DOI: 10.7251/GFP2616095G

UDC: 004.738.5:004.492(100)

Originalni naučni rad

Datum prijema rada:
2. jun 2026.

Datum prihvatanja rada:
10. jun 2026.

Kriminalistički i pravni izazovi nadzora elektronskih komunikacija u eri enkriptovanih platformi

Apstrakt: Savremeni razvoj informaciono-komunikacionih tehnologija doveo je do značajnih promjena u načinu ostvarivanja međuljudske komunikacije, ali istovremeno i do transformacije načina izvršenja i prikrivanja krivičnih djela. Poseban izazov za organe provođenja zakona predstavljaju enkriptovane komunikacione platforme i savremeni oblici digitalne komunikacije koji kriminalnim grupama omogućavaju visok stepen anonimnosti, sigurnosti i otežanog otkrivanja. Upotreba aplikacija poput SKY ECC, ANOM, Signal i sličnih sistema, kao i korištenje privremenih komunikacionih metoda, uključujući samobrišuće aplikacije, draft komunikaciju putem elektronske pošte i anonimne internet servise, značajno komplikuje primjenu posebnih istražnih radnji nadzora i tehničkog snimanja telekomunikacija.

Predmet rada odnosi se na kriminalističke i pravne izazove nadzora elektronskih komunikacija u eri enkriptovanih platformi, sa posebnim fokusom na zakonitost pribavljanja, korištenja i dokazne vrijednosti elektronskih dokaza u krivičnim postupcima. U radu se analiziraju savremeni modaliteti digitalne komunikacije koje koriste organizovane kriminalne grupe, tehničke i operativne prepreke u njihovom otkrivanju, kao i normativni okvir kojim je regulisana primjena posebnih istražnih radnji u Bosni i Hercegovini i međunarodnom pravu.

Posebna pažnja posvećena je pitanju prihvatljivosti dokaza pribavljenih putem međunarodne saradnje i ustupljenih podataka sa enkriptovanih platformi, naročito u kontekstu SKY ECC i ANOM predmeta, te odnosu između zaštite prava na privatnost i potrebe efikasnog krivičnog gonjenja. Analiziraju se i problemi autentifikacije, integriteta i pouzdanosti digitalnih dokaza, kao i izazovi digitalne forenzike u rekonstrukciji obrisanih ili skrivenih komunikacija.

Ključne riječi: elektronske komunikacije, enkriptovane platforme, SKY ECC, ANOM, posebne istražne radnje, nadzor telekomunikacija, elektronski dokazi.

Goran Gajić
Panevropski univerzitet "APEIRON", Banja Luka; Republika Srpska – Bosna i Hercegovina;
goranga@teol.net

1. UVOD

Savremeni razvoj informaciono-komunikacionih tehnologija i ubrzana digitalizacija društva doveli su do korjenitih promjena u načinu ostvarivanja komunikacije, razmjene podataka i izvršenja brojnih društvenih aktivnosti. Elektronske

komunikacije postale su dominantan oblik privatne, poslovne i institucionalne interakcije, pri čemu savremene internet platforme omogućavaju brz i globalno dostupan prenos informacija. Paralelno sa tehnološkim napretkom razvijaju se i novi modaliteti izvršenja krivičnih djela, posebno u oblasti organizovanog kriminala, trgovine opojnim drogama, terorizma, krijumčarenja ljudi i drugih oblika transnacionalnog kriminaliteta. Organizovane kriminalne grupe sve češće koriste sofisticirane oblike digitalne komunikacije zasnovane na enkripciji, anonimnosti i privremenom čuvanju podataka, čime se značajno otežava otkrivanje, dokumentovanje i dokazivanje krivičnih djela.

Poseban izazov za organe provođenja zakona predstavljaju enkriptovane komunikacione platforme poput SKY ECC, ANOM, Signal i sličnih aplikacija koje korisnicima omogućavaju visok stepen zaštite identiteta i sadržaja komunikacije. Pored toga, savremene kriminalne strukture koriste i različite alternativne metode prikrivene komunikacije, uključujući privremeno instaliranje aplikacija za razmjenu poruka, korištenje draft komunikacije putem elektronske pošte, VPN servisa, TOR mreže i drugih alata za prikrivanje digitalnog identiteta. Takvi modaliteti komunikacije stvaraju ozbiljne operativne, tehničke i pravne izazove u primjeni posebnih istražnih radnji nadzora i tehničkog snimanja telekomunikacija, naročito u kontekstu zakonitosti pribavljanja i korištenja elektronskih dokaza u krivičnom postupku.

Predmet ovog rada odnosi se na kriminalističke i pravne izazove nadzora elektronskih komunikacija u eri enkriptovanih platformi, sa posebnim fokusom na zakonitost pribavljanja, korištenja i dokazne vrijednosti elektronskih dokaza u savremenim krivičnim postupcima. Istraživanje obuhvata analizu savremenih oblika digitalne komunikacije koje koriste organizovane kriminalne grupe, tehničkih i operativnih ograničenja u njihovom otkrivanju, kao i normativnog okvira kojim se uređuje primjena posebnih istražnih radnji u Bosni i Hercegovini i međunarodnom pravu. Posebna pažnja posvećena je pitanjima prihvatljivosti dokaza pribavljenih putem međunarodne saradnje i ustupljenih podataka sa enkriptovanih platformi, naročito u kontekstu predmeta SKY ECC i ANOM, te odnosu između zaštite prava na privatnost i potrebe efikasnog krivičnog gonjenja.

Problem istraživanja proizlazi iz činjenice da postojeći normativni i institucionalni mehanizmi često ne prate dovoljno brzo tehnološki razvoj komunikacionih sistema i savremene metode prikrivanja komunikacije koje koriste izvršioci krivičnih djela. U praksi se sve češće postavlja pitanje zakonitosti podataka pribavljenih putem međunarodnih operacija protiv enkriptovanih mreža, njihove procesne prihvatljivosti i mogućnosti validacije pred sudovima. Istovremeno, potreba za efikasnim otkrivanjem i dokazivanjem najtežih oblika kriminaliteta nerijetko dolazi u koliziju sa pravom na privatnost i zaštitom osnovnih ljudskih prava, što dodatno usložnjava pravnu i društvenu dimenziju ovog problema.

Cilj rada jeste da se interdisciplinarnim pristupom analiziraju ključni kriminalistički, tehnički i pravni izazovi u oblasti nadzora elektronskih komunikacija, te da se sagleda efikasnost postojećih mehanizama za otkrivanje i dokazivanje krivičnih djela izvršenih korištenjem enkriptovanih platformi. U radu će se koristiti normativno-pravna, komparativna i analiza sadržaja, uz primjenu metode studije slučaja kroz analizu međunarodnih operacija protiv platformi SKY ECC i ANOM. Naučna i društvena opravdanost istraživanja ogleda se u činjenici da razvoj enkriptovanih komunikacionih sistema stvara nove izazove za kriminalistiku, krivično procesno pravo i bezbjednosni sektor u cjelini, dok istovremeno raste potreba za usklađivanjem represivnih mehanizama sa međunarodnim standardima zaštite ljudskih prava i sloboda.

2. TEORIJSKO-POJMOVNI OKVIR ELEKTRONSKIH KOMUNIKACIJA I NADZORA

2.1. Pojam i razvoj elektronskih komunikacija

Elektronske komunikacije predstavljaju svaki oblik prenosa informacija putem elektronskih, elektromagnetnih, optičkih ili drugih tehničkih sistema koji omogućavaju razmjenu podataka na daljinu. Njihov razvoj usko je povezan sa razvojem telekomunikacionih tehnologija, od prvih analognih telefonskih sistema do savremenih digitalnih i internet komunikacionih platformi. Tradicionalne telekomunikacije bile su zasnovane prvenstveno na fiksnoj telefoniji, radio-komunikacijama i kasnije mobilnim mrežama, pri čemu je komunikacija uglavnom bila ograničena na prenos glasa i relativno jednostavnih podataka. Takvi sistemi bili su centralizovani, tehnički predvidivi i relativno dostupni za zakoniti nadzor od strane državnih organa.

Razvojem digitalnih tehnologija dolazi do transformacije komunikacionih sistema iz analognih u digitalne mreže, čime se značajno povećava brzina prenosa podataka, sigurnost komunikacije i mogućnost globalnog povezivanja korisnika.[1] Digitalizacija komunikacija omogućila je objedinjavanje različitih oblika komunikacije – glasa, slike, teksta i multimedijalnih sadržaja – u jedinstvene internet protokole i komunikacione sisteme. Internet je postao dominantna infrastruktura savremenih komunikacija, dok su mobilni uređaji omogućili stalnu povezanost korisnika i gotovo neograničenu razmjenu podataka.

Savremene internet komunikacione platforme predstavljaju složene sisteme koji korisnicima omogućavaju razmjenu poruka, glasovnu i video komunikaciju, dijeljenje sadržaja i uspostavljanje virtuelnih mreža komunikacije. Platforme poput WhatsApp-a, Vibera, Telegram-a, Signal-a i drugih aplikacija zasnovane su na internet infrastrukturi i koriste različite modele zaštite komunikacije, uključujući napredne metode enkripcije.[2] Njihova osnovna karakteristika jeste decentralizovan i globalan karakter komunikacije, zbog čega tradicionalni modeli nadzora telekomunikacija postaju sve manje efikasni.

Poseban tehnološki i bezbjednosni izazov predstavljaju enkriptovane komunikacije. Enkripcija podrazumijeva proces pretvaranja podataka u kodirani oblik koji je razumljiv isključivo ovlaštenim korisnicima koji posjeduju odgovarajući ključ za dešifrovanje. Savremene komunikacione platforme sve češće koriste end-to-end enkripciju, pri čemu sadržaj komunikacije ostaje nedostupan čak i pružaocima usluga komunikacije.[3] Takav model zaštite komunikacija značajno unapređuje zaštitu privatnosti korisnika, ali istovremeno otežava rad organa provođenja zakona u otkrivanju i dokazivanju krivičnih djela.

Savremeni trendovi u oblasti elektronskih komunikacija karakterišu se rastućom upotrebom anonimnih mreža, decentralizovanih komunikacionih sistema, cloud infrastrukture i privremenih komunikacionih modela. Kriminalne grupe sve češće koriste aplikacije sa mogućnošću automatskog brisanja sadržaja, anonimne elektronske naloge, VPN servise, TOR mrežu i druge alate koji otežavaju identifikaciju korisnika i praćenje komunikacije. Time elektronske komunikacije postaju ne samo sredstvo svakodnevne društvene interakcije, već i važan instrument organizovanog i transnacionalnog kriminaliteta.

---

1 Castells, M. (2010). *The Rise of the Network Society* (2nd ed.). Wiley-Blackwell.

2 Kizza, J. M. (2020). *Guide to Computer Network Security* (6th ed.). Springer.

3 Greenberg, A. (2022). *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Doubleday.

2.2. Pojam nadzora elektronskih komunikacija

Nadzor elektronskih komunikacija predstavlja skup operativnih, tehničkih i pravnih mjera kojima se omogućava praćenje, presretanje, evidentiranje i analiza komunikacija radi otkrivanja, dokazivanja i sprečavanja krivičnih djela i ugrožavanja bezbjednosti. U savremenim bezbjednosnim sistemima nadzor komunikacija predstavlja jednu od najznačajnijih posebnih istražnih radnji, naročito u borbi protiv organizovanog kriminala, terorizma i drugih oblika teškog kriminaliteta.

Sa operativnog i kriminalističkog aspekta, nadzor elektronskih komunikacija omogućava prikupljanje podataka o načinu djelovanja kriminalnih grupa, njihovoj hijerarhiji, kontaktima, logistici i planiranju izvršenja krivičnih djela. Elektronske komunikacije često predstavljaju ključni izvor kriminalističko-obavještajnih podataka, jer omogućavaju rekonstrukciju kontakata, utvrđivanje međusobnih veza izvršilaca i identifikaciju strukture kriminalnih mreža.[4] U savremenim istragama upravo digitalna komunikacija postaje jedan od najvažnijih izvora dokaznog materijala.

Posebne istražne radnje predstavljaju zakonom propisane mjere kojima se, pod određenim uslovima i uz sudsku kontrolu, privremeno ograničavaju pojedina prava i slobode radi otkrivanja i dokazivanja najtežih oblika kriminaliteta. Nadzor i tehničko snimanje telekomunikacija spada među najintruzivnije posebne istražne radnje jer direktno zadire u pravo na privatnost i tajnost komunikacija.[5] Zbog toga savremeni pravni sistemi propisuju stroge uslove za njihovu primjenu, uključujući postojanje osnova sumnje, proporcionalnost mjere, sudsko odobrenje i vremensko ograničenje trajanja nadzora.

Tehnički nadzor komunikacija obuhvata različite metode presretanja i evidentiranja komunikacionog saobraćaja, uključujući nadzor telefonskih razgovora, internet saobraćaja, elektronske pošte i komunikacije putem aplikacija za razmjenu poruka. Međutim, razvoj enkriptovanih platformi značajno je smanjio efikasnost tradicionalnih metoda presretanja komunikacija. Organi provođenja zakona danas se suočavaju sa situacijom da mogu identifikovati komunikacioni saobraćaj i određene metapodatke, ali ne i sadržaj same komunikacije zbog primjene naprednih sistema enkripcije.[6]

Poseban značaj u savremenim istragama imaju elektronski dokazi. Elektronski dokaz predstavlja svaki podatak koji je nastao, pohranjen ili prenesen u digitalnom obliku i koji može imati dokaznu vrijednost u krivičnom postupku. Specifičnost elektronskih dokaza ogleda se u njihovoj promjenljivosti, mogućnosti brisanja, modifikacije i prikrivanja, kao i u činjenici da se često nalaze na udaljenim serverima ili u međunarodnim cloud sistemima. Zbog toga pitanja autentičnosti, integriteta i zakonitosti pribavljanja elektronskih dokaza imaju poseban značaj u savremenom krivičnom procesnom pravu.

2.3. Kriminalistički značaj elektronskih komunikacija

Elektronske komunikacije danas predstavljaju jedan od najvažnijih elemenata organizovanog kriminalnog djelovanja. Organizovane kriminalne grupe koriste savremene komunikacione platforme za planiranje, koordinaciju i prikrivanje kriminalnih aktivnosti, pri čemu digitalna komunikacija omogućava brzo međunarodno povezivanje i visok ste-

[4] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

[5] Harris, D., O'Boyle, M., Bates, E., & Buckley, C. (2023). *Law of the European Convention on Human Rights* (5th ed.). Oxford University Press.

[6] Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). Sage Publications.

pen operativne sigurnosti.[7] Enkriptovane platforme koriste se za organizovanje krijumčarskih ruta, koordinaciju distribucije opojnih droga, pranje novca i druge aktivnosti transnacionalnog kriminaliteta.

Poseban bezbjednosni problem predstavlja korištenje enkriptovanih komunikacija u terorističkim aktivnostima. Terorističke organizacije koriste internet komunikacione platforme za regrutaciju, propagandu, finansiranje i koordinaciju aktivnosti svojih članova. End-to-end enkripcija i anonimni komunikacioni sistemi omogućavaju skriveno djelovanje i otežavaju pravovremeno otkrivanje planiranih napada i bezbjednosnih prijetnji. Upravo zbog toga pitanje zakonitog nadzora elektronskih komunikacija ima izuzetno važnu preventivnu i represivnu funkciju u savremenim sistemima nacionalne i međunarodne bezbjednosti.

Trgovina opojnim drogama predstavlja jednu od oblasti u kojoj su enkriptovane komunikacije doživjele najširu praktičnu primjenu. Kriminalne grupe koriste specijalizovane telefone i aplikacije poput SKY ECC i ANOM za koordinaciju međunarodnih pošiljki narkotika, finansijskih transakcija i komunikaciju između članova kriminalnih organizacija. Međunarodne policijske operacije usmjerene protiv takvih platformi pokazale su da su enkriptovane mreže postale ključna infrastruktura savremenog organizovanog kriminala.[8]

Savremeni oblici digitalne konspiracije zasnivaju se na prikrivanju identiteta, korištenju anonimnih komunikacionih naloga i otežavanju digitalne identifikacije korisnika. Kriminalci koriste VPN servise, TOR mreže, privremene elektronske naloge, samobrišuće aplikacije i decentralizovane komunikacione sisteme kako bi izbjegli identifikaciju i nadzor.[9] Pored toga, sve češće se koriste metode kratkotrajne instalacije aplikacija za razmjenu poruka, komunikacija putem draft opcija elektronske pošte i korištenje više digitalnih identiteta. Takvi oblici digitalne konspiracije predstavljaju ozbiljan izazov za kriminalistiku, digitalnu forenziku i krivično procesno pravo, jer zahtijevaju stalno unapređenje tehničkih, operativnih i pravnih kapaciteta organa provođenja zakona.

3. PRAVNI OKVIR NADZORA ELEKTRONSKIH KOMUNIKACIJA

3.1. Međunarodni pravni standardi

Pravni okvir nadzora elektronskih komunikacija počiva na potrebi uspostavljanja ravnoteže između dva legitimna interesa: s jedne strane, zaštite prava na privatnost, tajnost komunikacija i zaštite ličnih podataka, a s druge strane, potrebe države da efikasno otkriva, sprečava i dokazuje najteže oblike kriminaliteta. U evropskom pravnom prostoru osnovni polazni standard predstavlja član 8. Evropske konvencije o ljudskim pravima, kojim se štiti pravo na poštovanje privatnog i porodičnog života, doma i prepiske. Svako zadiranje države u komunikacije građana mora biti zakonito, imati legitiman cilj i biti nužno u demokratskom društvu. Upravo ti kriterijumi čine osnovni test zakonitosti mjera nadzora elektronskih komunikacija.

Praksa Evropskog suda za ljudska prava posebno je značajna jer je kroz niz pred-

---

[7] Europol. (2023). *Serious and Organised Crime Threat Assessment (SOCTA) 2023*. Publications Office of the European Union.

[8] Europol. (2021). *Decoding the EU's Most Threatening Criminal Networks*. Publications Office of the European Union.

[9] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). "Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime." *International Journal of Cyber Criminology*, 8(1), 1–20.

meta razvila standarde koji se odnose na tajni nadzor, presretanje komunikacija, masovni nadzor i pristup komunikacionim podacima. Sud zahtijeva da zakon koji omogućava nadzor bude dovoljno jasan, dostupan i predvidljiv, odnosno da građanin može razumno znati pod kojim uslovima državne vlasti mogu zadirati u njegovu privatnost.[10] Pored toga, zakon mora propisivati kategorije lica koja mogu biti obuhvaćena nadzorom, vrste krivičnih djela za koja se mjera može odrediti, trajanje mjere, postupak čuvanja, korištenja i uništavanja podataka, kao i djelotvoran nadzor nad primjenom mjera. U predmetima *Big Brother Watch and Others v. the United Kingdom* i *Centrum för Rättvisa v. Sweden* Evropski sud je posebno naglasio značaj nezavisnog odobravanja, kontrole selektora, nadzora nad pristupom presretnutom materijalu i zaštite novinarskih i povjerljivih komunikacija.[11]

Ovi standardi imaju neposredan značaj za krivične istrage u kojima se koriste podaci iz elektronskih komunikacija. Nije dovoljno da mjera nadzora bude formalno propisana zakonom; ona mora biti konkretno obrazložena, proporcionalna cilju koji se želi postići i podvrgnuta efektivnoj sudskoj ili drugoj nezavisnoj kontroli. U kontekstu savremenih enkriptovanih platformi to pitanje postaje još složenije, jer se podaci često pribavljaju u okviru međunarodnih operacija, putem stranih nadležnih organa ili od pružalaca digitalnih usluga koji se nalaze izvan teritorije države koja vodi krivični postupak.

Budimpeštanska konvencija o cyber kriminalu predstavlja najznačajniji međunarodni instrument u oblasti cyber kriminala i elektronskih dokaza. Ona ne uređuje samo inkriminacije vezane za računarske sisteme, već i procesne mehanizme za prikupljanje, čuvanje, pretres, oduzimanje i razmjenu elektronskih dokaza. Savjet Evrope Budimpeštansku konvenciju označava kao najkoherentniji međunarodni okvir za cyber kriminal i elektronske dokaze, ali i kao osnov za međunarodnu saradnju država članica.

Poseban značaj u savremenom kontekstu ima Drugi dodatni protokol uz Budimpeštansku konvenciju, koji je usmjeren na efikasniji prekogranični pristup elektronskim dokazima. On uvodi dodatne mehanizme saradnje, uključujući bržu međunarodnu pravnu pomoć, saradnju u hitnim situacijama i određene oblike direktne saradnje sa pružaocima usluga. Eurojust posebno ističe da Protokol ima za cilj unapređenje pristupa elektronskim dokazima koji se nalaze pod kontrolom pružalaca usluga u drugim državama, naročito u pogledu pretplatničkih i saobraćajnih podataka.[12]

Za Bosnu i Hercegovinu je naročito važno što se, prema podacima Savjeta Evrope iz 2025. godine, vode aktivnosti usmjerene ka potpisivanju i implementaciji Drugog dodatnog protokola. To pokazuje da se domaći sistem postepeno uključuje u savremene evropske tokove koji se odnose na elektronske dokaze, međunarodnu pravnu pomoć i saradnju sa digitalnim servisima.[13]

---

[10] Harris, D., O'Boyle, M., Bates, E., & Buckley, C. (2023). *Law of the European Convention on Human Rights* (5th ed.). Oxford University Press.

[11] European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15; European Court of Human Rights. (2021). *Centrum för Rättvisa v. Sweden*, Application no. 35252/08.

[12] Eurojust. (2022). *The Second Additional Protocol to the Budapest Convention on Cybercrime and enhanced cross-border access to electronic evidence*. Eurojust Publications Office.

[13] Council of Europe. (2025). *Bosnia and Herzegovina moves towards the signature and implementation of the Second Additional Protocol to the Convention on Cybercrime*. CyberSEE Project.

Međunarodna pravna pomoć i razmjena podataka danas imaju centralno mjesto u istragama koje se odnose na enkriptovane platforme. Razlog je jednostavan: komunikacija se odvija globalno, serveri se često nalaze u jednoj državi, korisnici u drugoj, a krivični postupak se vodi u trećoj. Zbog toga se zakonitost elektronskih dokaza ne može posmatrati samo kroz nacionalni procesni okvir, nego i kroz pravila međunarodne saradnje, uzajamnog priznanja, zaštite podataka i poštovanja osnovnih prava. U tom smislu, međunarodni standardi zahtijevaju da se elektronski dokazi ne pribavljaju proizvoljno, već putem pravno uređenih procedura koje omogućavaju provjeru njihovog porijekla, integriteta, autentičnosti i zakonitosti.

3.2. Nacionalni pravni okvir Bosne i Hercegovine

Nacionalni pravni okvir Bosne i Hercegovine za nadzor elektronskih komunikacija zasniva se prvenstveno na krivičnoprocesnim propisima, propisima o komunikacijama, zaštiti ličnih podataka i pravilima koja uređuju nadležnosti policijskih, tužilačkih i bezbjednosnih organa. U krivičnom postupku najvažniji osnov predstavljaju odredbe o posebnim istražnim radnjama, među kojima se nalazi i nadzor i tehničko snimanje telekomunikacija. Prema Krivičnom postupku BiH, posebne istražne radnje mogu se odrediti za zakonom propisana krivična djela, pod uslovom da se dokazi ne mogu pribaviti na drugi način ili bi njihovo pribavljanje bilo povezano sa nesrazmjernim teškoćama.

Krivičnoprocesni aspekt posebnih istražnih radnji zahtijeva postojanje procesnih garancija koje sprečavaju proizvoljnu primjenu nadzora. To podrazumijeva da inicijativa za određivanje mjere mora biti zasnovana na konkretnim činjenicama, da tužilac mora obrazložiti potrebu za primjenom mjere, a sud mora izvršiti stvarnu, a ne samo formalnu kontrolu prijedloga.[14] Sudska naredba mora biti dovoljno određena u pogledu lica, sredstva komunikacije, vrste mjere, trajanja i svrhe nadzora. U suprotnom, postoji rizik da dokaz bude osporen kao nezakonit ili da se dovede u pitanje proporcionalnost zadiranja u privatnost.

U Bosni i Hercegovini dodatnu složenost predstavlja institucionalna struktura bezbjednosnog i policijskog sistema. Nadležnosti su raspoređene između državnog, entitetskog, kantonalnog i nivoa Brčko distrikta, dok se krivični postupci vode pred različitim pravosudnim organima u zavisnosti od stvarne i mjesne nadležnosti. U praktičnom smislu, to znači da uspješna primjena mjera nadzora zahtijeva jasnu koordinaciju tužilaštava, sudova, policijskih agencija, regulatornih tijela i, po potrebi, međunarodnih partnera. Kod elektronskih dokaza pribavljenih iz inostranstva dodatno se uključuju mehanizmi međunarodne pravne pomoći, kontakt tačke za cyber kriminal, zajednički istražni timovi ili drugi oblici operativne saradnje.[15]

Zakon o komunikacijama Bosne i Hercegovine uređuje osnovni regulatorni okvir u oblasti komunikacija i uspostavlja ulogu Regulatorne agencije za komunikacije. Iako taj zakon nije procesni propis za krivične istrage, on je važan jer uređuje komunikacioni sektor, pružaoce usluga i regulatorni ambijent u kojem se odvijaju elektronske komunikacije.

Zaštita prava na privatnost i proporcionalnost mjera posebno su važni u kontekstu elektronskih komunikacija. Ustavni i konvencijski standardi zahtijevaju da svako ograni-

[14] Simović, M., & Simović, V. (2021). *Krivično procesno pravo Bosne i Hercegovine*. Pravni fakultet Univerziteta u Banjoj Luci.

[15] Council of Europe. (2020). *Cybercrime Policies/Strategies of Bosnia and Herzegovina*. Council of Europe Cybercrime Programme Office.

čenje privatnosti bude zasnovano na zakonu, neophodno radi legitimnog cilja i srazmjerno ozbiljnosti prijetnje ili krivičnog djela. To znači da nadzor komunikacija ne može biti rutinska istražna mjera, nego izuzetna mjera koja se primjenjuje kada blaže mjere nisu dovoljne. Ovaj princip je posebno važan kod pristupa metapodacima, jer se u savremenoj praksi sve više prepoznaje da i podaci o komunikaciji — ko, kada, gdje i s kim komunicira — mogu otkriti veoma osjetljive informacije o privatnom životu pojedinca.

U oblasti zaštite ličnih podataka BiH je 2025. godine dobila novi Zakon o zaštiti ličnih podataka, objavljen u „Službenom glasniku BiH" broj 12/25, što je značajno za sve oblike obrade podataka, uključujući obradu podataka u vezi sa krivičnim osudama, krivičnim djelima i bezbjednosnim mjerama. Time se pravni okvir dodatno približava evropskim standardima zaštite podataka, iako će njegova stvarna vrijednost zavisiti od praktične primjene, institucionalnog nadzora i usklađivanja sektorskih propisa sa krivičnoprocesnim potrebama.

U savremenom kontekstu, nacionalni pravni okvir mora odgovoriti na nekoliko ključnih izazova: kako zakonito pristupiti podacima koji se nalaze kod stranih pružalaca usluga; kako obezbijediti sudsku kontrolu nad mjerama koje tehnički sprovode drugi organi ili druge države; kako razlikovati sadržaj komunikacije od metapodataka; i kako obezbijediti da digitalni dokazi budu prihvatljivi, provjerljivi i upotrebljivi u krivičnom postupku. Upravo na tim pitanjima se vidi da tradicionalni model nadzora telekomunikacija više nije dovoljan za enkriptovano i globalizovano digitalno okruženje.

3.3. Zakonitost elektronskih dokaza

Zakonitost elektronskih dokaza predstavlja jedno od najosjetljivijih pitanja savremenog krivičnog postupka. Elektronski dokaz može biti sadržaj poruke, zapis komunikacije, metapodatak, log zapis, lokacijski podatak, podatak sa mobilnog uređaja, računara, servera, cloud naloga ili komunikacione platforme. Njegova dokazna vrijednost ne zavisi samo od sadržaja, već i od načina na koji je pribavljen, sačuvan, dokumentovan i prezentovan sudu.[16]

Pojam zakonitog dokaza podrazumijeva da je dokaz pribavljen u skladu sa zakonom, uz poštovanje procesnih garancija i osnovnih prava lica na koje se odnosi. Kod nadzora elektronskih komunikacija to znači da mora postojati valjana sudska naredba, zakonski osnov, jasno određen obim mjere, proporcionalnost i poštovanje pravila o trajanju i upotrebi prikupljenih podataka. Ako je mjera sprovedena mimo zakonskih uslova, bez nadležnog odobrenja ili u širem obimu od dozvoljenog, postoji ozbiljan rizik da se dokaz ocijeni nezakonitim.

Lanac čuvanja digitalnih dokaza ima poseban značaj jer elektronski podaci mogu biti lako izmijenjeni, obrisani, kopirani ili kompromitovani. Za razliku od klasičnih materijalnih dokaza, digitalni dokaz najčešće postoji u obliku zapisa koji se može tehnički reprodukovati, prebacivati i analizirati različitim forenzičkim alatima. Zbog toga je neophodno precizno dokumentovati ko je, kada, gdje i na koji način pristupio podacima, kojim alatom je izvršeno izuzimanje, da li je izrađena forenzička kopija, da li su korištene hash vrijednosti i kako je obezbijeđen integritet podataka od trenutka izuzimanja do prezentovanja pred sudom.[17]

---

[16] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

[17] Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.

Problemi autentičnosti i integriteta posebno dolaze do izražaja kod podataka sa enkriptovanih platformi. Sud mora biti u mogućnosti da provjeri da li komunikacija zaista potiče od određenog korisnika, da li je sadržaj potpun, da li je mijenjan i da li postoji pouzdana veza između digitalnog identiteta i stvarnog lica. U praksi to često zahtijeva kombinovanje više izvora: sadržaja poruka, metapodataka, lokacijskih podataka, finansijskih tragova, izjava svjedoka, rezultata pretresa, forenzičkog vještačenja uređaja i drugih dokaza. Sam digitalni zapis, naročito ako je pribavljen iz inostranstva, mora biti procesno i tehnički provjerljiv.

Dokazi pribavljeni putem međunarodne saradnje otvaraju dodatna pitanja. U predmetima koji se odnose na platforme kao što su SKY ECC i ANOM, domaći organi često ne učestvuju neposredno u prvobitnom presretanju ili tehničkom pribavljanju podataka, već dobijaju već prikupljene podatke od stranih organa. Tada se postavlja pitanje da li domaći sud treba da ispituje samo zakonitost njihovog prijema i korištenja u domaćem postupku ili i zakonitost načina na koji su podaci prvobitno pribavljeni u drugoj državi. Ovo pitanje u praksi može dovesti do različitih tumačenja, naročito ako odbrana osporava autentičnost, cjelovitost ili porijeklo podataka.[18]

Postojeći krivičnoprocesni okvir u Bosni i Hercegovini još uvijek ne daje dovoljno precizne odgovore na pitanja procesne provjere elektronskih dokaza pribavljenih putem međunarodnih operacija protiv enkriptovanih platformi. De lege ferenda, bilo bi opravdano normativno preciznije urediti uslove prihvatljivosti i način verifikacije prekogranično pribavljenih digitalnih dokaza.

Savremeni evropski trendovi idu u pravcu jačanja mehanizama prekograničnog pristupa elektronskim dokazima, ali uz istovremeno insistiranje na zaštiti osnovnih prava. Drugi dodatni protokol uz Budimpeštansku konvenciju i aktuelne rasprave o elektronskim dokazima ukazuju da budući sistem neće moći počivati isključivo na sporoj klasičnoj međunarodnoj pravnoj pomoći, nego na bržim, standardizovanim i kontrolisanim procedurama saradnje.[19]

Za Bosnu i Hercegovinu to znači da pitanje elektronskih dokaza treba posmatrati kroz tri međusobno povezana nivoa. Prvi je normativni nivo, koji zahtijeva jasna pravila o pribavljanju, čuvanju, analizi i korištenju digitalnih dokaza. Drugi je institucionalni nivo, koji zahtijeva obučene tužioce, istražioce, sudije i digitalne forenzičare. Treći je međunarodni nivo, koji zahtijeva efikasnu saradnju sa drugim državama, međunarodnim organizacijama i pružaocima digitalnih usluga. Bez povezivanja ova tri nivoa, elektronski dokazi mogu ostati tehnički dostupni, ali procesno ranjivi.

Zbog toga se zakonitost elektronskih dokaza ne može svesti samo na pitanje da li je određeni podatak pronađen ili preuzet. Ključno je da se može dokazati njegovo zakonito porijeklo, tehnička vjerodostojnost, neprekinut lanac čuvanja, povezanost sa konkretnim licem i relevantnost za predmet krivičnog postupka. Upravo na tom mjestu se spajaju pravna, kriminalistička i forenzička dimenzija nadzora elektronskih komunikacija.

---

[18] Fair Trials. (2023). *A Comparative Study of the Use of EncroChat and Sky ECC Data in Criminal Proceedings Across Europe*. Fair Trials International.

[19] Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Council of Europe.

4. ENKRIPTOVANE PLATFORME KAO IZAZOV KRIMINALISTIČKIM ISTRAGAMA

4.1. Tehnološke karakteristike enkriptovanih platformi

Savremene enkriptovane komunikacione platforme predstavljaju jedan od najznačajnijih tehnoloških izazova za kriminalističke istrage i primjenu posebnih istražnih radnji. Njihov razvoj rezultat je potrebe za zaštitom privatnosti korisnika, bezbjednosti podataka i zaštite komunikacija od neovlaštenog pristupa. Međutim, iste tehnološke karakteristike koje štite legitimnu komunikaciju građana istovremeno omogućavaju i kriminalnim strukturama visok stepen operativne sigurnosti i otežavaju rad organa provođenja zakona.

Osnovu savremenih sigurnih komunikacionih sistema čini end-to-end enkripcija. Riječ je o modelu zaštite komunikacije u kojem se sadržaj poruke šifruje na uređaju pošiljaoca i može biti dešifrovan isključivo na uređaju primaoca. Pružalac komunikacione usluge nema pristup sadržaju komunikacije niti posjeduje tehničku mogućnost njenog čitanja u prenosu.[20] Za razliku od tradicionalnih telekomunikacionih sistema, gdje je operator mogao omogućiti pristup sadržaju komunikacije na osnovu sudske naredbe, kod savremenih enkriptovanih aplikacija često nije moguće tehnički pristupiti sadržaju poruke ni uz postojanje zakonskog ovlaštenja. Upravo zbog toga organi provođenja zakona sve više prelaze sa klasičnog presretanja komunikacija na pristup krajnjim uređajima, digitalnu forenziku i analizu metapodataka.

Pored enkripcije, značajan element savremenih platformi jeste anonimizacija korisnika. Brojne aplikacije omogućavaju registraciju bez stvarnog identiteta korisnika, korištenje virtuelnih telefonskih brojeva, anonimnih e-mail adresa i pseudonima, dok određene platforme uopšte ne zahtijevaju verifikaciju identiteta. Dodatni problem predstavlja činjenica da korisnici često pristupaju komunikacionim servisima putem VPN servisa, TOR mreže ili drugih alata za prikrivanje IP adrese i lokacije.[21] Time se otežava identifikacija korisnika, određivanje mjesta komunikacije i povezivanje digitalnog identiteta sa konkretnim fizičkim licem.

Savremeni komunikacioni sistemi sve češće koriste privremene i samobrišuće komunikacije. Aplikacije omogućavaju automatsko brisanje poruka nakon određenog vremenskog perioda, deaktivaciju mogućnosti pravljenja snimaka ekrana, nestajanje multimedijalnih sadržaja nakon pregleda i druge funkcije koje smanjuju mogućnost naknadnog dokazivanja komunikacije.[22] Takve funkcionalnosti imaju legitiman značaj u zaštiti privatnosti korisnika, ali istovremeno predstavljaju ozbiljan problem za kriminalističke istrage, jer se komunikacija često briše prije nego što organi provođenja zakona uspiju pribaviti sudsku naredbu ili izvršiti forenzičko izuzimanje uređaja.

Posebnu složenost savremenih komunikacionih sistema predstavlja cloud infrastruktura i decentralizacija podataka. Podaci se više ne nalaze nužno na jednom uređaju ili serveru, već se čuvaju u distribuiranim sistemima koji mogu obuhvatati više država i različite pružaoce usluga. Time se otežava određivanje nadležnosti, pribavljanje podataka i primjena nacionalnih pravnih mehanizama. U pojedinim slučajevima sadržaj komunikacije može biti fizički smješten u jednoj državi, metapodaci u drugoj, a korisnik i krivični po-

[20] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

[21] Moore, T., & Rid, T. (2016). "Cryptopolitik and the Darknet." *Survival*, 58(1), 7–38.

[22] Kessler, G. C. (2021). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.

stupak u trećoj državi.[23] Takva decentralizacija dodatno komplikuje međunarodnu pravnu pomoć i postavlja pitanje primjene nacionalnog suvereniteta u digitalnom prostoru.

Savremeni trendovi pokazuju da razvoj komunikacionih platformi ide ka povećanju nivoa privatnosti, decentralizacije i tehničke otpornosti na nadzor. U tom smislu, tehnološki razvoj direktno utiče na transformaciju kriminalističkih metoda i zahtijeva kontinuirano prilagođavanje operativnih, forenzičkih i pravnih mehanizama savremenim digitalnim okruženjima.

4.2. SKY ECC, ANOM i slične platforme

Platforme SKY ECC, ANOM, EncroChat i slični sistemi predstavljaju specifičan oblik enkriptovanih komunikacionih mreža koje su razvijene sa ciljem pružanja maksimalnog nivoa sigurnosti i anonimnosti korisnicima. Za razliku od komercijalnih aplikacija dostupnih široj javnosti, ove platforme bile su prvenstveno usmjerene prema korisnicima koji zahtijevaju visok stepen tajnosti komunikacije, uključujući organizovane kriminalne grupe.[24]

Način funkcionisanja ovih platformi zasnivao se na kombinaciji hardverske i softverske zaštite. Korisnicima su često prodavani posebno modifikovani mobilni uređaji sa uklonjenim standardnim funkcijama poput GPS-a, kamere ili mikrofona, dok je komunikacija bila dostupna isključivo putem enkriptovanih aplikacija. Sistemi su koristili višeslojnu enkripciju, servere raspoređene u više država i mehanizme automatskog brisanja podataka.[25] Određene platforme imale su čak i funkcije daljinskog uništavanja sadržaja uređaja ili aktiviranja posebnog „panic" režima kojim se trenutno brišu svi podaci u slučaju opasnosti od otkrivanja.

U praksi su ovakve platforme veoma brzo postale dominantno sredstvo komunikacije organizovanih kriminalnih grupa koje se bave trgovinom opojnim drogama, pranjem novca, krijumčarenjem oružja, međunarodnim krijumčarenjem ljudi i drugim oblicima teškog kriminaliteta. Komunikacija putem takvih sistema kriminalnim grupama omogućavala je visok nivo konspiracije i osjećaj sigurnosti da komunikacija ne može biti presretnuta. Posebno je značajno što su članovi kriminalnih organizacija često vjerovali da upravo korištenje ovakvih platformi garantuje apsolutnu anonimnost i nemogućnost praćenja.[26]

Međunarodne operacije protiv platformi SKY ECC, EncroChat i ANOM predstavljaju jedan od najznačajnijih primjera savremene međunarodne policijske i obavještajne saradnje. Operacija protiv platforme ANOM bila je specifična po tome što je sama platforma razvijena i kontrolisana od strane američkog FBI-a u saradnji sa međunarodnim partnerima, pri čemu su kriminalne grupe nesvjesno koristile komunikacioni sistem pod kontrolom organa provođenja zakona. U slučaju EncroChat-a i SKY ECC-a, evropske policijske i pravosudne institucije uspjele su kompromitovati infrastrukturu sistema i pristupiti velikom broju komunikacija korisnika.[27] Takve operacije rezultirale su hiljadama hapšenja, zaplje-

---

[23] Broadhurst, R., & Chang, L. Y. C. (2013). "Cybercrime in Asia: Trends and Challenges." *Asian Handbook of Criminology*, 49–64.

[24] Europol. (2021). *Decoding the EU's Most Threatening Criminal Networks*. Publications Office of the European Union.

[25] Cox, J. (2024). *Dark Wire: The Incredible True Story of the Largest Sting Operation Ever*. PublicAffairs.

[26] United Nations Office on Drugs and Crime (UNODC). (2023). *Global Study on Homicide and Organized Crime*. United Nations.

[27] Federal Bureau of Investigation (FBI). (2021). *ANOM Platform Operation – Operation Trojan*

nama narkotika, oružja i novca, kao i otkrivanjem brojnih organizovanih kriminalnih mreža širom Evrope.

Međutim, upravo su ove operacije otvorile brojna pravna pitanja u vezi sa zakonitošću pribavljanja, ustupanja i korištenja podataka. U mnogim državama postavljeno je pitanje da li su domaći organi imali dovoljno informacija o načinu pribavljanja podataka, da li je poštovan nacionalni procesni okvir i da li su optuženi imali mogućnost djelotvornog osporavanja autentičnosti i zakonitosti dokaza.[28] Poseban problem predstavlja činjenica da se veliki dio tehničkih detalja međunarodnih operacija često tretira kao povjerljiv, što dodatno komplikuje procesnu provjeru dokaza pred sudovima.

U savremenoj sudskoj praksi sve više dolazi do sukoba između potrebe efikasnog suprotstavljanja organizovanom kriminalitetu i zahtjeva za zaštitom prava na pravično suđenje, privatnost i djelotvornu sudsku kontrolu. Upravo zbog toga pitanja povezana sa SKY ECC i ANOM predmetima imaju mnogo širi značaj od pojedinačnih krivičnih postupaka, jer otvaraju pitanje budućeg pravnog modela postupanja sa prekograničnim elektronskim dokazima i tajnim digitalnim operacijama.

4.3. Savremeni oblici prikrivene digitalne komunikacije

Savremeni organizovani kriminal karakteriše stalna adaptacija na metode rada organa provođenja zakona. Zbog toga kriminalne grupe razvijaju različite oblike prikrivene digitalne komunikacije koji prevazilaze klasične modele korištenja enkriptovanih aplikacija. Danas se sve češće koriste kombinovane metode komunikacije kojima je cilj smanjiti mogućnost identifikacije korisnika i otežati digitalnu forenzičku rekonstrukciju komunikacije.

Komercijalne aplikacije poput WhatsApp-a, Viber-a, Telegram-a i Signal-a postale su široko rasprostranjene i među kriminalnim strukturama upravo zbog visokog nivoa enkripcije i globalne dostupnosti. Posebno se izdvaja Signal, koji važi za jednu od sigurnijih platformi zbog otvorenog protokola enkripcije i ograničenog čuvanja podataka o korisnicima.[29] Kriminalne grupe često koriste više različitih aplikacija paralelno, pri čemu se jedna koristi za svakodnevnu komunikaciju, druga za osjetljive informacije, a treća za hitne ili kratkotrajne kontakte.

U praksi je sve prisutnija privremena instalacija i brisanje aplikacija. Korisnici instaliraju aplikaciju samo u trenutku komunikacije, nakon čega je uklanjaju sa uređaja zajedno sa sadržajem komunikacije. Time pokušavaju izbjeći naknadno forenzičko pronalaženje komunikacije tokom pretresa uređaja. Dodatno, koriste se sekundarni uređaji, anonimni SIM brojevi i uređaji kupljeni bez registracije identiteta, što dodatno otežava povezivanje komunikacije sa konkretnim licem.[30]

Jedan od posebno zanimljivih oblika prikrivene komunikacije jeste komunikacija putem draft poruka na e-mail servisima. Dva ili više korisnika koriste isti pristupni nalog elektronske pošte, pri čemu poruke ne šalju klasično, već ih ostavljaju u draft folderu. Dru-

Shield. U.S. Department of Justice; Europol. (2021). *EncroChat and Sky ECC Operations*. Europol Media Releases.

[28] Fair Trials. (2023). *A Comparative Study of the Use of EncroChat and Sky ECC Data in Criminal Proceedings Across Europe*. Fair Trials International.

[29] Marlinspike, M., & Perrin, T. (2016). *The Signal Protocol*. Open Whisper Systems Documentation.

[30] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

gi korisnik pristupa nalogu, pročita sadržaj i po potrebi ga izbriše ili izmijeni. Na taj način ne nastaje klasičan trag elektronske pošte u sistemu razmjene poruka, što može otežati otkrivanje komunikacije.[31]

VPN servisi, TOR mreža i anonimni servisi predstavljaju dodatni nivo zaštite digitalnog identiteta. VPN omogućava prikrivanje stvarne IP adrese i geografske lokacije korisnika, dok TOR mreža komunikaciju usmjerava kroz više anonimnih čvorova širom svijeta. Time se otežava identifikacija izvora komunikacije i praćenje internet aktivnosti korisnika.[32] Pored toga, određene kriminalne strukture koriste dark web komunikacione forume, anonimne platforme za razmjenu datoteka i decentralizovane komunikacione mreže koje funkcionišu bez centralnog servera.

Savremeni oblici prikrivene komunikacije pokazuju da organizovani kriminal sve više koristi principe digitalne konspiracije, odnosno kombinovanje tehničkih, operativnih i psiholoških metoda radi smanjenja mogućnosti otkrivanja. Time se kriminalističke istrage suočavaju sa potrebom stalnog tehnološkog prilagođavanja i razvoja novih metoda digitalne forenzike i kriminalističko-obavještajne analitike.

4.4. Operativni izazovi organa provođenja zakona

Razvoj enkriptovanih komunikacionih platformi i savremenih metoda digitalne konspiracije doveo je do značajnog smanjenja efikasnosti tradicionalnih metoda nadzora telekomunikacija. Organi provođenja zakona danas se suočavaju sa situacijom da često mogu identifikovati postojanje komunikacije, ali ne i njen sadržaj. Time se klasični modeli presretanja telefonskih razgovora i komunikacija sve više zamjenjuju složenijim oblicima digitalne forenzike, analize metapodataka i pristupa krajnjim uređajima.[33]

Jedan od najvećih operativnih problema jeste nemogućnost presretanja sadržaja komunikacije kod sistema koji koriste end-to-end enkripciju. Čak i kada postoji zakonita sudska naredba, pružaoci usluga često tehnički nisu u mogućnosti dostaviti sadržaj komunikacije jer ga ne posjeduju u čitljivom obliku.[34] Organi provođenja zakona tada se oslanjaju na alternativne metode poput pristupa uređajima korisnika, instaliranja specijalizovanih istražnih alata ili pribavljanja podataka iz sigurnosnih kopija i cloud sistema.

Savremeni razvoj enkriptovanih komunikacija pokazuje da tradicionalni koncept nadzora telekomunikacija više nije dovoljan za efikasno otkrivanje organizovanog kriminaliteta. Buduće normativne reforme morale bi preciznije urediti odnos između tehničkih mogućnosti digitalnog nadzora i procesnih garancija zaštite osnovnih prava.

Poseban izazov predstavlja identifikacija korisnika komunikacionih platformi. Kriminalne grupe koriste pseudonime, anonimne SIM kartice, virtuelne brojeve, privremene uređaje i različite identitete kako bi prikrile stvarne korisnike komunikacije. U praksi nije dovoljno dokazati postojanje određene komunikacije; potrebno je dokazati ko je konkretnu komunikaciju koristio, sa kojeg uređaja, u kojem vremenskom periodu i sa kojom svrhom. Upravo zbog toga elektronski dokazi često zahtijevaju kombinovanje sa drugim dokazima, uključujući nadzor kretanja, finansijske istrage, svjedočenja i rezultate pretresa.

---

[31] Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

[32] Moore, T., & Rid, T. (2016). "Cryptopolitik and the Darknet." *Survival*, 58(1), 7–38.

[33] Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). Sage Publications.

[34] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Tehničke i forenzičke prepreke dodatno komplikuju savremene istrage. Savremeni mobilni uređaji koriste napredne sigurnosne mehanizme, uključujući hardversku enkripciju, biometrijsku zaštitu, automatsko zaključavanje i mogućnost daljinskog brisanja podataka. Digitalna forenzika zbog toga postaje izuzetno složena i zahtijeva specijalizovana znanja, sofisticiranu opremu i stalno prilagođavanje novim tehnologijama.[35] Pored toga, veliki problem predstavlja kratko vrijeme dostupnosti određenih podataka, naročito kod aplikacija koje koriste samobrišuće komunikacije.

U praksi se sve više pokazuje da uspješnost savremenih istraga ne zavisi isključivo od zakonskih ovlaštenja, već od nivoa tehničke opremljenosti i stručne osposobljenosti organa provođenja zakona. Zbog toga bi razvoj digitalne forenzike trebalo posmatrati kao strateški prioritet savremenih bezbjednosnih sistema.

Međunarodna saradnja predstavlja neophodan, ali često spor i komplikovan segment savremenih istraga elektronskih komunikacija. Podaci se nalaze u različitim državama, pod kontrolom privatnih kompanija koje posluju prema različitim pravnim režimima. Razlike u nacionalnim zakonodavstvima, zaštiti podataka, standardima privatnosti i procedurama međunarodne pravne pomoći često dovode do kašnjenja ili nemogućnosti pribavljanja relevantnih podataka.[36] U hitnim slučajevima takva kašnjenja mogu direktno ugroziti uspješnost istrage ili mogućnost sprečavanja krivičnih djela.

Sporost klasičnih mehanizama međunarodne pravne pomoći često nije kompatibilna sa dinamikom savremenih digitalnih istraga, naročito kod komunikacija koje koriste privremeno čuvanje podataka i automatsko brisanje sadržaja.

Savremeni operativni izazovi pokazuju da se kriminalističke istrage elektronskih komunikacija više ne mogu zasnivati isključivo na tradicionalnim metodama nadzora telekomunikacija. Efikasno suprotstavljanje organizovanom kriminalitetu u digitalnom okruženju zahtijeva integraciju kriminalističkih, tehničkih, forenzičkih i međunarodnopravnih mehanizama, kao i kontinuirano unapređenje stručnih i tehnoloških kapaciteta organa provođenja zakona.

5. ZAKLJUČAK

Savremeni razvoj informaciono-komunikacionih tehnologija i ubrzana digitalizacija društvenih odnosa doveli su do suštinske transformacije načina izvršenja, prikrivanja i dokazivanja krivičnih djela. Enkriptovane komunikacione platforme, decentralizovani sistemi razmjene podataka i savremeni oblici digitalne konspiracije značajno su izmijenili operativno okruženje u kojem djeluju organi provođenja zakona. Tradicionalni modeli nadzora telekomunikacija, zasnovani prvenstveno na presretanju sadržaja komunikacije putem operatora, sve više gube efikasnost u uslovima end-to-end enkripcije, anonimnih komunikacionih servisa i globalno distribuirane digitalne infrastrukture. Time elektronske komunikacije postaju ne samo tehničko, već i složeno pravno, kriminalističko i bezbjednosno pitanje.

Rezultati istraživanja potvrđuju polaznu pretpostavku da savremene enkriptovane platforme značajno otežavaju primjenu posebnih istražnih radnji i smanjuju efikasnost tradicionalnih metoda nadzora komunikacija. Istovremeno je potvrđeno da postoje odre-

[35] Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

[36] Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Council of Europe.

đene normativne i institucionalne nedorečenosti u oblasti pribavljanja, razmjene i korištenja elektronskih dokaza, posebno kada se radi o podacima pribavljenim putem međunarodne saradnje i prekograničnih operacija protiv enkriptovanih mreža. Analiza međunarodne i domaće prakse pokazuje da se savremeni krivični postupci sve više suočavaju sa potrebom uspostavljanja ravnoteže između efikasnog krivičnog gonjenja i zaštite prava na privatnost, pravično suđenje i kontrolu zakonitosti primjene posebnih istražnih radnji.

Naučni doprinos rada ogleda se u interdisciplinarnom sagledavanju problema nadzora elektronskih komunikacija kroz povezivanje kriminalističkog, krivičnoprocesnog, tehničkog i međunarodnopravnog aspekta. Poseban značaj rada jeste u sistematizaciji savremenih oblika digitalne komunikacije i analizi njihovog uticaja na dokazivanje krivičnih djela u eri enkriptovanih platformi. Rad ukazuje da savremeni elektronski dokazi više ne mogu biti posmatrani isključivo kao tehnički podaci, već kao složeni procesni i forenzički elementi čija dokazna vrijednost zavisi od zakonitosti pribavljanja, očuvanog lanca čuvanja, autentičnosti i mogućnosti sudske provjere.

Praktični značaj istraživanja ogleda se u identifikovanju ključnih operativnih izazova sa kojima se suočavaju policijske, tužilačke i pravosudne institucije u savremenim digitalnim istragama. Posebno se ukazuje na potrebu jačanja digitalne forenzike, specijalizacije istražilaca i tužilaca, unapređenja međunarodne operativne saradnje i razvoja zajedničkih standarda za postupanje sa elektronskim dokazima. Analiza pokazuje da uspješnost savremenih istraga sve manje zavisi od klasičnog presretanja komunikacija, a sve više od sposobnosti integracije kriminalističko-obavještajnih podataka, digitalne forenzike, analize metapodataka i međunarodne razmjene informacija.

Sa krivičnoprocesnog aspekta, posebno je značajno pitanje zakonitosti i procesne prihvatljivosti dokaza pribavljenih putem međunarodnih operacija protiv enkriptovanih platformi. Savremena sudska praksa pokazuje da elektronski dokazi zahtijevaju mnogo strožije standarde provjere nego tradicionalni materijalni dokazi, naročito u pogledu autentičnosti, integriteta i mogućnosti djelotvornog osporavanja od strane odbrane. Time se potvrđuje da razvoj savremenih istražnih tehnologija mora biti praćen odgovarajućim razvojem procesnih garancija i mehanizama zaštite osnovnih ljudskih prava.

Kriminalistički aspekt istraživanja potvrđuje da organizovani kriminal i druge ozbiljne bezbjednosne prijetnje sve više koriste principe digitalne konspiracije, anonimnosti i tehničke zaštite komunikacija. To zahtijeva kontinuirano prilagođavanje metoda rada organa provođenja zakona, razvoj specijalizovanih kapaciteta i uspostavljanje savremenih modela digitalnih istraga. Budući razvoj kriminalistike i krivičnog procesnog prava nesumnjivo će biti uslovljen sposobnošću država da odgovore na izazove enkriptovanih komunikacija uz očuvanje demokratskih standarda, vladavine prava i zaštite osnovnih sloboda građana.

Budući razvoj krivičnog procesnog prava nesumnjivo će biti uslovljen potrebom redefinisanja tradicionalnih koncepata nadzora komunikacija u uslovima masovne enkripcije i decentralizovanih digitalnih sistema.

U tom smislu, unapređenje sistema nadzora i dokazivanja zahtijeva modernizaciju normativnog okvira, preciznije regulisanje elektronskih dokaza, efikasnije mehanizme međunarodne saradnje i kontinuirano stručno usavršavanje svih subjekata uključenih u digitalne istrage. Samo integrisanim pristupom koji povezuje pravne, tehničke, kriminalističke i međunarodne mehanizme moguće je obezbijediti efikasno suprotstavljanje savremenim oblicima organizovanog i transnacionalnog kriminaliteta u digitalnom okruženju.

LITERATURA

Broadhurst, R., & Chang, L. Y. C. (2013). "Cybercrime in Asia: Trends and Challenges." *Asian Handbook of Criminology*.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). "Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime." *International Journal of Cyber Criminology*, 8(1).

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

Castells, M. (2010). *The Rise of the Network Society* (2nd ed.). Wiley-Blackwell.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. ETS No. 185.

Council of Europe. (2020). *Cybercrime Policies/Strategies of Bosnia and Herzegovina*. Council of Europe Cybercrime Programme Office.

Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Council of Europe.

Council of Europe. (2025). *Bosnia and Herzegovina moves towards the signature and implementation of the Second Additional Protocol to the Convention on Cybercrime*. CyberSEE Project.

Cox, J. (2024). *Dark Wire: The Incredible True Story of the Largest Sting Operation Ever*. PublicAffairs.

European Convention on Human Rights. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Council of Europe.

European Court of Human Rights. (1978). *Klass and Others v. Germany*, Application no. 5029/71.

European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15.

European Court of Human Rights. (2021). *Centrum för Rättvisa v. Sweden*, Application no. 35252/08.

Europol. (2021). *Decoding the EU's Most Threatening Criminal Networks*. Publications Office of the European Union.

Europol. (2023). *Serious and Organised Crime Threat Assessment (SOCTA) 2023*. Publications Office of the European Union.

Eurojust. (2022). *The Second Additional Protocol to the Budapest Convention on Cybercrime and enhanced cross-border access to electronic evidence*. Eurojust Publications Office.

Fair Trials. (2023). *A Comparative Study of the Use of EncroChat and Sky ECC Data in Criminal Proceedings Across Europe*. Fair Trials International.

Federal Bureau of Investigation (FBI). (2021). *ANOM Platform Operation – Operation Trojan Shield*. U.S. Department of Justice.

Greenberg, A. (2022). *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Doubleday.

Harris, D., O'Boyle, M., Bates, E., & Buckley, C. (2023). *Law of the European Convention on Human Rights* (5th ed.). Oxford University Press.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Kessler, G. C. (2021). *Digital Evidence and Computer Crime* (4th ed.). Academic Press.

Kizza, J. M. (2020). *Guide to Computer Network Security* (6th ed.). Springer.

Marlinspike, M., & Perrin, T. (2016). *The Signal Protocol*. Open Whisper Systems Documentation.

Moore, T., & Rid, T. (2016). "Cryptopolitik and the Darknet." *Survival*, 58(1).

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Simović, M., & Simović, V. (2021). *Krivično procesno pravo Bosne i Hercegovine.* Pravni fakultet Univerziteta u Banjoj Luci.

United Nations Office on Drugs and Crime (UNODC). (2023). *Global Study on Homicide and Organized Crime*. United Nations.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). Sage Publications.

Zakon o komunikacijama Bosne i Hercegovine, „Službeni glasnik BiH", br. 31/03, 75/06, 32/10 i 98/12.

Zakon o krivičnom postupku Bosne i Hercegovine, „Službeni glasnik BiH", br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13 i 65/18.

Zakon o zaštiti ličnih podataka Bosne i Hercegovine, „Službeni glasnik BiH", br. 12/25.

Criminalistic and Legal Challenges of Electronic Communications Surveillance in the Era of Encrypted Platforms

Prof. dr Goran Gajić

Pan-European University "APEIRON", goranga@teol.net

Abstract: The contemporary development of information and communication technologies has led to significant changes in the manner of interpersonal communication, while simultaneously transforming the methods of committing and concealing criminal offences. Encrypted communication platforms and modern forms of digital communication represent a particular challenge for law enforcement agencies, as they enable criminal groups to achieve a high level of anonymity, security, and resistance to detection. The use of applications such as SKY ECC, ANOM, Signal, and similar systems, as well as temporary communication methods including self-destructing applications, draft communication via e-mail services, and anonymous internet services, considerably complicates the implementation of special investigative measures involving the surveillance and technical interception of telecommunications.

The subject of this paper concerns the criminalistic and legal challenges of electronic communications surveillance in the era of encrypted platforms, with a particular focus on the legality of obtaining, using, and assessing the evidentiary value of electronic evidence in criminal proceedings. The paper analyses contemporary forms of digital communication used by organized criminal groups, the technical and operational obstacles involved in detecting such communications, as well as the normative framework governing the implementation of special investigative measures in Bosnia and Herzegovina and international law.

Special attention is devoted to the admissibility of evidence obtained through international cooperation and data transferred from encrypted platforms, particularly in the context of SKY ECC and ANOM cases, as well as to the relationship between the protection of the right to privacy and the necessity of effective criminal prosecution. The paper also examines issues related to the authentication, integrity, and reliability of digital evidence, together with the challenges of digital forensics in reconstructing deleted or concealed communications.

Keywords: electronic communications, encrypted platforms, SKY ECC, ANOM, special investigative measures, telecommunications surveillance, electronic evidence.