-komunikacionih tehnologija doveo je i do premeštanja tradicionalnih krivičnih dela iz *offline* u *online* prostor (Buxton & Bingham, 2015). I pored aktivnog naučnog i praktičnog delovanja na polju borbe protiv krivičnih dela povezanih sa informaciono-komunikacionim tehnologijama (IKT), u pravnoj nauci još uvek ne postoji jedinstvena i opšteprihvaćena definicija visokotehnološkog kriminaliteta (Barrio Andres, 2011; Pisarić, 2013, p. 292; Phillips *et al.*, 2022). Prema Budimpeštanskoj konvenciji, visokotehnološki kriminalitet obuhvata tri vrste krivičnih dela: krivična dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema, krivična dela u vezi sa računarima i krivična dela sadržaja (ETS No. 185, 2001). Ova klasifikacija, iako najšire prihvaćena u međunarodnom kontekstu, ne iscrpljuje sve oblike visokotehnološkog kriminaliteta koji se javljaju u praksi.

Ne ulazeći detaljnije u teorijska pitanja o podelama i ontološkim razlikama unutar pojma visokotehnološkog kriminaliteta (Wall, 2017; Phillips *et al.*, 2022), ključno je istaći da su njegove fenomenološke osobenosti, uključujući anonimnost, transnacionalnost i digitalnu volatilnost dokaza, neposredna posledica sofisticirane prirode savremenih IKT sistema.

2.1. Tehničke karakteristike darkneta

Činjenica da ljudi putem interneta mogu u jednoj državi preduzeti radnju koja će prouzrokovati posledicu u drugoj državi ili u više drugih država, pri čemu to mogu činiti gotovo potpuno anonimno, jasno ukazuje na brojne potencijalne probleme u otkrivanju, dokazivanju i gonjenju učinilaca krivičnih dela koja se vrše *online* (Pisarić, 2013, p. 292; Baron Quintero, 2023, p. 176; Čučilović, 2025, p. 326).

U kontekstu otkrivanja i dokazivanja krivičnih dela izvršenih u *online* prostoru bitno je da znamo da svaki uređaj koji se povezuje na mrežu zasnovanu na internet protokolu ima jedinstveni brojčani identifikator – takozvanu IP adresu,[2] čija je osnovna funkcija identifikacija uređaja i omogućavanje međusobne komunikacije između njih preko interneta (Đukić, 2025, p. 149). Upravo je praćenje IP adrese prvi korak ka identifikovanju osumnjičenog kada su u pitanju krivična dela izvršena *online* (Kumar Shrivastava, 2021, p. 47). Problem je, međutim, u tome što je svega oko 4% sadržaja na internetu vidljivo i dostupno korisnicima uobičajenih veb-pretraživača, dok najveći deo interneta čini takozvani *deepweb*, čiji sadržaj nije indeksiran te je za pristup navedenom sadržaju neophodno korišćenje posebnih softvera, koji su kreirani tako da dodatno štite anonimnost korisnika. Treba ukazati da veći deo sadržaja koji se nalazi na *deepweb*-u nije kriminalan, već su u pitanju potpuno legalni sadržaji koji nisu dostupni javnosti

[2] Internet Protocol Address.

zbog zaštite privatnosti ili poverljivosti informacija[3] (Omar & Ibrahim, 2020, p. 110; Kumar Shrivastava, 2021, p. 46).

Budući da se u standardnoj IP komunikaciji saobraćaj odvija direktno između pošiljaoca i primaoca, obe strane posredno otkrivaju međusobne IP adrese, čime je narušena anonimnost. TOR[4] mreža, koja se zasniva na *Onion rutiranju,* prvobitno razvijena u okviru istraživačkog projekta američke mornarice i NSA, u cilju bezbedne komunikacije vladinih agencija i novinara, 2002. godine postala je dostupna i širem građanstvu (Buxton & Bingham, 2015, p. 5; Korać, Prlja & Diligenski, 2016, p. 357). Upravo je mogućnost privatnih lica da pristupe TOR mreži dominantno uticala na pojavu i širenje takozvanog *darkneta* koji se koristi za obavljanje kriminalne delatnosti i plasiranje kriminalnih ideja, a koji u suštini čini samo jedan mali deo *deepweb*-a (Kumar Shrivastava, 2021, p. 46).

Suština TOR mreže se ogleda u tome što se umesto uspostavljanja direktne komunikacije između uređaja na mreži, komunikacija odvija preko određenog broja *nodova*, odnosno čvorova (Korać, Prlja & Diligenski, 2016, p. 357). Čvorova za *rutiranje* saobraćaja u mreži ima najmanje tri. Prvi (ulazni) čvor u lancu zna IP adresu i lokaciju korisnika, ali ne zna krajnju destinaciju. Srednji čvor zna prethodni i sledeći sloj u lancu, ali ne zna ko su korisnici ni ka kome je zahtev upućen. Poslednji (izlazni) čvor dešifruje poslednji sloj i prosleđuje zahtev ka željenoj destinaciji, ali mu je nepoznata početna destinacija (Dinglendine, Mathewson & Syverson, 2004).

Upravo ove tehničke karakteristike TOR mreže i *darkneta* dodatno komplikuju otkrivanje identiteta izvršilaca i dokazivanje krivičnih dela u digitalnom prostoru, čime se dovodi u pitanje delotvornost postojećih tradicionalnih dokaznih mehanizama.

2.2. Ograničenja posebnih dokaznih radnji u digitalnom prostoru

Darknet je deo TOR mreže na kojoj se nalaze skriveni servisi dostupni samo unutar TOR mreže. Van TOR mreže, lokacije (serveri) ovih servisa ostaju nepoznati i nevidljivi. Zahvaljujući ovim karakteristikama, *darknet* sadrži i servise na kojima se obavljaju kriminalne delatnosti, poput trgovine drogom ili dečje pornografije, iako se deo sadržaja odnosi i na legalne aktivnosti koje zahtevaju visok nivo anonimnosti, poput novinarstva ili političkog aktivizma pod represivnim režimima (Omar & Ibrahim, 2020, p. 111). *Linkovi* za ulaz na *darknet* servis nalaze se na skrivenim direktorijumima (npr. „*The Hidden Wiki*“) kojima je moguće pristupiti korišćenjem TOR pretraživača (Korać, Prlja & Diligenski, 2016, p. 360).

[3] Na primer, serveri državnih organa, privatnih kompanija, e-mail naloga i sl.

[4] The Onion Router.

Kada se putem TOR pretraživača uspostavi pouzdana komunikacija sa prvim čvorom u TOR mreži, podaci se *enkriptuju* i šalju kroz zamršenu mrežu „tunela" u TOR mreži, sve do izlaznog čvora koji sadrži potpuno otvorenu informaciju koja nije *enkriptovana*. Osnovna ideja TOR mreže je da nijedan pojedinačni čvor u lancu nema kompletan uvid u celu putanju i identitet, pri čemu se i same putanje periodično automatski menjaju (Korać, Prlja & Diligenski, 2016, p. 358). Ako zahvaljujući ljudskoj grešci, uz pomoć OSINT-a[5], istražni organi i dođu do skrivenog sajta sa inkriminišućim sadržajem, nije moguće rekonstruisati rutu do prvog čvora koji zna IP adresu stvarnog korisnika, upravo zahvaljujući *enkripciji* i decentralizaciji TOR mreže. Istražnim organima je u tom slučaju poznat samo sadržaj sajta i IP adresa poslednjeg čvora (Chertoff & Jardine, 2021, p. 2). Na taj način, anonimnost izvršioca krivičnog dela ostaje zaštićena.

Stoga, iako tehnički postoji mogućnost da istražni organi otkriju postojanje inkriminišućeg sadržaja na *darknetu*, činjenica da ne mogu identifikovati korisnika kao konkretno fizičko lice čini primenu opštih i posebnih dokaznih radnji procesno neizvodljivom.

3. Studija slučaja – operacija *Playpen*

Playpen je bio sajt dečje pornografije na *darknetu*. U decembru 2014. godine, FBI je dobio informaciju da server na kome je *hostovan Playpen* sajt ima grešku u konfiguraciji koja otkriva pravu IP adresu i lokaciju servera (Chertoff & Jardine, 2021, p. 3). FBI je u januaru 2015. godine zaplenio server *Playpen*-a i odneo ga u svoje prostorije u Istočnoj Virdžiniji. FBI nije javno objavio da je zaplenio server *Playpen*-a, niti je korisnicima onemogućavao pristup sajtu. Međutim, TOR mreža je štitila identitet korisnika i administratora *Playpen*-a. Po zahtevu FBI-ja, sud u Istočnoj Virdžiniji je 20. februara 2015. godine izdao takozvani NIT (*Network Investigative Technique*) nalog, kojim se FBI-ju dozvoljava korišćenje specijalizovanog softverskog alata za identifikaciju korisnika, te tako omogućio da FBI identifikuje oko 100.000 korisnika *Playpen*-a, koliko ih je pristupilo ovom sajtu u periodu od 20. februara do 4. marta 2015. godine (*United States v Wagner*, 2020, p. 3).

NIT je zapravo *malver* koji je FBI infiltrirao u server koji je *hostovao Playpen*. U trenutku kada korisnik pristupi *Playpen*-u unošenjem korisničkog imena i lozinke, istovremeno na svoj računar preuzima i NIT, koji je zatim na server pod kontrolom FBI-ja slao određene informacije, između ostalog i IP adresu računara sa kojeg je pristupljeno *Playpen*-u (*United States v. Levin*, 2017, p. 6).

[5] Open-Source Intelligence – prikupljanje podataka i informacija iz otvorenih i javno dostupnih izvora na internetu (Bugarski, 2020, p. 182).

Ovakav način prikupljanja dokaza, iako izuzetno efikasan, otvorio je brojna pravna pitanja u vezi sa jurisdikcijom, pravom na privatnost i zakonitošću korišćenja *malvera* u krivičnom postupku.

3.1. Pravne dileme u sudskoj praksi i odjeci u pravnoj nauci

Pošto se server *Playpen*-a nalazio na teritoriji Istočne Virdžinije, nalog za korišćenje *malvera* NIT izdao je sud u Istočnoj Virdžiniji. S obzirom na to da je reč o specifičnom tehničkom sredstvu čija je upotreba vezana za digitalni prostor u kome nema državnih, regionalnih, okružnih ni drugih fizičkih granica, identifikovane su IP adrese korisnika sajta koji su se nalazili širom SAD. Treba naglasiti da je NIT prikupljao isključivo podatke o uređaju i njegovim tehničkim karakteristikama (tzv. *non-content data*), poput IP adrese, MAC adrese i operativnog sistema, dok nije zahvatao sadržinu komunikacije, što je relevantno i u pogledu njegovog ustavnopravnog tretmana.[6] Nakon identifikovanja IP adrese korisnika, FBI je pribavljao nove naloge za pretres stana i računara konkretnog osumnjičenog od mesno nadležnog suda, prema mestu nalaženja računara (*United States v. Levin,* 2017, p. 7; *United States v. Anzalone*, 2019, p. 4; *United States v. Wagner*, 2020, p. 4). Pretragom računara konkretnih osumnjičenih pronađeni su inkriminišući materijali dečje pornografije, te je većina osumnjičenih optužena za posedovanje materijala dečje pornografije.

U krivičnim postupcima koji su proistekli iz operacije *Playpen* otvorila su se brojna sporna pitanja, oko kojih nije postojao jedinstven stav ni u sudskoj praksi ni u pravnoj teoriji.

3.1.1. Nadležnost i član 41 Federalnih pravila o krivičnom postupku

Prvo sporno pitanje odnosilo se na potencijalno kršenje člana 41 Federalnih pravila o krivičnom postupku (Federal Rules of Criminal Procedure – Fed. R. Crim. P., 2016) od strane suda u Istočnoj Virdžiniji. Odbrana je gotovo jednoglasno isticala da sud u Istočnoj Virdžiniji nije imao nadležnost za izdavanje NIT naloga koji bi važio izvan teritorije njegovog okruga. Apelacioni sud je utvrdio da su prigovori odbrane neosnovani jer se NIT nalog odnosio na server koji se nalazio na teritoriji suda koji ga je izdao (*United States v. Levin*, 2017; *United States v. Anzalone*, 2019; *United States v. Wagner*, 2020). U slučaju *United States v. Matish* sud je instaliranje *malvera* u virtuelnom svetu tumačio analogno instaliranju uređaja za praćenje u realnom svetu, te zaključio da se može smatrati da je korisnik otišao na virtuelni

[6] Više o razlici između *content data* i *non-content data*, načinu na koji se pribavljaju i njihovom dokaznom tretmanu vid. Bugarski, 2020.

put u Istočnu Virdžiniju na čijoj se teritoriji nalazio server *Playpen*-a svaki put kada je pristupio sajtu (Widenhouse, 2017, p. 157). Međutim, ovakvo rezonovanje suda je oštro kritikovano u delu teorije u kome se smatra da mesto pretresa nije bio server *Playpen*-a u Istočnoj Virdžiniji, već računar korisnika koji se nalazio van teritorijalne nadležnosti suda koji je nalog izdao (Widenhouse, 2017, p. 162).

Iako zbog zabrane retroaktivnog dejstva zakona nema uticaja na slučajeve proistekle iz operacije *Playpen,* ova operacija je ostvarila značajan uticaj na normativnom planu i direktno doprinela reformi procesnog zakonodavstva SAD, koje sada eksplicitno dozvoljava sudu na čijoj bi se teritoriji mogle dogoditi aktivnosti povezane sa krivičnim delom da izda nalog za korišćenje daljinskog pristupa za pretres elektronskog skladišta, za zaplenu ili kopiranje elektronski sačuvanih informacija koje se nalaze unutar ili van tog okruga, ukoliko je okrug u kome se nalaze mediji ili informacije prikriven upotrebom tehnoloških sredstava (Fed. R. Crim. P., 2016, 41(b) (6)).

3.1.2. Četvrti amandman i IP adresa

Drugo sporno pitanje odnosilo se na potencijalno kršenje četvrtog amandmana Ustava SAD, koji štiti pravo pojedinaca na privatnost, odnosno sigurnost njihove ličnosti, domova, prepiske i stvari od neopravdanih pretresa i zaplena (Widenhouse, 2017, p. 149). Kako bi pružio efektivnu zaštitu proklamovanom pravu na privatnost, četvrti amandman zahteva da svako zadiranje države u privatnu sferu pojedinca ima svoj osnov u sudskom nalogu. Da bi bio zakonit, sudski nalog mora ispuniti tri kumulativno propisana uslova: 1) mora ga izdati nadležan sud, 2) mora se zasnivati na krivično-procesno relevantnom stepenu sumnje (tzv. *probable cause*) i 3) mora biti određen kako u pogledu mesta koje se pretresa, tako i u pogledu predmeta i lica koje se pleni, odnosno zadržava (tzv. *particularity*) (*United States v. Wagner,* 2020, p. 9). Pravo na privatnost u SAD je korigovano takozvanom doktrinom trećeg lica *(Third-party doctrine)*, prema kojoj informacije koje je osumnjičeni dobrovoljno podelilo sa trećim licima ne uživaju zaštitu po četvrtom amandmanu, te organima krivičnog gonjenja za njihovo pribavljanje nije neophodan sudski nalog (Widenhouse, 2017, p. 157).

Ograničenja doktrine trećeg lica uspostavljena u presudi *Carpenter v. United States* označila su prelomni trenutak u razumevanju digitalne privatnosti, pomerajući fokus sa toga kome su tehnički dostupni podaci na to da li pojedinac zadržava legitimno očekivanje privatnosti nad tim podacima, što direktno utiče na tumačenje da li je pribavljanje IP adrese putem NIT-a zaštićeno ili ne. Naime, sama činjenica da je osumnjičeni pristupio *darknetu* i podelio svoju IP adresu sa TOR čvorom, ne znači da je odustao od zaštite svoje privatnosti (*Carpenter v. United States*, 2018,

pp. 18-23). Uprkos tome, apelacioni sudovi u SAD nisu zauzeli jedinstven stav u pogledu pitanja da li primena NIT-a predstavlja pretres u smislu četvrtog amandmana. Uopšteno govoreći, oni sudovi koji su se fokusirali na IP adresu smatrali su da ne postoji legitimno očekivanje privatnosti u vezi sa IP adresom, te da u konkretnom slučaju nije došlo do pretresa. S druge strane, sudovi koji su korišćenje NIT-a tumačili kao upad u zaštićeno digitalno okruženje smatrali su da je u konkretnom slučaju došlo do pretresa (Widenhouse, 2018, p. 159). U slučajevima u kojima je primena NIT-a posmatrana kao pretres, sudovi su smatrali da je NIT nalog izdat od strane suda u Istočnoj Virdžiniji ispunjavao propisane uslove u pogledu osnovane sumnje (sajt na *darknetu*, neophodnost unošenja korisničkog imena i lozinke za pristup sajtu, naslovna strana sajta koja je ukazivala na nezakonitu sadržinu sajta) i određenosti (jasno su precizirana lica prema kojima se nalog primenjuje – korisnici *Playpen*-a, i digitalni podaci koji će biti prikupljeni[7]) (*United States v. Levin*, 2017; *United States v. Anzalone,* 2019; *United States v. Wagner*, 2020).

3.1.3. Zakonitost vladinog postupanja (outrageous conduct)

Imajući u vidu da je *Playpen* bio sajt dečje pornografije, činjenica da je sajt nastavio da radi i pod kontrolom FBI-ja otvorila je pitanje zakonitosti *Playpen* operacije. Budući da FBI tokom *Playpen* operacije nije kreirao *Playpen* sajt, nije menjao funkcionalnost sajta, nije dodavao nove sadržaje dečje pornografije, nije dodavao nove korisnike, niti je postojeće korisnike prinudio da pristupaju sajtu i preuzimaju inkriminišući sadržaj, prigovori odbrane o nezakonitom postupanju FBI-ja (*outrageous government conduct*)[8] u sudskim postupcima nisu zabeležili željeni uspeh (*United States v. Wagner*, 2020, pp. 31-33).

[7] Na osnovu NIT naloga FBI je bio ovlašćen da prikupi sledeće informacije: 1) stvarnu IP adresu računara koji je aktivirao *malver,* kao i datum i vreme kada je ta adresa identifikovana, 2) jedinstveni identifikator generisan od strane *malvera,* koji je omogućavao razlikovanje podataka prikupljenih sa raznih uređaja (u vidu kombinacije brojeva, slova i specijalnih karaktera), 3) informacije o operativnom sistemu računara, uključujući i njegovu vrstu (npr. Windows), verziju (npr. Windows 7) i arhitekturu (npr. x86), 4) informaciju o tome da li je *malver* već isporučen konkretnom računaru kako bi se izbeglo višestruko slanje, 5) naziv *hosta* računara koji je pristupio sajtu, 6) korisničko ime koje je aktivno u operativnom sistemu u trenutku pristupanja i 7) MAC adresa računara – jedinstveni identifikator mrežnog *interfejsa* uređaja (*United States v. Levin*, 2017, p. 6).

[8] Da bi uspela sa prigovorom nezakonitog postupanja organa krivičnog gonjenja, odbrana mora da dokaže ili prekomerno učešće konkretnog organa u izvršenju krivičnog dela, što podrazumeva kreiranje i upravljanje izvršenjem krivičnog dela od početka do kraja, ili da je radnjama organa krivičnog gonjenja okrivljeni prinuđen da izvrši krivično delo (*United States v. Wagner*, 2020, pp. 31-33).

3.1.4. Pravo odbrane na pristup dokazima

Konačno, operacija *Playpen* je otvorila pitanje krivično-procesne neravnopravnosti tužilaštva i odbrane u digitalnoj eri i ukazala na potencijalno kršenje prava na efektivnu odbranu i pristup dokazima kao segmentu prava na fer i pravično suđenje u kontekstu šestog amandmana (Steele, 2022). Suštinsko pitanje koje se postavlja jeste da li pravo na pravično suđenje i pristup dokazima podrazumeva pravo okrivljenog da se upozna sa karakteristikama i načinom funkcionisanja tehničkih sredstava upotrebljenih za prikupljanje dokaza protiv njega? Naime, u operaciji *Playpen*, FBI koristi sofisticirano tehničko sredstvo – NIT, kako bi prikupio određene dokaze i to čini bez znanja korisnika. Ukoliko bi odbrana želela da koristi slična tehnička sredstva ili da dobije podatke o NIT alatima, sudovi bi se gotovo sigurno pozivali na poverljivost metoda koji se, po pravilu, primenjuje tako da favorizuje tužilaštvo i onemogućava pristup dokazima od strane odbrane, čime se stvara procesna nejednakost (Waxler, 2021).

Kao izuzetak od ustanovljenog pravila, Chertoff & Jardine ističu slučaj *United States v. Michaud* u kome je sud usvojio zahtev odbrane i naložio tužilaštvu da odbrani dostavi kompletan izvorni kod *malvera* korišćenog za hakovanje računara optuženog, uključujući i eksploataciju koja je omogućila zaobilaženje bezbednosnih mehanizama TOR pretraživača. Ne želeći da otkrije sofisticirane tehnološke karakteristike NIT-a, tužilaštvo je u ovom slučaju odustalo od optužbe (Chertoff & Jardine, 2021, p. 14).[9]

Slučaj *Playpen* ukazuje na duboku tenziju između efikasnosti krivičnog gonjenja u digitalnom dobu i ustavnih garancija pravičnog suđenja i zaštite privatnosti, što ukazuje na nužnost redefinisanja postojećih procesnih pravila u svetlu novih tehnoloških izazova.

4. Etika, ljudska prava i digitalna represija

Korišćenje tehničkih sredstava za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata direktno je povezano sa pitanjem poštovanja prava na privatnost.

[9] Na evropskom kontinentu, pitanje obaveze policije i tužilaštva da odbrani učine dostupnim tehničko-tehnološke informacije o načinu pribavljanja dokaza iz kriptovane komunikacije, naročito nakon „probijanja" platformi *EnchroChat* i *Sky ECC*, dobilo je posebno na značaju. Prema stavu Evropskog suda za ljudska prava, pravo odbrane da bude upoznata sa svim dokazima kojima optužba raspolaže može biti ograničeno zarad zaštite javnog interesa, uključujući i zaštitu tajnih policijskih tehnika i metoda. Ipak, Vrhovni sud Italije zauzeo je stav da odbrana ima pravo da zahteva informacije o tehničkom načinu pribavljanja ovakvih podataka, dok je francuski Kasacioni sud ocenio da je policija dužna da pruži određeni nivo tehničkih detalja o pribavljenim dokazima iz *EnchroChat* komunikacija (Škulić, 2024).

U eri savremenog „*sajberfatalizma*"[10] koji se javlja u drugoj deceniji XXI veka kao reakcija na rastuće probleme digitalnih tehnologija, poput masovnog nadzora i manipulacije ličnim podacima od strane velikih tehnoloških kompanija (Garcia Mexia, 2022), bio je očekivan jak otpor prema reformi zakonodavstva koja bi organima krivičnog gonjenja omogućila da korišćenjem sofisticiranih tehničkih sredstava pristupe personalnom računaru i sa njega zaplene određene podatke, bez znanja korisnika računara. Čak i manje invazivni metodi, poput zadržavanja podataka o saobraćaju i lokaciji elektronskih komunikacija za potrebe krivičnog postupka, izazivaju oštro protivljenje dela stručne javnosti budući da predstavljaju značajno zadiranje u privatnost kao osnovno ljudsko pravo (Krnić Kulušić, 2022). Zabrinutost stručne javnosti zbog mogućih zloupotreba tehnički sofisticiranih alata i vršenja masovnog nadzora građana dostigla je vrhunac nakon „probijanja" kriptovanih komunikacionih platformi *EnchroChat* i *Sky ECC* od strane zajedničkih istražnih timova pojedinih država članica EU, uz učešće Europol-a i Eurojust-a (Bajović, 2022).

Međutim, prilikom razmatranja nespornih moralnih dilema koje se tiču dozvoljene granice do koje država sme da zadire u pravo na privatnost pojedinaca, ne smemo izgubiti iz vida da je stopa visokotehnološkog kriminaliteta u konstantom usponu i beleži gotovo eksponencijalni rast u poslednjoj deceniji. Reč je o grupi krivičnih dela kod kojih je tamna brojka izrazito visoka, na šta presudno utiče anonimnost izvršilaca krivičnih dela u digitalnom prostoru (Karović & Simović, 2022, p. 54). Stoga etička dilema ne može biti sagledana izolovano od realnih operativnih ograničenja sa kojima se suočavaju organi gonjenja. Studija slučaja *Playpen* jasno je pokazala da bi u konkretnom slučaju, bez korišćenja NIT-a, bilo praktično nemoguće identifikovati desetine hiljada učinilaca krivičnog dela dečje pornografije. Jednostavno rečeno, bez primene tehnički sofisticiranih alata za deanonimizaciju korisnika, organi krivičnog gonjenja nemaju mogućnost da identifikuju konkretnog učinioca krivičnog dela, a samim tim ni značajnije izglede za uspešno sprečavanje i suzbijanje krivičnih dela koja se vrše na *darknetu*.

Treba pomenuti da problem anonimizacije korisnika nije isključivo vezan za korisnike TOR mreže i *darkneta*, već se organi krivičnog gonjenja suočavaju sa sličnim problemima i u pogledu određenih zatvorenih zajednica na internet platformama, poput *Telegrama* koji odbija da postupa po zahtevima za pružanje korisničkih podataka, čak i u slučajevima gde postoji osnovana sumnja o izvršenju teških krivičnih dela[11] (Le Monde, 2024).

[10] „Sajberfatalizam" je termin kojim deo literature označava rastuće uverenje da je digitalni nadzor neizbežan.

[11] Osnivač i izvršni direktor *Telegrama* Pavel Durov uhapšen je u Francuskoj 24. avgusta 2024. godine, upravo zbog odbijanja saradnje u postupku identifikacije korisnika *Telegram* platforme, koji su navodno učestvovali u izvršenju teških krivičnih dela, uključujući i distribuciju dečje pornografije i trgovinu drogom (Le Monde, 2024)

Osnovno pitanje koje se u navedenom kontekstu postavlja jeste da li je upotreba inovativnih tehničkih alata za deanonimizaciju korisnika digitalno komunikacionih mreža i alata moralno sporna samo zato što narušava privatnost korisnika?[12]

Polazeći od čl. 8 Evropske konvencije o ljudskim pravima, te presuda Evropskog suda za ljudska prava, pravo na privatnost nije apsolutno pravo, već pravo koje može biti ograničeno u skladu sa zakonom, ukoliko je to neophodno u demokratskom društvu i proporcionalno legitimnom cilju (Art. 8, European Convention on Human Rights, 1950; *S. and Marper v. United Kingdom*, predstavka br. 30532/04 i br. 30566/04, presuda ECHR, 4. 12. 2008, par. 101-103). Iako nije apsolutno, pravo na privatnost mora biti zaštićeno kroz efektivni nadzor nad primenom mere kojom se ograničava pravo na privatnost i transparentnost procedure (*Roman Zakharov v. Russia*, predstavka br. 47143/06, presuda ECHR, 4. 12. 2015, par. 139).

S tim u vezi, umesto odbacivanja savremenih tehnoloških alata zbog rizika koje nose, rešenje treba tražiti u njihovom preciznom, zakonski utemeljenom i sudski kontrolisanom korišćenju. To bi podrazumevalo jasno propisivanje prirode, obima i trajanja ove mere, taksativno navođenje razloga zbog kojih je moguće tražiti određivanje mere, taksativno navođenje krivičnih dela kod kojih je moguće odrediti primenu mere (koja se ne mora poklapati sa listom krivičnih dela kod kojih je moguće odrediti primenu već postojećih posebnih dokaznih radnji), te određivanje organa nadležnog da odobri, sprovede i vrši nadzor nad primenom mere (*Klass and others v. Germany*, predstavka br. 5029/71, presuda ECHR, 6.9.1978, par. 50). Uvođenje posebne dokazne radnje za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata, uz jasno određene uslove i granice primene, predstavlja korak ka uspostavljanju ravnoteže između efikasnosti krivičnog gonjenja i zaštite osnovnih ljudskih prava u digitalnom dobu. Kada govorimo o našem krivičnoprocesnom zakonodavstvu, treba imati u vidu da bi propisivanje ovakve mere nužno zahtevalo i izmenu materijalnopravnih odredaba, budući da naš Krivični zakonik u čl. 300 kao krivično delo propisuje pravljenje i unošenje računarskih virusa, ne ostavljajući mogućnost da se takve radnje ovlašćeno preduzimaju (Bajović, 2022, p. 165).

5. Zaključak

Ukazujući na prednosti i značaj sofisticiranih tehničkih sredstava koja bi omogućila deanonimizaciju korisnika digitalno komunikacionih mreža i alata, ne smemo izgubiti iz vida potencijalne opasnosti koje bi primena ovakvih sredstava od strane organa krivičnog gonjenja sa sobom donela. U literaturi se uglavnom

[12] O konceptu balansiranja ljudskih prava i tehnoloških inovacija u digitalnom prostoru, kao i o potrebi redefinisanja ljudskih prava u digitalnom okruženju vid. Jelisavac Trošić & Gordanić, 2023.

ukazuje na opasnost od neselektivnog ili masovnog državnog „*hakovanja*" koje može imati i direktan ili indirektan uticaj na pravo na slobodu mišljenja, govora i udruživanja. Postoji i realna opasnost od prekomernog pretresa i mogućnosti da takvi alati zaplene i privatne podatke i podatke koji nisu u vezi sa krivičnim delom koji je predmet istrage (Shein, 2016; Access Now, 2016). Ipak, apriorno odbacivanje tehničkih dostignuća koja mogu obezbediti efikasno sprečavanje i suzbijanje teških krivičnih dela samo zahvaljujući potencijalnim opasnostima koje njihova primena podrazumeva može voditi ka održavanju uspostavljene asimetrije – država bi se dobrovoljno odrekla korišćenja tehnoloških inovacija koje omogućavaju otkrivanje i krivično gonjenje učinilaca teških krivičnih dela koji upravo zloupotrebljavaju tehnološke inovacije radi izbegavanja krivične odgovornosti.

Nasuprot tome, treba pristupiti kreiranju normativnog okvira koji bi omogućio zakonitu i restriktivnu primenu tehničkih sredstava za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata. Autorka predlaže uvođenje posebne dokazne radnje koja bi eksplicitno regulisala upotrebu digitalnih infiltracionih alata poput *malvera* u okviru istraga koje se vode povodom teških krivičnih dela učinjenih na *darknetu, Telegram* platformi i drugim sličnim platformama koje onemogućavaju pribavljanje korisničkih podataka neophodnih za otkrivanje identiteta izvršilaca, a čiji bi rezultati predstavljali osnov za primenu drugih opštih i posebnih dokaznih radnji koje su već propisane u krivično-procesnom zakonodavstvu. Da bi primena ovih alata bila u skladu sa međunarodnim standardima i praksom Evropskog suda za ljudska prava, neophodno je da u krivično-procesnom zakonodavstvu budu jasno i precizno propisani uslovi pod kojima je moguće koristiti tehnička sredstva za deanonimizaciju korisnika digitalnih komunikacionih mreža i alata u krivičnom postupku, kako bi se omogućila zakonita, proporcionalna i kontrolisana primena ovih instrumenata, bez ugrožavanja osnovnih ljudskih prava.

Literatura

Access Now. 2016. *A Human Rights Response to Government Hacking.* Dostupno na: https://www.accessnow.org/wp-content/uploads/2016/09/GovernmentHacking-Doc.pdf, 13. 7. 2025.

Bajović, V. 2022. EnchroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku. *Crimen*, 2, pp. 154-179. https://doi.org/10.5937/crimen2202154B7

Baron Quintero, S. 2023. Los delitos realizados mediante la Dark Net. *Revista Penal Mexico*, 23, pp. 175-194.

Barrio Andres, M. 2011. La ciberdelincuencia en el derecho español. *Revista de las Cortes Generales*, 83, pp. 273-305. https://doi.org/10.33426/rcg/2011/83/473

Bugarski, T. 2020. Prekogranična saradnja i pribavljanje elektronskih dokaza. U: Ristivojević, B. Bugarski, T., Orlović, S., Drakić, G., Tubić, B. (ur.), *Harmonizacija srpskog i mađarskog prava sa pravom Evropske unije.* Novi Sad: Univerzitet u Novom Sadu – Pravni fakultet, pp. 175-194.

Buxton, J. & Bingham, T. 2015. The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory, Policy Brief 7.* Dostupno na: https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf (10. 7. 2025).

Chertoff, M. & Jardine, E. 2021. Policing the Dark Web: Legal Challenges in the 2015 Playpen Case. *CIGI Papers*, 259, pp. 1-17.

Čučilović, I. 2025. Deepfake tehnologija: Krivičnopravne implikacije. *Crimen*, 15(3), pp. 325-342. https://doi.org/10.5937/crimen2403325C

Dinglendine, R., Mathewson, N. & Syverson, P. 2004. *Tor: The Second-Generation Onion Router.* Dostupno na: https://www.researchgate.net/publication/2910678_Tor_The_Second-Generation_Onion_Router, 7. 6. 2025. https://doi.org/10.21236/ADA465464

Đukić, A. 2018. Organizovani visokotehnološki kriminal: Pojam, razvoj i osnovne karakteristike. *Vojno delo*, 3, pp. 128-156. https://doi.org/10.5937/vojdelo1803128D

Đukić, D. 2025. Rešavanje sporova u vezi sa nazivom internet domena i nova rešenja u zakonodavstvu Evropske unije. *Strani pravni život*, 1, pp. 147-164. https://doi.org/10.56461/SPZ_25108KJ

Garcia Mexia, P. 2022. Contra el "ciberfatalismo": Beneficio y riesgo en la sociedad digital. *Revista de las Cortes Generales*, 114, pp. 285-354. https://doi.org/10.33426/rcg/2022/114/1724

Jelisavac Trošić, S. & Gordanić, J. 2023. Priznanje prava na pristup internetu kao samostalnog ljudskog prava – potencijali i prepreke. *Strani pravni život*, 3, pp. 375-394. https://doi.org/10.56461/SPZ_23301KJ

Karović, S. & Simović, M. 2022. Krivičnopravno suprotstavljanje visokotehnološkom – kompjuterskom kriminalitetu: Savremeni izazovi, dileme, perspektive. U: Kostić, J. & Matić Bošković, M. (ur.), *Digitalizacija u kaznenom pravu i pravosuđu.* Beograd: Institut za uporedno pravo, Institut za kriminološka i sociološka istraživanja, pp. 45-58. https://doi.org/10.56461/ZR_22.DUKPP.04

Korać, V., Prlja, D. & Diligenski, A. 2016. *Digitalna forenzika.* Beograd: Centar za nove tehnologije Viminacium, Arheološki institut Beograd, Institut za uporedno pravo.

Krnić Kulušić, A. 2022. The retention of traffic and location electronic communications data in European Union for the purpose of criminal proceedings. U: Kostić, J. & Matić Bošković, M. (ur.). *Digitalizacija u kaznenom pravu i pravosuđu.* Beograd: Institut za uporedno pravo, Institut za kriminološka i sociološka istraživanja, pp. 117-130. https://doi.org/10.56461/ZR_22.DUKPP.09

Kumar Shrivastava, P. 2021. Electronic Evidence in Crime Investigation: Darknet & Policing. *The Indian Police Journal*, 68(3), pp. 43-50.

Omar, Z. M. & Ibrahim, J. 2020. An Overview of Darknet, Rise and Challenges and Its Assumptions. *International Journal of Computer Science and Information Technology Research*, 8(3), pp. 110-116.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S. & Aiken, M. P. 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Science*, 2, pp. 379-398. https://doi.org/10.3390/forensicsci2020028

Pisarić, M. 2013. Potrebni normativni odgovor na probleme otkrivanja i dokazivanja dela visokotehnološkog kriminala. U: *Zbornik radova Pravnog fakulteta u Novom Sadu*. Novi Sad: Pravni fakultet Univerziteta u Novom Sadu, pp. 291-307.

Prlja, D. & Reljanović, M. 2009. Visokotehnološki kriminal: Uporedna iskustva. *Strani pravni život*, 3, pp. 161-184.

Shein, M. 2016. Cybercrime and the Fourth Amendment. *The Champion*. Washington DC: National Association of Criminal Defense Lawyers, pp. 36-62. Dostupno na: https://federalcriminallawcenter.com/wp-content/uploads/2017/03/Cybercrime-and-the-Fourth-Amendment.pdf, 14. 7. 2025.

Shortis, P., Aldridge, J. & Barratt, M. 2020. Drug cryptomarket futures: Structure, function and evolution in response to law enforcement actions. In: *Research Handbook on International Drug Policy.* Manchester: The University of Manchester, pp. 355-379. Dostupno na: https://research.manchester.ac.uk/en/publications/drug-cryptomarket-futures-structure-function-and-evolution-in-res, 1. 7. 2025. https://doi.org/10.4337/9781788117067.00031

Steele, R. 2022. Equalizing Access to Evidence: Criminal Defendants and the Stored Communications Act. *The Yale Law Journal*, 131, pp. 1584-1640.

Škulić, M. 2018. *Organizovani kriminalitet: Pojam, pojavni oblici, krivična dela i krivični postupak*. Drugo izmenjeno i dopunjeno izdanje. Beograd: Službeni glasnik.

Škulić, M. 2024. Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje – kao što su *Sky ECC* i *EnchroChat. Crimen,* 1, pp. 3-55. https://doi.org/10.5937/crimen2401003S

Wall, D. 2017. Towards a Conceptualisation of Cloud (Cyber)crime. In: Tryfonas, T. (ed.), *Human Aspects of Information Security, Privacy and Trust*. New York: Springer International, pp. 529-539. https://doi.org/10.1007/978-3-319-58460-7_37

Wexler, R. 2021. Privacy as Privilege: The Stored Communications Act and Internet Evidence. *Harvard Law Review*, 134, pp. 2721-2793. https://doi.org/10.2139/ssrn.3673403

Widenhouse, K. 2017. Playpen, the NIT, and Rule 41(b): Electronic "searches" for those who do not wish to be found. *Journal of Business & Technology Law*, 13(1), pp. 143-169.

Pravni izvori

CETS, 2001. Council of Europe, Convention on Cybercrime (ETS No. 185) od 23. 11. 2001. godine. Dostupno na: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, 11. 6. 2025.

European Convention on Human Rights, 1950, Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms od 4. 11. 1950. godine. Dostupno na: https://www.echr.coe.int/documents/d/echr/convention_eng, 1. 8. 2025.

United States Courts. 2016. Federal Rules of Criminal Procedure od 6. 12. 2016. godine. Dostupno na: https://www.uscourts.gov/file/document/rules-criminal-procedure, 3. 6. 2025.

Sudska praksa

Carpenter v. United States, Judgement of the Supreme Court of the United States of June 22, 2018 (585 U.S. (2018))

Klass and others v. Germany, predstavka br. 5029/71, presuda ECHR, 6.9.1978.

Roman Zakharov v. Russia, predstavka br. 47143/06, presuda ECHR, 4.12.2015.

S. and Marper v. United Kingdom, predstavka br. 30562/04 i br. 30566/04, presuda ECHR, 4.12.2008.

United States v. Anzalone, Judgement of the United States Court of Appeals of April 24, 2019 (Case No. 17-1454, 1st Cir.)

United States v. Levin, Judgement of the United States Court of Appeals of October 27, 2017 (Case No. 16-1567, 1st Cir.)

United States v. Wagner, Judgement of the United States Court of Appeals of March 3, 2020 (D.C. No. 5:17-CR-40097-DDC-1)

Internet izvori

Le Monde. *Telegram CEO Pavel Durov charged but released under judicial supervision*. 2024. Dostupno na: https://www.lemonde.fr/en/france/article/2024/08/29/telegram-ceo-pavel-durov-charged-but-released-under-judicial-supervision_6723047_7.html, 1. 8. 2025.