KRIMINALISTIČKE, KRIMINOLOŠKE I PRAVNE TEME

ČASOPIS ZA KRIMINALISTIČKU, KRIMINOLOŠKU I PRAVNU TEORIJU I PRAKSU

Kanton Središnja Bosna
Srednjobosanski kanton
Ministarstvo obrazovanja, znanosti, mladih, kulture i sporta

Izdavanje 5 (petog) broja Časopisa kriminalističke, kriminološke i pravne teme, finansijski je podržalo Ministarstvo obrazovanja nauke, mladih, kulture i sporta Vlade Srednjobosasnkog kantona/Kantona Središnja Bosna.

IZDAVAČ

CENTAR ZA KRIMINALISTIČKA, KRIMINOLOŠKA I PRAVNA ISTRAŽIVANJA

.....

SJEDIŠTE REDAKCIJE ČASOPISA

Ul. Školska 23, 72270 Travnik

GLAVNI I ODGOVORNI UREDNIK

Prof.dr.sci. Adnan PIRIĆ

Tiraž

100 primjeraka

ISSN

2744-2799

UDK

343.9

SADRŽAJ

ČASOPIS ZA KRIMINALISTIČKU, KRIMINOLOŠKU I PRAVNU TEORIJU I PRAKSU

Centar za kriminalistička, kriminološka i pravna istraživanja osnovan je sredinom 2020.godine, te je u isto vrijeme utemeljen kao samostalna organizacija kriminalista, kriminologa, pravnika i drugih srodnih zanimanja, što je jedinstven primjer u Bosni i Hercegovini.

„Kriminalističke, kriminološke i pravne teme, Časopis za kriminalističku, kriminološku i pravnu teoriju i praksu, ustanovljen je kao „glasilo“ članova Centra, koje doprinosi ostvarivanju zajedničkih programskih interesa kriminalista, kriminologa, pravnika i drugih srodnih zanimanja u profesionalnom unapređenju struke i razvijanju najviših moralnih vrijednosti, kriminalističke, kriminološke i pravne etike i kulture. Časopis objavljuje članke naučnog i stručnog karaktera iz oblasti kriminalistike, kriminologije, prava i drugih srodnih naučnih disciplina te teorijska istraživanja i studije iz uprednog prava i domaće prakse, kao i materijale sa naučnih, stručnih i konsulantskih javnih rasprava i drugih skupova kriminalista, kriminologa, pravnika i drugih srodnih naučnih disciplina. Časopis objavljuje referate, saopštenja i diskusije u kojima se poklanja pažnja svemu onome što se zbiva u našem kriminalističkom, kriminološkom, pravnom i uopšte društvenom životu i društvu u cjelini, a što na bilo koji način doprinosi stvaranju vladavine prava i moderne pravne države, odnosno izgrađivanju i normalnom funkcionisanju pravnog i društvenog sistema. Na njegovim stranicama objavljuju se i odabrane odluke iz sudske, upravne, arbitražne, i druge prakse, osvrti i prikazi novih knjiga iz pravne kriminalističke, kriminološke i druge društvene književnosti, kao i raznovrsni prilozi iz svakodnevne prakse. Kao glasilo kriminalista, kriminologa, pravnika i drugih zainteresovanih osoba, Časopis prati njihovo djelovanje i o tome obavještava čitaoce i ukupnu javnost.

Broj, 5 **Godina V** **Travnik 2026.**

Ovaj broj Časopisa namjenjen je svima onima koji imaju profesionalnu, ali i moralnu odgovornost i obavezu blagovremeno i odgovarajuće reagovati na bilo koji način u skladu sa svojom ulogom.

RIJEČ UREDNIKA

Poštovane/i čitateljice i čitatelji, veliko mi je zadovoljstvo i čast predstaviti novi a po redu peti broj Časopisa, „Kriminalističke, kriminološke i pravne teme“ broj; V za 2026. godinu, koji sadrži šest naučnih i stručnih radova. Peti/1 broj Časopisa započinje radom autorice: Atine Perković na temu, “Uloga umjetne inteligencije (AI) u radu policije“, ovaj rad detaljno analizira mogućnosti i ograničenja primjene (AI) u policijskom sektoru, s posebnim naglaskom na pravni i institucionalni okvir Bosne i Hercegovine. Rad se metodološki zasniva na analizi relevantne naučne literature, međunarodnih smjernica i regulatornih dokumenata, uz komparativni osvrt na prakse razvijenih zemalja. Dok rezultati analize ukazuju da (AI) može doprinijeti povećanju efikasnosti policijskih agencija, boljem upravljanju resursima i unapređenju preventivnog djelovanja, posebno u oblastima prediktivnog policijskog rada, video-nadzora, digitalne forenzike i operativnog planiranja. Drugi rad u ovom broju Časopisa, je tekst koji sadrži jedno vrlo zanimljivo viđenje “Procjene nivoa javne svijesti i poznavanja rizika kibernetičke sigurnosti u sistemima upravljanja i kontrole kritične infrastrukture u Bosni i Hercegovini“, autorice Inde Kreso. Rad suštinski predstavlja prvo empirijsko istraživanje u Bosni i Hercegovini koje analizira nivo javne svijesti, znanja i percepcije rizika kibernetičke sigurnosti u sistemima upravljanja i kontrole kritične infrastrukture *(eng. Operation Technology - OT/eng. Industrial Control Systems - ICS).* Iako su tehničke i inženjerske mjere zaštite najbitnije i osnovne, ljudski faktor, svijest, povjerenje i percepcija stanovništva ostaje presudan za jačanje otpornosti i zaštitu kritične infrastrukture u Bosni i Hercegovini. Analiza rezultata pokazuje da javnost BiH ispravno percipira ozbiljnost i važnost kibernetičkih prijetnji i da posjeduje relativno dobar nivo općeg znanja o zaštiti kritične infrastrukture. Također, javnost vjeruje u sposobnost CERT BiH tima (koji još uvijek nije u potpunosti funkcionalan), u njihovu spremnost i stručnost, dok nemaju tako veliko povjerenje u institucionalnu zaštitu i spremnost. Da je psihološko profiliranje počinioca jedna od važnijih, ali istovremeno i najmanje korištenih savremenih metoda prevencije kriminaliteta u zemljama regiona, piše nam na istoimenu temu kolegica Maida Muratović u trećem po redu radu našeg petog broja u 2026.godini. Motiv kolegice za analiziranje ove teme leži u potrebi temeljitijeg razumijevanja ljudi u sopstvenom okruženju i identifikaciji osobe čije bi karakteristike mogle ukazivati na kriminogeni potencijal. Cilj rada jes da se analizom profilisanja kriminogene ličnosti prevenira nasilje i smanji broj žrtava. U savremenim društvima, posebno onima suočenim s porastom kriminaliteta, prirodno se nameće pitanje: da li je svaka osoba potencijalni počinitelj krivičnog djela. Naglasak nije na stigmatizaciji, nego na razlikovanju rizičnih i nerizičnih osobina, razumijevanju utjecaja okoline, stresa, trauma i predispozicija na ponašanje pojedinca. Uz nadahnuće i proaktivnost kolege Prohan Rusmira, koji vrlo temeljito uz podršku moje malenkosti analizira jednu posve “novu” i nadasve aktuelnu temu zainteresiranim stakeholderima našeg Časopisa na raspolaganju je četvrti rad ovog broja na temu; “Uloga savremene medicine u funkciji otkrivanja i dokazivanja krivičnih djela”, nastojimo na drugačiji način čitateljima predstaviti medicinu, odnosno kao spoj naučnog i praktičnog. Medicina kao naučna i praktična disciplina svoju ulogu u polju kriminalistike i krivičnog prava dokazuje kroz sudsko-medicinska vještačenja, čiji je permanentni zadatak otkrivanje i razjašnjavanje objektivnih činjenica kod počinjenih krivičnih djela: tjelesne povrede; utvrđivanje vremena i uzroka smrti, sudsko-

medicinska obdukcija leševa; vještačenje dijelova tjela; toksikološka vještačenja; biološka traseologija; makrotragovi i kontaktni mikrotragovi drugog porijekla; genetika nasljeđivanja; postupak indentifikacije, i td... kod otkrivanja krivičnog djela i izvršioca. Međutim razvojem medicine, a posebno Medicinske kriminalistike, uočljiva je njena preokupacija čovječijim životom, njegovom zaštitom i svim krivičnopravnim regulativama koje iz toga proizilaze. Iz navedenog proizilazi potreba za kontinuiranom saradnjom između medicinara, kriminalista i pravnika. Činjenice da savremene organizirane kriminalne grupe (OKG) djeluju u prostoru koji je istovremeno fizički i digitalni, pri čemu njihovo kriminalno ponašanje generira značajne javno dostupne informacijske tragove u svom vrlo zanimljivom pritupu ovakvoj tematici piše nam kolega Emir Muhić, na temu „Praktična primjena osint metoda u istraživanju organiziranih kriminalnih grupa.“ Koelga smatra da, iako digitalni prostor postaje centralno operativno okruženje savremenog kriminalnog djelovanja, metode prikupljanja obavještajnih podataka iz otvorenih izvora (OSINT) u praksi krim-obavještajnog rada, kao i u akademskim istraživanjima, ostaju nedovoljno konceptualizirane i rijetko razmatrane kao zaseban analitički pristup. Motiv za pisanje ovog rada kolega pronalazi u potrebi da prikaže praktičnu i analitičku upotrebu OSINT metoda u identifikaciji, mapiranju i praćenju OKG, sa fokusom na njihovu primjenu u različitim fazama istražnog postupka. Pa tako se u radu identifikuju ključni OSINT izvori, relevantne analitičke metode i predlažu osnovni modeli primjene OSINT-a u krim-obavještajnom radu, s ciljem unapređenja razumijevanja i operativne upotrebe otvorenih izvora u suzbijanju organiziranog kriminala. O „specifičnosti online groominga i kriminološkim implikacijima digitalnog okruženja“, a posljednjem šestom po redu tekstu u ovom broju Časoposa svoj osvrt donosi nam kolegica Aldina Bjelić, kolegica precizno analizira specifičnosti online groominga kao procesnog i manipulativnog oblika seksualne eksploatacije djece, s posebnim naglaskom na psihološke, kriminalne i digitalne dimenzije ovog fenomena. U teoretskom dijelu prikazuje faze manipulacije, tipologije počinilaca i obrasce ponašanja koji omogućavaju izgradnju prividno sigurnog odnosa između djeteta i groomera. Dok posebnu pažnju posvećuje digitalnom okruženju, koje svojim tehničkim karakteristikama, anonimnošću i infrastrukturom više platformi omogućava fragmentiranost tragova i otežava rekonstrukciju komunikacijskog toka. Kolegica na kraju zaključuje, da je online grooming kompleksan fenomen koji zahtijeva interdisciplinarni pristup, jačanje digitalne pismenosti i razvoj preventivnih strategija koje uvažavaju psihološke, tehnološke i društvene komponente rizika.

Na kraju, prilika je ovo da se zahvalimo svim autoricama/autorima na dostavljenim radovima, recenzenticama i recenzentima, te članicama i članovima redakcije, koji su svojim sugestijama i prijedlozima unaprijedili kvalitet i omogućili publiciranje još jednog izdanja časopisa, „Kriminalističke, kriminološke i pravne teme“. Nadam se da će čitateljice i čitatelji i u ovom broju pronaći interesantne i upotrebljive sadržaje.

Glavni i odgovorni urednik

Prof.dr.sci. Adnan Pirić

U Travniku, 31.03.2026.godine

ULOGA UMJETNE INTELIGENCIJE (AI) U RADU POLICIJE

MA Atina Perković, PhDc
atinaperkovic@fkn.unsa.ba

Sažetak: *razvoj umjetne inteligencije (AI) značajno utiče na transformaciju savremenog policijskog rada, omogućavajući efikasniju analizu kriminalnih obrazaca, unapređenje preventivnih aktivnosti i bržu obradu digitalnih dokaza. Cilj ovog rada je analizirati mogućnosti i ograničenja primjene AI u policijskom sektoru, s posebnim naglaskom na pravni i institucionalni okvir Bosne i Hercegovine. Metodološki, rad se zasniva na analizi relevantne naučne literature, međunarodnih smjernica i regulatornih dokumenata, uz komparativni osvrt na prakse razvijenih zemalja. Rezultati analize ukazuju da AI može doprinijeti povećanju efikasnosti policijskih agencija, boljem upravljanju resursima i unapređenju preventivnog djelovanja, posebno u oblastima prediktivnog policijskog rada, video-nadzora, digitalne forenzike i operativnog planiranja. Međutim, istovremeno su identificirani značajni rizici vezani za zaštitu privatnosti, algoritamsku pristrasnost i problem transparentnosti odlučivanja, što zahtijeva strogu regulaciju i snažne nadzorne mehanizme. U kontekstu Bosne i Hercegovine, dodatni izazovi uključuju fragmentiranu institucionalnu strukturu, ograničene finansijske resurse i nedostatak specijaliziranih IT kadrova. Zaključno, rad naglašava potrebu za faznim i odgovornim uvođenjem AI tehnologija u policijski rad, uz paralelno jačanje pravnog okvira, institucionalnih kapaciteta i edukacije policijskih službenika, kako bi se osigurala ravnoteža između unapređenja sigurnosti i zaštite temeljnih ljudskih prava.*

Ključne riječi: *umjetna inteligencija; policijski rad; javna sigurnost; zaštita osobnih podataka; prediktivno policijsko djelovanje; digitalna forenzika; Bosna i Hercegovina.*

1. UVOD

Digitalna transformacija predstavlja jedan od ključnih procesa modernizacije javnog sektora, uključujući i institucije zadužene za sigurnost i provođenje zakona. Razvoj informacijskih i komunikacijskih tehnologija omogućio je obradu velikih količina podataka u realnom vremenu, automatizaciju administrativnih i operativnih procesa te unapređenje analitičkih kapaciteta policijskih agencija. U tom kontekstu, umjetna inteligencija (AI) sve češće se prepoznaje kao strateški alat za unapređenje efikasnosti, preciznosti i brzine policijskog djelovanja (OECD, 2019; European Commission, 2025). Primjena AI tehnologija u sigurnosnom sektoru povezana je i s konceptom „pametnih gradova“, gdje se kroz integraciju senzorskih mreža, video-nadzora i analitičkih platformi nastoji unaprijediti javna sigurnost i prevencija kriminaliteta. Takvi sistemi omogućavaju policiji bržu identifikaciju sigurnosnih prijetnji, bolju koordinaciju operativnih resursa te kvalitetnije donošenje odluka zasnovanih na podacima (Europol, 2025). Suvremeni sigurnosni izazovi karakterizirani su visokom razinom složenosti, transnacionalnim djelovanjem kriminalnih mreža i sve većom upotrebom digitalnih tehnologija od strane počinitelja krivičnih djela. Kibernetički kriminal bilježi kontinuirani rast, uključujući krađe identiteta, finansijske prevare, ransomware napade i zloupotrebu podataka, što značajno opterećuje kapacitete tradicionalnih policijskih metoda (U.S. Department of Justice, 2024). Istovremeno, terorizam i nasilni ekstremizam sve češće

koriste digitalne platforme za radikalizaciju, regrutaciju i operativnu koordinaciju, dok organizirani kriminal koristi sofisticirane finansijske i komunikacijske kanale za prikrivanje ilegalnih aktivnosti. Ovakvi oblici kriminaliteta zahtijevaju napredne analitičke alate sposobne za prepoznavanje obrazaca, povezivanje podataka iz različitih izvora i ranu detekciju prijetnji, što značajno prevazilazi mogućnosti klasičnih policijskih baza podataka (INTERPOL, 2023.; Europol, 2025). Uvođenje AI u policijski rad motivirano je potrebom za povećanjem operativne efikasnosti, unapređenjem preventivnog djelovanja i boljim upravljanjem resursima. AI sistemi omogućavaju automatiziranu analizu velikih skupova podataka, uključujući kriminalističke evidencije, video-snimke, podatke s društvenih mreža i digitalne tragove, čime se značajno skraćuje vrijeme potrebno za istrage i identifikaciju sumnjivih obrazaca ponašanja (Lum & Isaac, 2016). Posebno značajnu ulogu AI ima u prediktivnom policijskom djelovanju, gdje se statističkim i mašinskim modelima procjenjuje vjerovatnoća pojave kriminala u određenim područjima ili u vezi s određenim profilima događaja. Također, biometrijske tehnologije, poput prepoznavanja lica, omogućavaju bržu identifikaciju osumnjičenih osoba i efikasnije upravljanje javnim skupovima, ali istovremeno otvaraju ozbiljna pitanja privatnosti i zaštite ljudskih prava (European Data Protection Board, 2023; Council of Europe, 2021). Dodatni razlog za primjenu AI tehnologija odnosi se na racionalizaciju troškova i bolje planiranje policijskih aktivnosti, posebno u državama s ograničenim budžetskim kapacitetima, gdje se kroz optimizaciju patrola i prioritizaciju intervencija može postići veći sigurnosni učinak uz iste ili manje resurse (Europol, 2025).

2. UMJETNA INTELIGENCIJA: POJMOVNO ODREĐENJE I OSNOVNE TEHNOLOGIJE

Umjetna inteligencija (AI) predstavlja područje računalnih znanosti koje se bavi razvojem sistema sposobnih za obavljanje zadataka koji inače zahtijevaju ljudsku inteligenciju, poput učenja, zaključivanja, prepoznavanja obrazaca, razumijevanja jezika i donošenja odluka. Prema OECD-u (2019), AI sistemi su digitalni sistemi koji, za zadani skup ciljeva, donose preporuke ili odluke koje utiču na fizičko ili virtualno okruženje, koristeći se analizom podataka i algoritamskim modelima. U kontekstu policijskog rada, umjetna inteligencija ne zamjenjuje ljudsko odlučivanje, već služi kao alat za podršku odlučivanju, omogućavajući bržu i precizniju obradu informacija te identifikaciju obrazaca koji nisu lako uočljivi klasičnim analitičkim metodama (Europol, 2025). Machine learning (ML) predstavlja podgranu umjetne inteligencije koja omogućava sistemima da automatski uče iz podataka i poboljšavaju svoje performanse bez eksplicitnog programiranja za svaki pojedinačni zadatak. Algoritmi strojnog učenja prepoznaju statističke obrasce u velikim skupovima podataka i na osnovu toga generiraju predikcije ili klasifikacije (NIST, 2023). U policijskom kontekstu, ML se koristi za analizu kriminalističkih baza podataka, identifikaciju rizičnih lokacija, predviđanje ponavljanja kaznenih djela te detekciju sumnjivih finansijskih transakcija povezanih s organiziranim kriminalom. Ipak, pouzdanost ovih sistema uveliko zavisi od kvaliteta i reprezentativnosti ulaznih podataka, što otvara pitanje mogućih pristrasnosti i pogrešnih procjena (Lum & Isaac, 2016). Deep learning (DL) predstavlja napredniji oblik strojnog učenja koji se zasniva na višeslojnim neuronskim mrežama sposobnim za obradu kompleksnih i nestrukturiranih podataka, poput slika, video-zapisa i govora. Ovi modeli su posebno učinkoviti u zadacima prepoznavanja lica, registarskih tablica, ponašajnih obrazaca i

glasovnih komandi (EDPB, 2023). Zahvaljujući visokoj preciznosti u obradi vizualnih podataka, deep learning je postao ključna tehnologija u sistemima video-nadzora i biometrijske identifikacije, koji se sve češće koriste u policijskim istragama i kontroli javnih prostora. Međutim, upravo ova tehnologija izaziva i najveće zabrinutosti u pogledu privatnosti, masovnog nadzora i mogućnosti zloupotrebe, zbog čega međunarodne institucije insistiraju na strogoj regulaciji njene primjene u policijskom sektoru (Council of Europe, 2021). Analitika velikih podataka odnosi se na proces prikupljanja, integracije i analize izuzetno velikih i raznolikih skupova podataka koji dolaze iz različitih izvora, uključujući baze policijskih evidencija, društvene mreže, mobilne uređaje, nadzorne kamere i senzorske sisteme. Cilj je otkrivanje skrivenih veza, trendova i anomalija koje mogu ukazivati na sigurnosne prijetnje (U.S. Department of Justice, 2024). U kombinaciji s AI algoritmima, Big Data analitika omogućava policiji da povezuje informacije iz više sistema, prepoznaje kriminalne mreže i unaprijedi strateško planiranje operacija. Ipak, ovakav pristup nosi i značajne rizike u pogledu zaštite osobnih podataka, naročito ako se podaci prikupljaju bez jasnih pravnih osnova i nadzornih mehanizama (UNESCO, 2021). Na globalnom nivou, upotreba umjetne inteligencije u sektoru javne sigurnosti bilježi snažan rast, potaknuta razvojem digitalne infrastrukture, dostupnošću velikih količina podataka i sve većim sigurnosnim izazovima. Policijske agencije širom svijeta koriste AI za prediktivno policijsko djelovanje, automatsku analizu video-materijala, digitalnu forenziku i upravljanje kriznim situacijama (INTERPOL, 2023.). Istovremeno, međunarodne organizacije naglašavaju potrebu za odgovornom i zakonitom primjenom AI, posebno u kontekstu zaštite ljudskih prava. Evropska unija je, kroz AI Act, uvela stroge kategorije rizika za primjene AI u policiji, pri čemu su biometrijski sistemi u realnom vremenu svrstani među visokorizične ili zabranjene, osim u izuzetnim okolnostima (European Union, 2024). Ovakav regulatorni pristup ukazuje na nastojanje da se tehnološki napredak uskladi s temeljnim pravima građana. Koncept pametnih gradova (smart cities) podrazumijeva integraciju digitalnih tehnologija u urbano upravljanje s ciljem povećanja efikasnosti javnih usluga, uključujući i sigurnost. U tom okviru, AI se koristi za analizu podataka iz saobraćajnih sistema, javnih kamera, senzora i društvenih mreža kako bi se unaprijedila prevencija kriminala i odgovor na incidente (European Commission, 2025). Prediktivna sigurnost, kao dio ovog koncepta, zasniva se na modelima koji procjenjuju vjerovatnoću pojave kriminalnih aktivnosti u određenom vremenu i prostoru. Takvi sistemi omogućavaju policiji proaktivno raspoređivanje resursa i brže reagiranje na potencijalne prijetnje. Međutim, brojna istraživanja upozoravaju da prediktivni modeli mogu reprodukovati postojeće društvene nejednakosti ukoliko se treniraju na historijskim podacima koji već sadrže sistemske pristrasnosti (Richardson et al., 2019; Ensign et al., 2018).

3. PRIMJENA UMJETNE INTELIGENCIJE U POLICIJSKOM RADU

Primjena umjetne inteligencije u policijskim agencijama obuhvata širok spektar operativnih i analitičkih aktivnosti, od strateškog planiranja do podrške u konkretnim istragama. AI sistemi omogućavaju integraciju i obradu velikih količina podataka iz različitih izvora, čime se unapređuje situacijska svijest, ubrzava donošenje odluka i jača preventivna funkcija policije (Europol, 2025; INTERPOL, 2023.). Prediktivno policijsko djelovanje zasniva se na primjeni algoritama strojnog učenja koji analiziraju historijske podatke o

kriminalitetu s ciljem identifikacije obrazaca u vremenu, prostoru i načinu izvršenja krivičnih djela. Ovi modeli mogu ukazivati na povećani rizik kriminalnih aktivnosti u određenim područjima ili periodima, omogućavajući policiji da preventivno usmjeri svoje resurse (Lum & Isaac, 2016). Analiza kriminalnih obrazaca uključuje faktore poput vrste krivičnih djela, lokacija, vremena izvršenja i prethodnih incidenata, a u naprednijim sistemima i socioekonomske pokazatelje ili podatke o mobilnosti stanovništva. Takav pristup omogućava dublje razumijevanje dinamike kriminaliteta i podržava strateško planiranje sigurnosnih politika (U.S. Department of Justice, 2024). Jedna od ključnih prednosti prediktivnih modela je mogućnost proaktivnog djelovanja, odnosno usmjeravanja patrola i preventivnih aktivnosti u zone povećanog rizika prije nego što dođe do izvršenja krivičnih djela. Time se policijska djelatnost pomjera sa reaktivnog na preventivni pristup, što je u skladu sa savremenim konceptima javne sigurnosti (EUCPN, 2022). Međutim, istraživanja upozoravaju da prediktivni sistemi mogu reproducirati postojeće društvene pristrasnosti ukoliko se oslanjaju na historijske podatke koji odražavaju selektivne policijske prakse iz prošlosti. To može dovesti do tzv. „feedback loop“ efekta, gdje se ista područja stalno označavaju kao rizična, čime se dodatno povećava nadzor nad određenim zajednicama (Ensign et al., 2018; Richardson et al., 2019). Zbog toga se naglašava potreba za stalnom evaluacijom algoritama i ljudskim nadzorom nad njihovim preporukama. Deep learning tehnologije omogućile su značajan napredak u automatskoj analizi video-zapisa i biometrijskoj identifikaciji osoba. Sistemi za prepoznavanje lica koriste neuronske mreže za poređenje snimaka s bazama podataka osumnjičenih ili traženih osoba, čime se ubrzava identifikacija u istragama i potragama (EDPB, 2023). Ovakvi sistemi mogu biti korisni u otkrivanju počinitelja teških krivičnih djela, pronalasku nestalih osoba i identifikaciji osumnjičenih na javnim mjestima. Ipak, zbog visokog rizika od grešaka i mogućih povreda privatnosti, njihova upotreba u realnom vremenu podliježe strogim zakonskim ograničenjima u većini evropskih zemalja (European Union, 2024). Deel learning tehnologija se oslanja i na prediktivno policijsko djelovanje koje se koristi za prevenciju provala u stambene objekte i krađa automobila. U ovom području Nizozemska se često smatra pionirskom državom, jer je prva zemlja u svijetu koja je primijenila koncept prediktivnog policijskog djelovanja na nacionalnom nivou (Strikwerda, 2020). Njihov sistem za predviđanje kriminaliteta, poznat kao Crime Anticipation System (CAS), prvobitno je bio usmjeren na takozvana *krivična djela visokog uticaja*, odnosno provale u stanove i kuće, razbojništva i napade radi otuđenja imovine (Hardyns & Rummens, 2018). Međutim, vremenom je sistem proširen i na druge oblike kriminaliteta, uključujući džeparenje, provale u automobile, nasilna krivična djela, provale u poslovne objekte, kao i krađe bicikala. CAS funkcioniše tako što kombinuje demografske i socioekonomske podatke prikupljene iz tri osnovna izvora. To su Centralna baza podataka o kriminalitetu, općinske administrativne evidencije i Centralni zavod za statistiku Nizozemske. Prikupljeni podaci se zatim vizualiziraju u obliku takozvanih *toplotnih mapa* koje prikazuju područja s povećanim rizikom od kriminaliteta. Na osnovu tih mapa policija planira i usmjerava svoje operativne aktivnosti i intervencije. AI potpomognuti sistemi video-nadzora koriste se i za praćenje gužvi, detekciju neuobičajenog ponašanja i ranu identifikaciju potencijalnih sigurnosnih incidenata tokom sportskih, kulturnih i političkih okupljanja. Analiza kretanja mase i obrazaca ponašanja omogućava policiji da pravovremeno reagira na moguće stampede, sukobe ili druge oblike ugrožavanja javnog reda (INTERPOL,

2023.). Ovakvi sistemi doprinose boljem upravljanju javnim prostorima, ali zahtijevaju jasne protokole o prikupljanju, čuvanju i obradi podataka, kako bi se spriječilo masovno i neselektivno praćenje građana (Council of Europe, 2021). Mobilni telefoni predstavljaju ključni izvor digitalnih dokaza u savremenim kriminalističkim istragama. AI alati se koriste za automatsku klasifikaciju podataka, prepoznavanje obrazaca komunikacije, identifikaciju lokacijskih podataka i rekonstrukciju vremenskih linija događaja (U.S. Department of Justice, 2024). Primjenom strojnog učenja moguće je brzo pretraživati velike količine poruka, fotografija i aplikacijskih podataka, što značajno smanjuje vrijeme obrade dokaza i omogućava brže povezivanje osumnjičenih s konkretnim krivičnim djelima. Time se povećava efikasnost istraga, posebno u slučajevima organiziranog kriminala i terorizma. Društvene mreže postale su važan izvor informacija za praćenje kriminalnih aktivnosti, radikalizacije i planiranja krivičnih djela. AI sistemi mogu analizirati javno dostupne objave, mreže kontakata i obrasce komunikacije kako bi se identifikovali potencijalni sigurnosni rizici (Europol, 2025). Takva analiza omogućava rano prepoznavanje prijetnji i praćenje kriminalnih mreža, ali istovremeno otvara ozbiljna pitanja vezana za slobodu izražavanja, nadzor i mogućnost pogrešne interpretacije konteksta komunikacije. Zbog toga se naglašava potreba za jasnim zakonskim osnovama i sudskim nadzorom ovakvih aktivnosti (UNESCO, 2021). AI alati se koriste i za optimizaciju rasporeda policijskih patrola na osnovu analize historijskih podataka, saobraćajnih tokova i trenutnih sigurnosnih procjena. Ovakav pristup omogućava efikasnije korištenje ograničenih kadrovskih i materijalnih resursa, posebno u urbanim sredinama s visokim intenzitetom kriminalnih aktivnosti (EUCPN, 2022). Automatsko planiranje smjena i ruta patrola može smanjiti administrativno opterećenje policijskih službenika i povećati njihovu prisutnost na terenu, što pozitivno utiče na percepciju sigurnosti među građanima. Integracijom AI sistema s operativno-komunikacijskim centrima moguće je brže prepoznavanje hitnih situacija i automatsko usmjeravanje najbližih patrola prema mjestu incidenta. Analiza podataka iz sistema za hitne pozive, video-nadzora i senzora omogućava precizniju procjenu prioriteta intervencija (INTERPOL, n.d.). Brži odgovor na incidente ne samo da povećava šanse za sprječavanje daljih posljedica, već i doprinosi većem povjerenju javnosti u efikasnost policije. Ipak, pouzdanost ovakvih sistema zavisi od kvaliteta infrastrukture i interoperabilnosti baza podataka, što predstavlja poseban izazov za zemlje s fragmentiranim institucionalnim strukturama, poput Bosne i Hercegovine (Council of Europe, 2025).

4. PREDNOSTI PRIMJENE UMJETNE INTELIGENCIJE U POLICIJI

Primjena umjetne inteligencije u policijskom radu donosi niz operativnih, organizacijskih i strateških prednosti koje doprinose modernizaciji sigurnosnog sektora. AI sistemi omogućavaju policijskim agencijama da efikasnije odgovore na rastuće sigurnosne izazove, unaprijede kvalitet donošenja odluka i optimiziraju korištenje ograničenih resursa, što je posebno važno u zemljama s ograničenim budžetskim kapacitetima, poput Bosne i Hercegovine (Europol, 2025; OECD, 2019). Jedna od najznačajnijih prednosti primjene AI tehnologija jeste povećanje operativne efikasnosti policijskih službi. Automatizacija analitičkih i administrativnih procesa omogućava bržu obradu informacija, kraće trajanje istraga i efikasnije upravljanje predmetima. AI alati mogu simultano analizirati velike količine podataka iz više izvora, što značajno nadmašuje ljudske kapacitete u pogledu brzine i

obima obrade (U.S. Department of Justice, 2024). Na taj način policijski službenici mogu više vremena posvetiti terenskom radu, interakciji s građanima i preventivnim aktivnostima, dok se rutinski analitički zadaci prepuštaju automatiziranim sistemima. Ovakva preraspodjela rada doprinosi povećanju ukupne produktivnosti policijskih agencija (INTERPOL, n.d.). AI sistemi zasnovani na statističkim modelima i strojnome učenju omogućavaju donošenje odluka na temelju objektivnih podataka i unaprijed definiranih kriterija, čime se smanjuje utjecaj subjektivnih procjena i individualnih predrasuda u određenim fazama policijskog rada. Ovo je posebno važno u procesima procjene rizika, određivanja prioriteta intervencija i alokacije resursa (NIST, 2023). Iako se konačne odluke i dalje trebaju donositi uz ljudski nadzor, upotreba algoritamskih preporuka može doprinijeti većoj konzistentnosti i transparentnosti procedura. Međutim, važno je naglasiti da smanjenje subjektivnosti zavisi od kvaliteta podataka i dizajna algoritama, te da AI ne može u potpunosti eliminirati rizik od pristrasnosti ukoliko su ulazni podaci već opterećeni sistemskim nejednakostima (Richardson et al., 2019).Savremeni kriminalistički slučajevi često uključuju velike količine digitalnih dokaza, poput komunikacijskih zapisa, video-materijala i podataka s mobilnih uređaja. AI alati omogućavaju automatsko sortiranje, pretraživanje i povezivanje ovih informacija, čime se značajno skraćuje vrijeme potrebno za analizu i rekonstrukciju događaja (U.S. Department of Justice, 2024). Brža obrada podataka omogućava i pravovremeno reagiranje na sigurnosne prijetnje, što je ključno u slučajevima terorizma, nasilnog ekstremizma i organiziranog kriminala. Time se povećava vjerovatnoća sprječavanja daljih krivičnih djela i smanjuju potencijalne štete po javnu sigurnost (Europol, 2025). Uvođenje AI tehnologija omogućava racionalnije upravljanje ljudskim resursima unutar policijskih organizacija. Analiza podataka o kriminalitetu, saobraćaju i hitnim pozivima omogućava preciznije planiranje smjena, rasporeda patrola i specijaliziranih timova, čime se smanjuje nepotrebno rasipanje kadrovskih kapaciteta (EUCPN, 2022). Osim toga, automatizacija rutinskih poslova smanjuje administrativno opterećenje policijskih službenika i omogućava njihovu specijalizaciju u složenijim operativnim i istražnim zadacima. Dugoročno gledano, ovakav pristup može doprinijeti većem profesionalizmu policije, smanjenju sindroma sagorijevanja zaposlenih i boljoj kvaliteti usluge prema građanima (INTERPOL, n.d.). U kontekstu Bosne i Hercegovine, gdje su policijske strukture institucionalno fragmentirane i često suočene s nedostatkom stručnog IT kadra, ciljane AI aplikacije mogu predstavljati značajan alat za unapređenje koordinacije i efikasnosti, pod uslovom da se paralelno ulaže u edukaciju i jačanje tehničke infrastrukture (Council of Europe, n.d.).

5. RIZICI, ETIČKA I PRAVNA PITANJA U PRIMJENI UMJETNE INTELIGENCIJE U POLICIJI

Jedan od najvećih etičkih rizika primjene AI u policiji odnosi se na mogućnost masovnog nadzora građana, posebno kroz kombinaciju video-nadzora, biometrijskih tehnologija i analitike velikih podataka. Sistemi za prepoznavanje lica i praćenje kretanja mogu omogućiti kontinuirano praćenje pojedinaca u javnom prostoru, što može dovesti do ozbiljnog narušavanja prava na privatnost i slobodu kretanja (Council of Europe, 2021). Masovni nadzor može imati i tzv. „hladeći efekat“ (chilling effect) na demokratsko društvo, jer građani mogu izbjegavati javna okupljanja i izražavanje mišljenja iz straha od praćenja. Zbog toga se u evropskom pravnom okviru insistira na principima nužnosti,

proporcionalnosti i zakonitosti pri korištenju nadzornih tehnologija u policijskom radu (EDPB, 2023). U Evropskoj uniji zaštita osobnih podataka regulisana je Općom uredbom o zaštiti podataka (GDPR), koja propisuje stroge uslove za obradu osjetljivih i biometrijskih podataka, uključujući obavezu jasne pravne osnove, minimizaciju podataka i ograničenje svrhe obrade. Iako Bosna i Hercegovina nije članica EU, njen zakonodavni okvir u oblasti zaštite osobnih podataka u velikoj mjeri je usklađen s evropskim standardima, kroz Zakon o zaštiti osobnih podataka BiH i nadležnost Agencije za zaštitu osobnih podataka (Council of Europe, n.d.; Agencija za zaštitu osobnih podataka BiH, n.d.). Primjena AI sistema u policiji stoga mora biti u skladu s domaćim zakonodavstvom, uz jasno definisane procedure za prikupljanje, pohranu i obradu podataka, kao i mehanizme nezavisnog nadzora. U suprotnom, postoji rizik od nezakonite obrade podataka i povrede osnovnih prava građana (European Union, 2024). Algoritmi strojnog učenja treniraju se na historijskim podacima koji često odražavaju postojeće društvene nejednakosti i pristrasnosti u policijskim praksama. Ako su određene društvene ili etničke grupe bile češće predmet policijskih intervencija u prošlosti, algoritam može takve obrasce „naučiti“ i reproducirati u budućim preporukama, čime se povećava rizik diskriminacije (Lum & Isaac, 2016; Richardson et al., 2019). Ovakva situacija može dovesti do etničkog ili socijalnog profiliranja, gdje se pojedine zajednice nesrazmjerno često označavaju kao rizične, što dodatno narušava povjerenje građana u policiju i pravosudni sistem. Evropske i međunarodne institucije stoga naglašavaju potrebu za redovnim testiranjem algoritama na pristrasnost, transparentnost kriterija odlučivanja i uključivanje etičkih procjena prije uvođenja AI sistema u operativnu upotrebu (Europol, 2025; UNESCO, 2021). Mnogi napredni AI sistemi, posebno oni zasnovani na dubokom učenju, funkcionišu kao tzv. „black box“ modeli, čiji proces donošenja odluka nije lako razumljiv ni korisnicima ni nadzornim institucijama. Nedostatak objašnjivosti algoritama otežava provjeru zakonitosti i ispravnosti odluka koje utiču na prava građana, poput označavanja osoba kao rizičnih ili prioritetnih za policijsko postupanje (NIST, 2023). U policijskom kontekstu, gdje odluke mogu imati ozbiljne posljedice po slobodu i sigurnost pojedinca, nedostatak transparentnosti predstavlja značajan problem za ostvarivanje prava na pravičan postupak i pravni lijek. Zbog toga se sve više insistira na razvoju tzv. „objašnjive umjetne inteligencije“ (explainable AI), koja omogućava uvid u ključne faktore koji utiču na algoritamske preporuke (OECD, 2019).

Pitanje odgovornosti predstavlja jedno od najkompleksnijih pravnih pitanja u vezi s primjenom AI u policiji. U slučaju pogrešne identifikacije, nezakonite obrade podataka ili diskriminatornih odluka, postavlja se pitanje da li je odgovorna policijska institucija, proizvođač softvera ili pojedinac koji je koristio sistem (European Union, 2024). Evropski regulatorni okvir polazi od principa da krajnju odgovornost uvijek snosi institucija koja koristi AI sistem, te da tehnologija ne može biti izgovor za kršenje zakona ili ljudskih prava. To podrazumijeva obavezu policijskih agencija da osiguraju adekvatnu obuku zaposlenih, jasne procedure korištenja AI alata i mehanizme interne i eksterne kontrole (EDPB, 2023; Europol, 2025). U kontekstu Bosne i Hercegovine, dodatni izazov predstavlja složena institucionalna struktura i podijeljene nadležnosti policijskih agencija, što može otežati utvrđivanje odgovornosti u slučaju zloupotrebe ili tehničkih grešaka sistema. Stoga je neophodno uspostaviti jasne protokole odgovornosti i koordinacije među institucijama prije šire implementacije AI tehnologija u policijskom radu (Council of Europe, 2025).

6. NORMATIVNI I INSTITUCIONALNI OKVIR U BOSNI I HERCEGOVINI

Primjena umjetne inteligencije u policijskom radu u Bosni i Hercegovini mora se posmatrati u kontekstu složene ustavne strukture države, podijeljenih nadležnosti između entiteta, kantona i Brčko distrikta, te fragmentiranog policijskog sistema. Ovakva struktura značajno utiče na mogućnosti jedinstvene strategije digitalne transformacije sigurnosnog sektora i zahtijeva visok nivo međuinstitucionalne koordinacije (Council of Europe, n.d.). U tom okviru, normativni i institucionalni kapaciteti predstavljaju ključne faktore za zakonitu, etičku i efikasnu primjenu AI tehnologija u policiji. Zaštita osobnih podataka predstavlja temeljni pravni uslov za primjenu AI sistema koji obrađuju velike količine informacija o građanima. U Bosni i Hercegovini ova oblast regulisana je Zakonom o zaštiti osobnih podataka, koji je u značajnoj mjeri usklađen s evropskim standardima i principima iz GDPR-a, uključujući zakonitost obrade, ograničenje svrhe, minimizaciju podataka i prava ispitanika (Agencija za zaštitu osobnih podataka BiH, 2025). Primjena AI u policiji, posebno u oblastima biometrijske identifikacije, video-nadzora i analize digitalnih tragova, podrazumijeva obradu osjetljivih podataka, što zahtijeva postojanje jasne zakonske osnove i proporcionalnosti mjera. Policijske agencije su obavezne provoditi procjene utjecaja na zaštitu podataka (DPIA) prije uvođenja visokorizičnih sistema, te osigurati mehanizme nadzora i žalbe za građane (EDPB, 2023). U suprotnom, postoji visok rizik od povrede prava na privatnost i nezakonite obrade podataka. Krivično-pravni okvir u Bosni i Hercegovini uređen je kroz Krivični zakon BiH, kao i entitetske i kantonalne krivične zakone, koji definišu ovlasti policije u provođenju istraga, prikupljanju dokaza i primjeni posebnih istražnih radnji. Upotreba AI tehnologija mora biti u skladu s ovim propisima, posebno u dijelu koji se odnosi na nadzor komunikacija, praćenje osoba i prikupljanje digitalnih dokaza, gdje je u većini slučajeva potrebna sudska naredba (Council of Europe, 2025). Uvođenje automatiziranih analitičkih sistema ne smije zaobići zakonske garancije prava na pravičan postupak, presumpciju nevinosti i proporcionalnost policijskih mjera. Evropski regulatorni okvir, uključujući AI Act, dodatno naglašava da se AI sistemi u policiji smatraju visokorizičnim, te da njihova upotreba mora biti strogo kontrolisana i dokumentovana (European Union, 2024). Iako AI Act formalno ne važi u BiH, njegovi standardi predstavljaju relevantan referentni okvir za buduće zakonodavne reforme. Efikasna primjena AI sistema zahtijeva razvijenu digitalnu infrastrukturu, uključujući interoperabilne baze podataka, sigurne mrežne sisteme, savremene servere i softverske platforme za analitiku podataka. U Bosni i Hercegovini, nivo digitalizacije policijskih agencija značajno varira između različitih administrativnih jedinica, što otežava razmjenu podataka i zajedničko korištenje naprednih analitičkih alata (Council of Europe, 2025). Nedostatak jedinstvenih informacionih sistema i standardiziranih procedura predstavlja ozbiljnu prepreku za implementaciju kompleksnih AI rješenja, posebno onih koja se oslanjaju na integraciju podataka iz više izvora. Bez ulaganja u osnovnu digitalnu infrastrukturu, primjena AI tehnologija ostaje ograničena na pilot-projekte i izolirane inicijative (Europol, 2025). Pored tehničke opreme, ključni faktor uspješne primjene AI u policiji predstavlja stručnost i digitalna pismenost policijskih službenika. Korištenje naprednih analitičkih alata zahtijeva specijalizirane vještine iz oblasti informacionih tehnologija, statistike i digitalne forenzike, koje trenutno nisu ravnomjerno zastupljene u policijskim strukturama BiH (INTERPOL, 2023). Nedostatak kontinuirane

stručne obuke može dovesti do pogrešne interpretacije algoritamskih preporuka i prevelikog oslanjanja na tehnologiju, bez kritičke procjene rezultata. Zbog toga međunarodne organizacije preporučuju da se implementacija AI sistema mora pratiti sistematskim programima edukacije i jačanja kapaciteta zaposlenih (UNESCO, 2021). Implementacija AI tehnologija zahtijeva značajna finansijska ulaganja u softver, hardver, održavanje sistema i obuku kadra. U uslovima ograničenih budžeta i konkurentnih javnih potreba, policijske agencije u Bosni i Hercegovini često nemaju dovoljno sredstava za dugoročna tehnološka ulaganja (Council of Europe, 2025.). Zbog toga se kao realna opcija nameće fazni pristup uvođenju AI sistema, kroz pilot-projekte i korištenje međunarodnih fondova i donatorskih programa, posebno onih koje finansira Evropska unija. Međunarodna saradnja može igrati važnu ulogu u transferu znanja i tehnologija, ali dugoročna održivost sistema zavisi od sposobnosti domaćih institucija da osiguraju stabilno finansiranje i institucionalnu podršku (Europol, 2025).

7. MOGUĆNOSTI IMPLEMENTACIJE UMJETNE INTELIGENCIJE U POLICIJSKIM AGENCIJAMA BOSNE I HERCEGOVINE

Iako se Bosna i Hercegovina suočava s nizom institucionalnih i finansijskih ograničenja, postoje realne mogućnosti za postepenu i odgovornu implementaciju umjetne inteligencije u policijskom radu. Umjesto naglih i skupih sistemskih promjena, preporučuje se fazni pristup koji omogućava testiranje tehnologija, procjenu rizika i prilagođavanje lokalnom pravnom i organizacijskom kontekstu (Europol, 2025; INTERPOL, 2023). Takav pristup smanjuje vjerovatnoću neuspjeha i povećava prihvatanje tehnologije među policijskim službenicima i javnošću. Pilot-projekti predstavljaju početni i ključni korak u implementaciji AI sistema u policijskim agencijama. Njihova svrha je testiranje konkretnih aplikacija, poput analize kriminalnih obrazaca, digitalne forenzike ili optimizacije patrola, u ograničenom operativnom okruženju. Ovakvi projekti omogućavaju identifikaciju tehničkih problema, procjenu kompatibilnosti s postojećim informacionim sistemima i analizu organizacijskih izazova prije šire primjene tehnologije (NIST, 2023). Za Bosnu i Hercegovinu, pilot-projekti su posebno pogodni jer omogućavaju racionalno korištenje ograničenih resursa i izbjegavanje skupih investicija bez prethodne provjere koristi. Također, rezultati pilot-faza mogu poslužiti kao osnova za izradu nacionalnih ili entitetskih strategija digitalne transformacije policije (Council of Europe, 2025). Prije i tokom implementacije AI sistema neophodno je provoditi sistematske procjene rizika koje obuhvataju pravne, etičke i tehničke aspekte. To uključuje procjene utjecaja na zaštitu osobnih podataka (DPIA), analizu mogućih diskriminatornih efekata algoritama i procjenu cyber-sigurnosnih prijetnji (EDPB, 2023; UNESCO, 2021). Procjena rizika omogućava identifikaciju potencijalnih negativnih posljedica po prava građana i institucionalni integritet, te pomaže u definiranju zaštitnih mjera prije pune operativne upotrebe sistema. U kontekstu BiH, gdje su nadzorne institucije često kadrovski i tehnički ograničene, ovakve procjene imaju dodatni značaj za očuvanje zakonitosti i povjerenja javnosti. Nakon implementacije pilot-projekata i inicijalnih faza korištenja AI sistema, neophodno je provoditi redovne evaluacije njihove efikasnosti, zakonitosti i društvenih efekata. Evaluacija treba obuhvatiti operativne pokazatelje (smanjenje vremena istrage, povećanje rasvijetljenosti krivičnih djela), ali i utjecaj na prava građana i percepciju javnosti (OECD, 2019). Transparentno izvještavanje o rezultatima

primjene AI tehnologija može doprinijeti jačanju povjerenja javnosti i omogućiti korekcije sistema prije njihove šire institucionalne primjene. Bez ovakvih evaluacijskih mehanizama, postoji rizik da se tehnologije koriste bez jasnih dokaza o njihovoj stvarnoj korisnosti (Europol, 2025). Osnovni preduslov za uspješnu primjenu AI u policijskom radu jeste adekvatna digitalna pismenost policijskih službenika. To podrazumijeva razumijevanje osnovnih principa funkcionisanja informacionih sistema, upravljanja podacima i cyber-sigurnosti, kao i sposobnost kritičkog tumačenja algoritamskih preporuka (INTERPOL, 2023). Bez osnovnog nivoa digitalnih kompetencija, postoji opasnost od nekritičkog oslanjanja na tehnologiju ili pogrešne interpretacije rezultata analize, što može dovesti do operativnih grešaka i pravnih problema. Stoga se preporučuje uključivanje digitalnih vještina u redovne programe policijskog obrazovanja i stručnog usavršavanja (UNESCO, 2021). Pored opće digitalne pismenosti, neophodno je razvijati i specijalizirane profile unutar policijskih struktura, poput analitičara podataka, digitalnih forenzičara i IT sigurnosnih stručnjaka. Ovi kadrovi imaju ključnu ulogu u održavanju AI sistema, evaluaciji algoritama i saradnji s vanjskim tehnološkim partnerima (NIST, 2023). U BiH, gdje već postoji deficit IT stručnjaka u javnom sektoru, potrebno je razvijati stimulativne programe zapošljavanja i zadržavanja stručnog kadra, kao i saradnju s univerzitetima i istraživačkim institucijama. Time bi se osigurao dugoročni kapacitet za održivu primjenu naprednih tehnologija u policijskom radu (Europol, 2025). Evropska unija kroz različite fondove i programe, poput IPA fondova, Horizon Europe i Digital Europe, pruža finansijsku i tehničku podršku projektima digitalne transformacije javnog sektora, uključujući sigurnosne institucije. Iako BiH nema puni pristup svim programima, kroz pretpristupne mehanizme moguće je finansirati pilot-projekte, obuke i nabavku tehnološke opreme (European Commission, 2025.). Učešće u međunarodnim projektima omogućava ne samo pristup finansijskim sredstvima, već i prijenos znanja, standarda i najboljih praksi iz država članica EU, što je ključno za izgradnju održivih kapaciteta u policijskim agencijama BiH. Regionalna saradnja sa zemljama Zapadnog Balkana i šire predstavlja važan mehanizam za razmjenu iskustava u oblasti primjene AI u policijskom radu. Zajedničke obuke, regionalni projekti i razmjena operativnih podataka mogu doprinijeti boljoj borbi protiv transnacionalnog kriminala i harmonizaciji procedura (INTERPOL, 2023.; Europol, 2025). S obzirom na slične institucionalne izazove i sigurnosne prijetnje u regiji, regionalna saradnja omogućava efikasnije korištenje resursa i razvoj zajedničkih standarda odgovorne upotrebe AI tehnologija, uz poštivanje ljudskih prava i vladavine prava.

8. STVARNE POTREBE ZA AI U BIH

Primjena umjetne inteligencije u policijskom radu predstavlja kompleksan proces koji zahtijeva pažljivo usklađivanje tehnoloških mogućnosti sa zaštitom temeljnih ljudskih prava, realnim institucionalnim kapacitetima i očekivanjima građana. Iako AI nudi značajne potencijale za unapređenje sigurnosti, njena nekritička ili neregulisana upotreba može dovesti do ozbiljnih društvenih i pravnih posljedica (UNESCO, 2021; European Union, 2024). Jedno od ključnih pitanja u raspravi o primjeni AI u policiji jeste kako postići ravnotežu između potrebe za efikasnom zaštitom javne sigurnosti i obaveze poštivanja ljudskih prava, posebno prava na privatnost, nediskriminaciju i pravičan postupak. Tehnologije poput biometrijskog nadzora i prediktivnog policijskog djelovanja mogu značajno doprinijeti prevenciji kriminala,

ali istovremeno nose rizik prekomjernog nadzora i stigmatizacije određenih društvenih grupa (Council of Europe, 2021; EDPB, 2023). Evropski regulatorni okvir, uključujući AI Act, jasno naglašava da se sistemi umjetne inteligencije u policiji smatraju visokorizičnim i da njihova upotreba mora biti ograničena na strogo definirane situacije uz sudski i institucionalni nadzor (European Union, 2024). Ovakav pristup potvrđuje da sigurnost ne smije biti ostvarena po cijenu temeljnih prava, već da se tehnologija mora koristiti kao podrška zakonitom i proporcionalnom policijskom djelovanju, a ne kao zamjena za pravne procedure i profesionalnu procjenu policijskih službenika. U poređenju sa razvijenim državama Evropske unije i Sjedinjenih Američkih Država, Bosna i Hercegovina ima znatno ograničenije tehničke, finansijske i kadrovske kapacitete za implementaciju kompleksnih AI sistema u policijskom radu. Fragmentirana institucionalna struktura, nedovoljna interoperabilnost baza podataka i neujednačen nivo digitalizacije među policijskim agencijama dodatno otežavaju uvođenje naprednih tehnologija (Council of Europe, 2025). Dok razvijene zemlje raspolažu posebnim istraživačkim centrima, stabilnim budžetima i dugoročnim strategijama digitalne sigurnosti, BiH se uglavnom oslanja na projektno finansiranje i međunarodnu tehničku pomoć. To ukazuje da realna strategija za BiH ne treba biti masovna i skupa implementacija sofisticiranih sistema, već selektivna primjena AI alata u oblastima gdje se mogu ostvariti najveće koristi uz relativno niske troškove, poput digitalne forenzike i analitike kriminalnih podataka (Europol, 2025; INTERPOL, 2023). U tom smislu, fazni pristup, pilot-projekti i regionalna saradnja predstavljaju realističniji i održiviji model digitalne transformacije policije u BiH u odnosu na direktno preuzimanje rješenja iz tehnološki naprednijih država. Povjerenje građana u policiju predstavlja ključni faktor uspješnosti sistema javne sigurnosti. AI tehnologije mogu potencijalno doprinijeti povećanju tog povjerenja ukoliko rezultiraju bržim rješavanjem slučajeva, smanjenjem kriminaliteta i većom transparentnošću policijskog rada (OECD, 2019). Na primjer, efikasnije upravljanje incidentima i brža identifikacija počinitelja mogu poboljšati percepciju profesionalnosti i kompetentnosti policijskih službi. Međutim, suprotan efekat može nastati ukoliko građani dožive AI kao sredstvo masovnog nadzora ili diskriminatornog postupanja. Istraživanja pokazuju da percepcija nepravednog ili netransparentnog korištenja tehnologije može značajno narušiti povjerenje u institucije, posebno među društveno osjetljivim grupama (Richardson et al., 2019; Lum & Isaac, 2016). Stoga se može zaključiti da sama tehnologija ne garantuje povećanje povjerenja, već je presudan način na koji se ona implementira. Transparentna komunikacija s javnošću, jasni pravni okviri, nezavisni nadzor i mogućnost pravne zaštite građana predstavljaju ključne faktore koji određuju da li će primjena AI biti percipirana kao unapređenje sigurnosti ili kao prijetnja osnovnim slobodama (UNESCO, 2021; Europol, 2025). U kontekstu BiH, gdje je povjerenje u institucije već osjetljivo pitanje, odgovorna i ograničena primjena AI uz aktivno uključivanje javnosti može imati veći pozitivan učinak od brzog i netransparentnog uvođenja naprednih nadzornih tehnologija.

9. ZAKLJUČAK

Ovaj rad je pokazao da umjetna inteligencija predstavlja sve značajniji alat u savremenom policijskom radu, s potencijalom da unaprijedi analizu kriminalnih obrazaca, digitalnu forenziku, upravljanje resursima i preventivne aktivnosti. Primjene AI u oblastima prediktivnog policijskog djelovanja, video-nadzora, analize digitalnih dokaza i operativnog planiranja mogu doprinijeti većoj efikasnosti i bržem odgovoru na sigurnosne prijetnje, posebno u kontekstu rastućeg kibernetičkog kriminala, organiziranog kriminala i terorizma (Europol, 2025; INTERPOL, 2023.; U.S. Department of Justice, 2024). Istovremeno, analiza je ukazala na ozbiljne etičke i pravne rizike povezane s primjenom AI tehnologija, naročito u pogledu zaštite privatnosti, mogućnosti masovnog nadzora, algoritamske pristrasnosti i problema transparentnosti odlučivanja. Evropski i međunarodni standardi jasno naglašavaju da se AI u policijskom radu mora koristiti uz strogo poštivanje principa zakonitosti, proporcionalnosti i odgovornosti, uz obavezan institucionalni i sudski nadzor (European Union, 2024; UNESCO, 2021; EDPB, 2023). U kontekstu Bosne i Hercegovine, utvrđeno je da normativni okvir pruža osnovu za zaštitu osobnih podataka i zakonito postupanje policije, ali da institucionalni kapaciteti, tehnička infrastruktura i digitalne kompetencije kadra predstavljaju značajne prepreke za širu i kompleksniju primjenu AI sistema (Council of Europe, 2025; Agencija za zaštitu osobnih podataka BiH, 2025). Cilj rada bio je analizirati mogućnosti i ograničenja primjene umjetne inteligencije u policijskom radu, s posebnim naglaskom na pravni i institucionalni kontekst Bosne i Hercegovine. Kroz pregled osnovnih AI tehnologija, analiza konkretnih primjena u policiji, razmatranje etičkih i pravnih pitanja te procjenu institucionalne spremnosti, rad je dao sveobuhvatan uvid u složenost ovog procesa. Na osnovu rezultata analize, može se preporučiti nekoliko smjernica za budući razvoj politika i istraživanja u oblasti primjene AI u policijskom radu u Bosni i Hercegovini. Prije svega, potrebno je razviti jasne strateške dokumente na državnom i entitetskim nivoima koji će definirati prioritete digitalne transformacije policije, uz precizno određene pravne i etičke okvire za korištenje AI tehnologija. Daljnja istraživanja trebala bi se fokusirati na empirijsku procjenu efekata pilot-projekata AI sistema u policiji, uključujući njihovu stvarnu efikasnost, utjecaj na smanjenje kriminaliteta i percepciju javnosti. Posebno je važno ispitati kako različite zajednice doživljavaju primjenu nadzornih tehnologija i da li takve prakse utiču na povjerenje u policiju i institucije vlasti. Na nivou politika, preporučuje se jačanje saradnje s međunarodnim organizacijama i institucijama Evropske unije, korištenje dostupnih fondova za izgradnju tehničkih kapaciteta i ulaganje u kontinuiranu edukaciju policijskih službenika. Paralelno s tim, neophodno je osnažiti nadzorne mehanizme, uključujući nezavisne regulatorne institucije i sudski nadzor, kako bi se osigurala odgovorna i transparentna upotreba umjetne inteligencije u policijskom radu. Na taj način, Bosna i Hercegovina može postepeno razvijati moderan i tehnološki osnažen policijski sistem koji doprinosi javnoj sigurnosti, ali istovremeno poštuje temeljna prava i slobode građana.

10. LITERATURA

1. Agencija za zaštitu osobnih podataka Bosne i Hercegovine. (2025). *Publikacije i smjernice.* https://www.azlp.ba/GDPR_Menu/Smjernice/default.aspx?id=3393&langTag=bs-BA&template_id=149&pageIndex=1
2. CMS Legal. (2025). *Data protection and cybersecurity laws in Bosnia and Herzegovina.* https://cms.law
3. Council of Europe. (2021). *Guidelines on facial recognition.* https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html
4. Council of Europe. (n.d.). *Data protection in Bosnia and Herzegovina.* https://www.coe.int/en/web/data-protection/bosnia-and-herzegovina
5. Ensign, D., Friedler, S. A., Neville, S., Scheidegger, C., & Venkatasubramanian, S. (2018). Runaway feedback loops in predictive policing. In *Proceedings of FAT** 2018 (pp. 160–171). ACM.
6. European Commission. (2025.). *Artificial Intelligence Act: Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
7. European Crime Prevention Network (EUCPN). (2022). *Artificial intelligence and predictive policing: Risks and challenges.* https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf
8. European Data Protection Board. (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (Version 2.0).* https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en
9. European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union. https://eur-lex.europa.eu
10. Europol. (2025). *AI bias in law enforcement: A practical guide.* Europol Innovation Lab. https://www.europol.europa.eu/publications-events/publications/ai-bias-in-law-enforcement
11. Hardyns and Rummens, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, European Journal of Criminal Policy Research (2018) 24:201–218
12. INTERPOL. (2023). *Artificial intelligence toolkit.* https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit
13. Law Commission of Ontario. (2025). *AI in criminal justice project: Paper 2 – Law enforcement use of AI.* https://www.lco-cdo.org/wp-content/uploads/2025/08/LCO-AI-in-Criminal-Justice-Paper-2-Law-Enforcement-Use.pdf
14. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

15. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* https://www.nist.gov/itl/ai-risk-management-framework
16. OECD. (2019). *Recommendation of the Council on artificial intelligence.* https://www.oecd.org/going-digital/ai/principles/
17. Police Foundation (UK). (2025). *Policing and artificial intelligence.* https://www.police-foundation.org.uk/publication/policing-and-artificial-intelligence/
18. Reuters. (2025, February 4). EU lays out guidelines on misuse of AI by employers, websites and police. *Reuters.* https://www.reuters.com/technology/artificial-intelligence/eu-lays-out-guidelines-misuse-ai-by-employers-websites-police-2025-02-04/
19. Strikwerda, L. Predictive Policing: The Risks Associated with Risk Assessment,The Police J ournal 94:3 (2020), 422- 36, https:/ / dx.doi.org/ 10.1177/ 0032258X20947749
20. U.S. Department of Justice, Office of Legal Policy. (2024). *Artificial intelligence and criminal justice: Final report.* https://www.justice.gov/olp/media/1381796/dl
21. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence.* https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

THE ROLE OF ARTIFICIAL INTELLIGENCE (AI) IN POLICE WORK

Summary: *The development of artificial intelligence (AI) has significantly influenced the transformation of modern policing by enabling more efficient analysis of crime patterns, improved preventive activities, and faster processing of digital evidence. The aim of this paper is to analyze the possibilities and limitations of AI application in the police sector, with a particular focus on the legal and institutional framework of Bosnia and Herzegovina. Methodologically, the paper is based on an analysis of relevant scientific literature, international guidelines, and regulatory documents, with a comparative overview of practices in developed countries. The results of the analysis indicate that AI can contribute to increased efficiency of police agencies, better resource management, and enhanced preventive action, especially in the areas of predictive policing, video surveillance, digital forensics, and operational planning. However, significant risks related to privacy protection, algorithmic bias, and the lack of transparency in decision-making processes have also been identified, which requires strict regulation and strong oversight mechanisms. In the context of Bosnia and Herzegovina, additional challenges include a fragmented institutional structure, limited financial resources, and a lack of specialized IT personnel. In conclusion, the paper emphasizes the need for a phased and responsible introduction of AI technologies into policing, accompanied by strengthening the legal framework, institutional capacities, and continuous education of police officers, in order to ensure a balance between improving public security and protecting fundamental human rights.*

Keywords: *artificial intelligence; policing; public security; personal data protection; predictive policing; digital forensics; Bosnia and Herzegovina.*

PROCJENA NIVOA JAVNE SVIJESTI I POZNAVANJA RIZIKA KIBERNETIČKE SIGURNOSTI U SISTEMIMA UPRAVLJANJA I KONTROLE KRITIČNE INFRASTRUKTURE U BOSNI I HERCEGOVINI

dr. sc. Inda Kreso,
indakreso@fkn.unsa.ba

***Sažetak:**: Ovo istraživanje predstavlja prvo empirijsko istraživanje u Bosni i Hercegovini koje analizira nivo javne svijesti, znanja i percepcije rizika kibernetičke sigurnosti u sistemima upravljanja i kontrole kritične infrastrukture (eng. Operation Technology - OT/eng. Industrial Control Systems - ICS). Iako su tehničke i inženjerske mjere zaštite najbitnije i osnovne, ljudski faktor, svijest, povjerenje i percepcija stanovništva ostaje presudan za jačanje otpornosti i zaštitu kritične infrastrukture u Bosni i Hercegovini. Istraživanje je provedeno u periodu od 01.09.2025. godine do 31.10.2025. godine putem online upitnika, te je prikupljeno 206 validnih odgovora. Statistička analiza podataka izvršena je u RStudio i u R programskom jeziku za statističke proračune. Analiza rezultata pokazuje da javnost BiH ispravno percipira ozbiljnost i važnost kibernetičkih prijetnji i da posjeduje relativno dobar nivo općeg znanja o zaštiti kritične infrastrukture. Također, javnost vjeruje u sposobnost CERT BiH tima (koji još uvijek nije u potpunosti funkcionalan), u njihovu spremnost i stručnost, dok nemaju tako veliko povjerenje u institucionalnu zaštitu i spremnost. Većina ispitanih IT stručnjaka koji posluju u domenu kritične infrastrukture vjeruje da su obuke iz kibernetičke sigurnosti veoma korisne, dok sama analiza između percepcije rizika između IT stručnjaka i građana nije pokazala statistički značajnu razliku. Rezultati također upućuju na potrebu za jačanjem edukacije i medijske vidljivosti važnosti kibernetičke zaštite OT/ICS sistema. Navedeni rezultati, kao i sama studija mogu poslužiti kao polazna tačka i osnova za izradu nacionalnih programa obuke i strategija podizanja otpornosti kritične infrastrukture u Bosni i Hercegovini.*

***Ključne riječi:** kibernetička sigurnost, kritična infrastruktura, industrijski kontrolni sistemi, operativna tehnologija, javna svijest, Bosna i Hercegovina.*

1. UVOD

Kritična infrastruktura je gotovo pa potpuno digitalizovana, kako u svijetu, tako sve više i u Bosni i Hercegovini. Uprkos sve većoj digitalizaciji, vrlo često sistemi upravljanja i operativne tehnologije nisu dovoljno zaštićene od kibernetičnih napada koji predstavljaju rastuću prijetnju kritičnoj infrastrukturi. Kako je sigurnost kritične infrastrukture jedan od osnovnih i temeljnih pitanja nacionalne sigurnosti svake države, kibernetička odbrana kritične infrastrukture također predstavlja jednu od najbitnijih strategija. U kritičnu infrastrukturu spadaju: energetski sistemi, finansijski sektor, zdravstveni sistem, javna uprava, telekomunikacije i transport, te svi ostali sektori čiji bi prekid rada ili snabdijevanje mogao imati posljedice po ekonomski, društveni i politički poredak u jednoj državi. U digitalnom dobu u kakvom živimo, to također znači da bi samo jednim klikom napadač

mogao da prekine snabdijevanje osnovnih usluga, ugrozi živote svakog stanovnika, destabilizira društvo i naruši povjerenje u državne institucije. Ulaganja u kibernetičku odbranu i zaštitu kritične infrastrukture u Bosni i Hercegovini je ključno, međutim tehnička rješenja nisu dovoljna bez adekvatnog nivoa ljudske svijesti i edukacije. Upravo je svijest stanovništva o kibernetičkim prijetnjama na kritičnu infrastrukturu ključna u jačanju i poboljšanju otpornosti kompletnog društva. Kao jedan važan dio nacionalne strategije je i obrazovanje stanovništva, kontinuirana obuka zaposlenih u sektorima koji čini kritičnu infrastrukturu, te medijske kampanje o važnosti digitalne sigurnosti kritične infrastrukture. Bitno je naglasiti da kibernetična sigurnost nije samo tehničko pitanje, već i veoma bitno društveno pitanje i ključni nacionalni prioritet. Osnovna meta napada u sistemima kritične infrastrukture su uvijek sistemi upravljanja i kontrole koji se nazivaju operativne tehnologije (eng. Operational Technology) i industrijski kontrolni sistemi (eng. Industrial Control Systems) (Almedires & Almaiah, 2021; Ha et al., 2022). Oni su srce digitalizovanih sistema kritične infrastrukture koji upravljaju i kontrolišu svim operacijama i samim tim predstavljaju najvažniju metu napada kako bi se onesposobili (Simons Markusson, 2023). Istraživanje nivoa svijesti javnosti i poznavanja rizika kiberetičke sigurnosti u sistemima upravljanje i kontrole kritične infrastrukture u Bosni i Hercegovini do sada nije rađeno. Ovo istraživanje je zapravo prvo istraživanje koje sistematično prikuplja podatke vezane za stavove i percepciju bosanskohercegovačke javnosti kada je u pitanju kibernetička sigurnost kritične infrastrukture. Dosadašnja literatura je istraživala sigurnost kritične infrastrukture u Bosni i Hercegovini u nekoliko smjerova. Autori (Smajić & Bajramović, 2023) analiziraju stepen razvijenosti zaštite kritične infrastrukture u Bosni i Hercegovini naglašavajući da Bosna i Hercegovina nema jedinstven institucionalni i zakonodavni okvir koji je ujednačen na državnom nivou. Dalje autori (Smajić & Bajramović, 2023) ističu da složenost političko-administrativne strukture u Bosni i Hercegovini predstavlja osnovnu prepreku uspostavljanju efikasnosti sistema zaštite kritične infrastrukture, posebno u oblasti kibernetičkih prijetnji. Autor (Ermin Solak, 2022) analizira energetski sektor kao jedan od ključnih sektora kritične infrastrukture, naglašavajući da savremeni sigurnosni izazovi kao što su kibernetičke hibridne prijetnje mogu imati posljedice koje obuhvataju ekonomske, političke, infrastrukturne i ekološke faktore, te direktno opstruiraju stabilan i održiv energetski sektor Bosne i Hercegovine. Autori (Ahić & Hodžić, 2025) analiziraju strane uticaje, konkretno uticaj Kine na razvoj i sigurnost kritične infrastrukture u Bosni i Hercegovini i naglašavaju da se u zemljama koje nemaju dovoljno razvijen zakonski i institucionalni okvir, investicije u kritičnu infrastrukturu vrlo često koriste kao instrumenti ekonomskog i političkog uticaja. Autor (Popovski et al., 2023) naglašava da još uvijek sve države Zapadnog Balkana nemaju zakonsku regulativu kojom regulišu kritičnu infrastrukturu, a pogotovo kibernetički aspekt zaštite kritične infrastrukture. Bosna i Hercegovina je upravo jedna od država Zapadnog Balkana koja ne posjeduje navedeni zakon, a upravo je prema autoru (Popovski et al., 2023) zakonska usklađenost ključ jačanja sigurnosti kritične infrastrukture. Dalje, autori (Eva Nagyfejeo & Sarah Puello Alfonso, 2019) u izvještaju pod nazivom: "Cybersecurity Capacity Review Bosnia and Herzegovina" iz 2019. godine ističu da je za Bosnu i Hercegovinu osnovna uspostava nacionalne strategije kibernetičke sigurnosti. Evidentno je da postoji vidljiv nedostatak literature koji se tiče kibernetičke sigurnosti kritične infrastrukture u Bosni i Hercegovini, a posebno empirijskih podataka o stavu, percepciji i znanju stanovništva o

OT/ICS kibernetičkoj zaštiti. Ovo istraživanje je zapravo prvo istraživanje koje direktno adresira kibernetičku sigurnosti operativnih tehnologija i kontrolnih sistema u Bosni i Hercegovini koji su osnovna meta kibernetičkih napada.

2. METODOLOGIJA

Upitnik je proveden u periodu od 01.09.2025. godine do 31.10.2025. godine. Upitnik je distribuiran putem online platformi kao što su društvene mreže (LinkedIn, Facebook) te putem elektronske pošte i akademskih kanala komunikacije. Online anketa je imala cilj procjene nivo javnog znanja, svijesti i percepcije o kibernetičkoj sigurnosti operativnih i industrijskih kontrolnih sistema (OT/ICS) u Bosni i Hercegovini. Prikupljeno je ukupno 206 validnih odgovora, a sam upitnik se sastojao od 46 pitanja koja su bila podijeljena u četiri osnovne tematske oblasti. Prva tematska oblast obuhvata demografske podatke (spol, starosna dob, nivo i oblast obrazovanja, status zaposlenja, sektor i radno iskustvo) kako bi se definisao profil ispitanka. Druga tematska oblast se odnosi **na** profesionalnu povezanost s kritičnom infrastrukturom, odnosno na učešće u projektima vezanim za OT/ICS sigurnosti, pristup i dodir sa operativnim tehnologijama u svakodnenvom poslu, iskustvo sa kibernetičkim incidentima i institucionalne obuke. Treća oblast koju je upitnik obrađivao jeste nivo znanja i svijesti stanovništva o osnovnim i tehničkim konceptima OT/ICS sigurnosti, uključujući pojmove kao što su kritična infrastruktura, SCADA (eng. Supervisory Control and Data Acquisition), OT, IT sigurnost i poznati incidenti (Stuxnet, Triton, itd.). Četvrti dio upitnika jeste percepcija ozbiljnosti kibernetičkih prijetnji, povjerenje u CERT kapacitete, stavove o edukaciji i spremnosti institucija za efikasnu odbranu od kibernetičkih prijetnji. Cilj upitnika je bio i da ispita poznavanje općih pojmova kritične infrastrukture (opće indikatore) i pokazatelje institucionalne i profesionalne spremnosti (specifične pokazatelje). Kako bi upitnik, kao osnovni metodološki instrument ovog istraživanja, bio formiran u skladu sa međunarodnim istraživanjima, te kako bi se omogućilo poređenje rezultata s globalnim trendovima, upitnik je kreiran u skladu sa analizom iz ključnih svjetskih izvještaja ((Jason D. Christopher, 2024; Mark Bristow, 2021). Upitnik proveden u ovom istraživanju predstavlja naučno utemeljenu verziju jednih od najrelevatnijih izvora i okvira za procjenu kibernetičke otpornosti u operativnim tehnologijama i industrijskim kontrolnim sistemima. Svi prikupljeni podaci su analizirani i obrađeni u R studio korištenjem R programskom jezika za statističke proračune.

Ukupno je definisano sedam istraživačkih pitanja:

1. Kako javnost percepira ozbiljnost kibernetičkih prijetnji usmjerenih protiv kritične infrastrukture (OT/ICS)?
2. Koji je nivo javnog znanja i svijesti o konceptima i rizicima OT/ICS kibernetičke sigurnosti?
3. Koji je nivo povjerenja u sposobnosti nacionalnih CERT/CSIRT tijela da spriječe, otkriju i odgovore na OT/ICS kibernetičke prijetnje (uz napomenu da CERT tim u BiH još uvijek nije u potpunosti funkcionalan)?
4. U kojoj mjeri profesionalci koji rade s kritičnom infrastrukturom pohađaju obuke iz kibernetičke sigurnosti i koliko učinkovitim smatraju te obuke?
5. Postoji li statistički značajna razlika u percepciji ozbiljnosti cyber prijetnji između IT stručnjaka i građana u BiH?

6. Kako ispitanici percipiraju ranjivost različitih sektora kritične infrastrukture u Bosni i Hercegovini na kibernetičke napade?
7. Kako stanovništvo u Bosni i Hercegovini percipira zastupljenost tema o OT/ICS kibernetičke sigurnosti i kritičnoj infrastrukturi u domaćim medijima?
Rezultati istraživanja nakon obrade i analize prikupljenih podataka, kao i odgovori na istraživačka pitanja predstavljeni su u dijelu Rezultati.

3. REZULTATI

3.1. Percepcija ozbiljnosti kibernetičkih prijetnji prema kritičnoj infrastrukturi

Prvo istraživačko pitanje koje glasi: "Kako javnost percepira ozbiljnost kibernetičkih prijetnji usmjerenih protiv kritične infrastrukture (OT/ICS)?" odgovoreno je uz upotrebu deskriptivne statističke analize kako bi se pružio uvid u percepciju javnosti o kibernetičkim prijetnjama i napadima na kritičnu infrastrukturu u Bosni i Hercegovini. Rezultati su prikazani u Tabeli 1.

Pitanje	Srednja vrijednost	Medijan	SD	Min	Max
Koliko vjerujete da su kibernetičke prijetnje ozbiljne za nacionalnu sigurnost Bosne i Hercegovine?	4.44	5	0.81	3	5
Da li vjerujete da su kibernetičke prijetnje danas ozbiljnije od fizičkih prijetnji (terorizam, rat)?	3.39	5	1.97	1	5
Kompozitna mjera ozbiljnosti kibernetičkih prijetnji (kombinacija prethodna dva pitanja)	3.92	4.5	1.15	2	5

Tabela 1: Percepcija ozbiljnosti kibernetičkeprijetnji protiv kritične infrastrukture
Izvor 1: Autorska obrada podataka (2025)

Ispitanici smatraju da su kibernetičke prijetnje kritičnoj infrastrukturi u Bosni i Hercegovini veoma ozbiljne, što potvrđuje srednja vrijednost koja iznosi 4.44 koja je izračunata za pitanje "Koliko vjerujete da su kibernetičke prijetnje ozbiljne za nacionalnu sigurnost Bosne i Hercegovine?". Učesnici prepoznaju ozbiljnost potencijalnih kibernetičnih napada, te prepoznaju opasnost i potencijalno kompromitovanje ključnih sistema od nacionalnog značaja kao što su energetika i električna struja, vodosnadbijevanje, telekomunikacije i ostalo. Također, ispitanici vjeruju da su kibernetički rizici rastuća opasnost, no većina i dalje smatra da su konvencionalne fizičke prijetnje kao što su terorizam i rat opasnije po društvo i državu. Navedeno se ogleda u umjereno visokom nivou zabrinosti (Srednja vrijednost = 3,39, SD = 1,97) prilikom odgovora na pitanje "Da li vjerujete da su kibernetičke prijetnje danas ozbiljnije od fizičkih prijetnji (terorizam, rat)?". Kombinovanjem ova dva indikatora u složeni indeks percepcije (M = 3,92, SD = 1,15), rezultati upućuju na visok nivo svijesti i percipiranja ozbiljnosti rizika kibernetičke sigurnosti u industrijskim i operativnim sistemima među javnošću. Javnost u Bosni i Hercegovini sve više prepoznaje rizike od kibernetičkih

prijetnji, te u skladu sa globalnim trendovima bosanskohercegovačko stanovništvo razumije sve veću povezanosti između kibernetičke sigurnosti i nacionalne otpornosti.

3.2. Nivo znanja i svijesti javnosti o OT/ICS kibernetičkoj sigurnosti

Dalje, rezultati analize drugog istraživačko pitanja koje glasi "Koji je nivo javnog znanja i svijesti o konceptima i rizicima OT/ICS kibernetičke sigurnosti?", predstavljeni su u Tabeli 2. Ispitanici imaju relativno dobro poznavanje osnovnih koncepata, kao i zadovoljavajući nivo svijesti o operativnih tehnologijama (OT). Analizirani rezultati ukazuju na nedostatak dovoljnog nivoa znanja o više tehničkim i inženjerskim pitanjima kao što su razliku između IT i OT sigurnosti (M = 3.14), te naročito Purdue model (M = 2.15). Svijest stanovništva je uglavnom fokusirana na opće pojmove.

Istraživačko pitanje / stavka iz ankete	Prosjek	Tumačenje
Da li znate šta je kritična infrastruktura?	3.95	Većina ispitanika je upoznata s pojmom kritične infrastrukture. Opšti nivo svijesti je visok.
Da li znate koji se sektori smatraju dijelom kritične infrastrukture?	4.24	Najviši nivo znanja; ispitanici mogu prepoznati sektore kao što su energetika, vodosnabdijevanje i zdravstvo.
Da li ste čuli za pojam ICS (Industrijski kontrolni sistemi)?	3.43	Umjerena upoznatost sa pojmom, mnogi su čuli za pojam, ali razumijevanje je površno.
Da li ste čuli za pojam OT (Operativna tehnologija)?	3.80	Relativno visok nivo upoznatosti, jer pojam OT postaje sve prepoznatljiviji u javnosti.
Da li znate razliku između IT i OT sigurnosti?	3.14	Nizak nivo razumijevanja ukazuje na nedostatak tehničkog znanja među općom populacijom.
Da li znate šta je SCADA sistem?	3.27	Umjerena svijest vezano za poznavanje SCADA sistema. Ispitanici su uglavnom čuli za pojam, ali nisu upoznati s detaljima.
Da li znate šta predstavlja Purdue model u OT sigurnosti?	2.15	Najniža ocjena; gotovo nepoznat pojam, previše tehnički i specijaliziran za većinu ispitanika.
Da li ste čuli za kibernetičke napade kao što su Stuxnet ili Triton?	3.64	Umjerena upoznatost sa nekim od najpoznatijih kibernetičkih napada na kritičnu infrastrukturu.

Tabela 2: Znanje i svijest ispitanika o OT/ICS konceptima i rizicima u oblasti kibernetičke sigurnosti kritične infrastrukture
Izvor 2: Autorska obrada podataka (2025)

3.3. Povjerenje u sposobnosti nacionalnih CERT/CSIRT timova

Rezultati analize za treće istraživačko pitanje koje glasi **"**Koji je nivo povjerenja u sposobnosti nacionalnih CERT/CSIRT tijela da spriječe, otkriju i odgovore na OT/ICS kibernetičke prijetnje?**",** predstavljeno je u Tabeli 3. Rezultati ukazuju na visok nivo povjerenja u CERT tim koji ima zadatak da spriječi i otkrije kibernetičke prijetnje (M = 4.13, SD = 1.66)**.** Većina ispitanika ima povjerenje u institucionalnu spremnost CERT-a BiH, iako

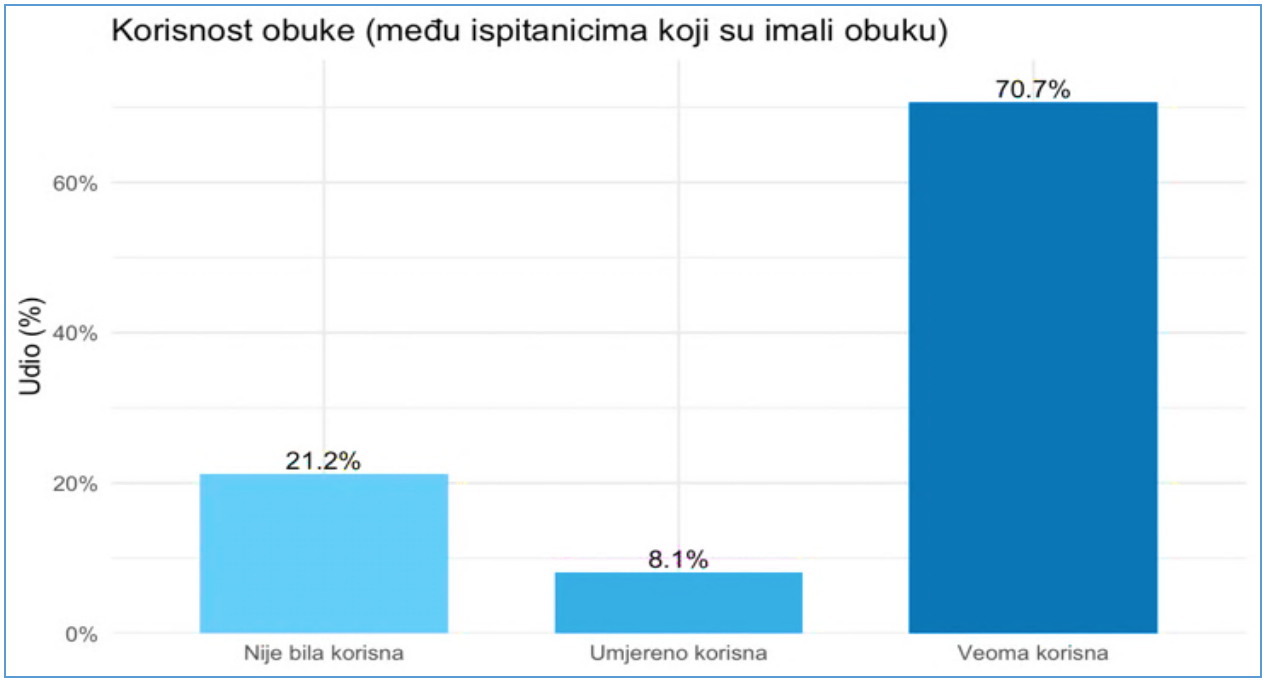
je manji broj učesnika pokazao umjeren ili nizak nivo povjerenja. Iako Bosna i Hercegovina još uvijek nema u potpunosti funkcionalan nacionalni CERT/CSIRT tim, u upitniku je uključena ova kategorija kako bi se procijenila percepcija povjerenja u ideju i ulogu takvog tima**,** odnosno u potencijalnu instituciju koja bi imala mandat da koordinira odgovor na kibernetičke incidente. Stoga se dobiveni rezultati ne odnose na stvarni institucionalni učinak, već na opće povjerenje ispitanika u stručnost i koncept tehničkog autoriteta koji bi CERT/CSIRT tim predstavljao u državnom kontekstu.

Statistička mjera	Opis	Vrijednost
Srednja vrijednost (Mean)	Prosječan nivo povjerenja u sposobnosti nacionalnog CERT/CSIRT tima	4.13
Medijana (Median)	Središnja vrijednost na skali povjerenja od 1 do 5	5.00
Standardna devijacija (SD)	Varijacija u odgovorima koja pokazuje razlike u percipiranom povjerenju	1.66
Minimum (Min)	Najniža prijavljena vrijednost povjerenja	1
Maksimum (Max)	Najviša prijavljena vrijednost povjerenja	5

Tabela 3: Povjerenje u sposobnosti CERT/CSIRT timova
Izvor 3: Autorska obrada podataka (2025)

3.4. Iskustva i percepcija korisnosti obuka iz OT/ICS kibernetičke sigurnosti

Četvrto istraživačko pitanje glasi: "U kojoj mjeri profesionalci koji rade s kritičnom infrastrukturom pohađaju obuke iz kibernetičke sigurnosti i koliko učinkovitim smatraju te obuke?" Ispitanici koji rade u nekom od sektora kritične infrastrukture davali su odgovore vezano za obuke koje su imali u sklopu svog radnog iskustva. Veliki dio ispitanika je naveo da smatraju da su obuke koje su imali bile izuzetno korisne (70,7%), dok 21,2% smatra da obuke nisu bile korisne u njihovom svakodnevnom poslu. Grafički prikaz rezultata odgovora na četvrto istraživačko pitanje, predstavljen je Slikom 1. Navedena analiza upućuje na to da postojeći programi obuka u značajnoj mjeri ispunili očekivanja učesnika i doprinijeli jačanju njihovih kompetencija u oblasti OT/ICS kibernetičke sigurnosti. Navedeni nalazi se poklapaju i sa statistikom u svjetskih istraživanjima. Bitno je naglasiti da su obuke u oblasti kibernetičke sigurnosti u sektorima kritične infrastrukture od ključnog značaja, te da mnogi autori ističu važnost i bitnost kontinurianih edukacija u ovoj oblasti. Naime, autor (Ramezan et al., 2023) navodi da je u sektorima kritične infrastrukture potrebna kombinacija znanja, vještina, certifikacije i iskustva kako bi se kreirao kvalitetan kadar, dok autor (Matthew J. Kirkland et al., 2021) naglašava važnost efikasnih laboratorijskih simulacija u edukativne svrhe. Također izvještaj iz 2019. godine (Eva Nagyfejeo & Sarah Puello Alfonso, 2019) ukazuje da u Bosni i Hercegovini nema institucionalno razvijen okvir za edukacije u oblasti kibernetičke sigurnosti kritične infrastrukture, te je od iznimne važnosti da se kreiraju edukativne politike i program.



Slika 1: Procjena korisnosti obuke iz kibernetičke sigurnosti OT/ICS sistema.
Izvor 4: Autorska obrada podataka (2025)

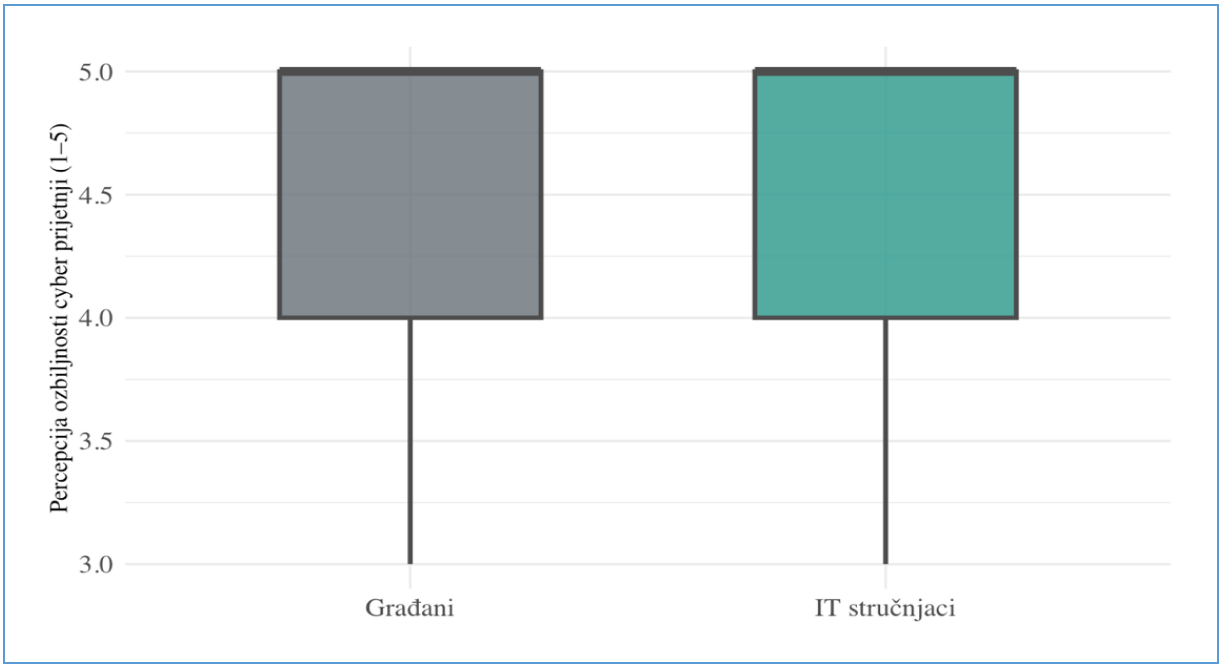
3.5. Poređenje percepcije ozbiljnosti prijetnji između IT stručnjaka i građana

Peto istraživačko pitanje glasi: "Postoji li statistički značajna razlika u percepciji ozbiljnosti kibernetičkih prijetnji između IT stručnjaka i građana u BiH?". Tabela 4 prikazuje deskriptivnu statistiku izvršenu nad prikupljenim podacima.

Grupa	N	Sredina	SD	Medijan
Građani	142	4.47	0.73	5
IT stručnjaci	64	4.56	0.68	5

Tabela 4: Percepcija ozbiljnosti cyber prijetnji: IT stručnjaci naspram građana Izvor 5: Autorska obrada podataka (2025)

Obje grupe ispitanika (i IT stručnjaci i građani) su ostvarili visoke prosječne vrijednosti (M = 4.56 i M = 4.47) i medijan vrijednost koja iznosi 5, što ukazuje da i jedna i druga grupa jednako smatra da su kibernetičke prijetnje na kritičnu infrastrukturu veoma ozbiljne. Pošto je zavisna varijabla izražena ordinalno, uz pomoć Likert skale sa rasponom od 1 do 5, za poređenje ovih grupa korišten je Mann–Whitney U test (W = 5033.5, p = 0.563).

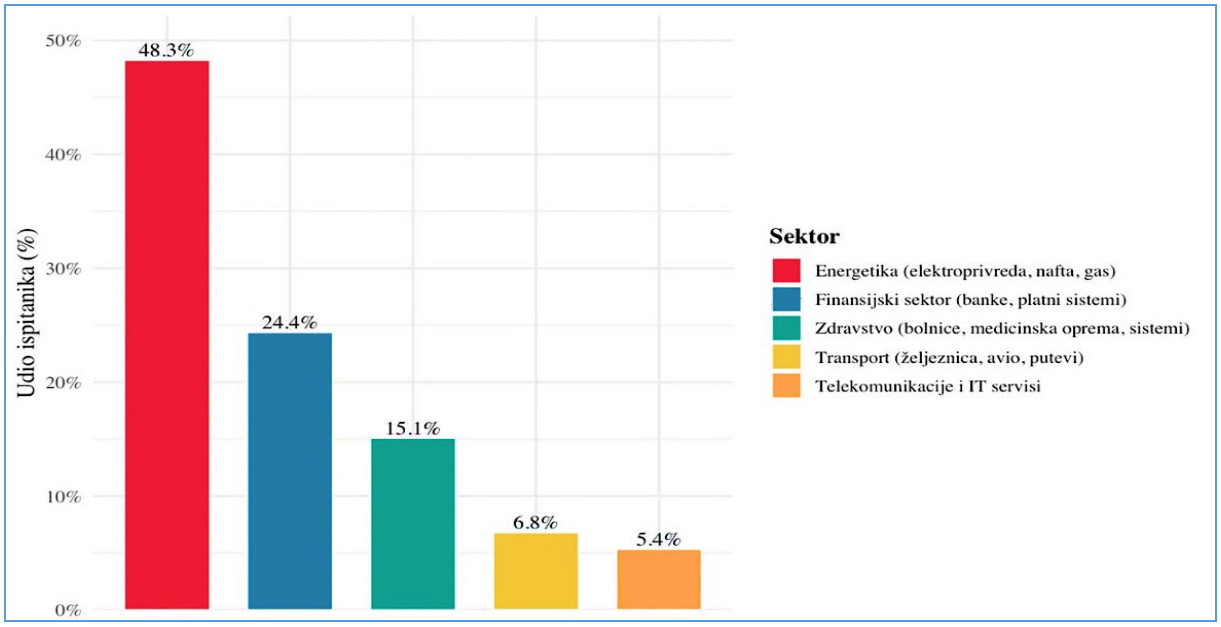


Slika 2: Raspodjela percepcije ozbiljnosti kibernetičkih prijetnji između IT stručnjaka i građana (Likert skala 1–5).
Izvor 6: Autorska obrada podataka (2025)

Navedeni statistički test se koristi kada pretpostavka o normalnoj distribuciji nije zadovoljena, kada su podaci kategorizirani ili imaju ograničen broj vrijednosti. Rezultati testa *(W = 5033.5, p = 0.563)* ukazuju na činjenicu da nema značajnih statističkih razlika između percepcije građana i IT stručnjaka u testnom uzorku. Obje grupe jednako procijenjuju kibernetičke prijetnje na OT/ICS sisteme veoma opasnim i ozbiljnim. Slika 2 prikazuje vizuelni prikaz raspodjele percepcije ozbiljnosti kibernetičkih prijetnji između IT stručnjaka i građana.

3.6. Percepcija ranjivosti sektora kritične infrastrukture

Šesto istraživačko pitanje glasi: "Kako ispitanici percipiraju ranjivost različitih sektora kritične infrastrukture u Bosni i Hercegovini na kibernetičke napade?". Rezultati analize grafički prikazani na Slici 3 pokazuju percepciju ispitanika o tome koji sektor iz domena kritične infrastrukture u Bosni i Hercegovini smatraju najugroženijim i najranjivijim od kibernetičkih napada. Prema odgovorima, 48.3% ispitanika smatra da je najranjiviji energetski sektor. Navedeni rezultat je u skladu sa svjetskim trendovima u kojima se energetska infrastruktura uvijek ističe kao osnovna meta napada kako zbog svoje važnosti, tako i zbog zavisnosti od kompleksnih SCADA/ICS sistema. Sljedeći sektor koji je prepoznat kao izuzetno ranjiv jeste finansijski sektor **(**24.4%**).**



Slika 3: Percepcija najugroženijih sektora kritične infrastrukture u Bosni i Hercegovini. Izvor 7: Autorska obrada podataka (2025)

Navedeni rezultat svjedoči sve većoj svijesti i znanju o kibernetičkim rizicima u bankama i platnim sistemima, posebno u kontekstu digitalizacije finansijskih usluga. Na trećem mjestu je zdravstveni sektor (15.1%), na četvrtom transporta (6.8%), te iza odmah slijede telekomunikacije i IT servisi (5.4%). Sektori transporta i telekomunkacija su ocijenjeni kao najmanje ugroženi, iako navedeni stavovi nisu u skladu sa globalnim istraživanjima u kojima se ističe da su upravo digitalna povezanost sektora kritične infrastrukture može predstavljati značajan vektor napada. Predstavljeni rezultati također ukazuju na nedovoljni nivo svijesti javnosti o rizicima koji prate digitalnu transformaciju transportnih i telekomunikacijskih sistema, uprkos njihovoj ključnosti za funkcionisanje moderne kritične infrastrukture.

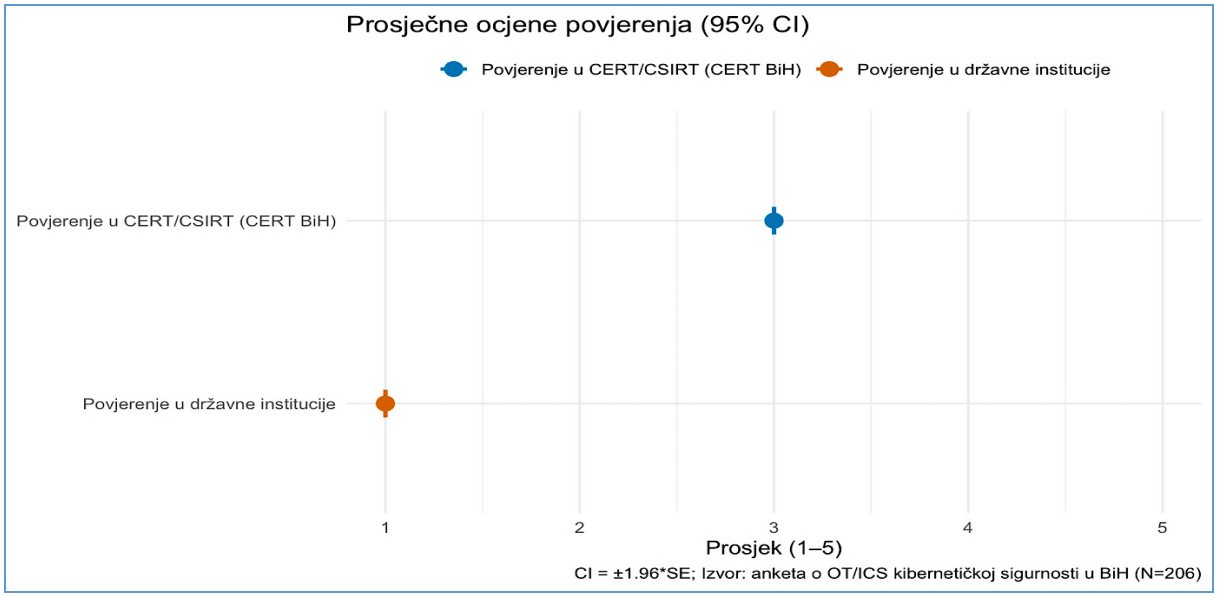
3.7. Medijska zastupljenost tema OT/ICS kibernetičke sigurnosti

Sedmo postavljeno istraživačko pitanje u ovoj studiji tiče se zastupljenosti tema vezanih za OT/ICS kibernetičke sigurnost i kritičnu infrastrukturu u bosanskohercegovačkim medijima. Rezultati upitnika ukazuju na to da većina ispitanika smatra da teme vezane za OT/ICS kibernetičke sigurnost i kritičnu infrastrukturu nisu dovoljno zastupljene u bosanskohercegovačkim medijima (81.1%). Samo 18.9% smatra suprotno, te je jasno da postoji nedovoljno medijsko ukazivanje na važnost ove teme, što opet direktno utiče na nivo javne svijesti i razumijevanja kibernetičkih rizika.

4. DISKUSIJA

Veoma je interesantno naglasiti da nalazi upućuju na određeni raskorak između tehničkog i institucionalnog povjerenja stanovništva u sigurnost kritične infrastrukture u Bosni i Hercegovini. Navedeno se ogleda u činjenici da postoji statistički značajna razlika između povjerenja u CERT tim i povjerenja u institucije Bosne i Hercegovine, iako je planirani CERT tim dio institucija Bosne i Hercegovine. Ovdje je opet bitno naglasiti da CERT tim za odgovor na kibernetičke prijetnje još uvijek nije potpuno funkcionalan u Bosni i

Hercegovini na državnom nivou. Međutim nalazi sugerišu da ispitanici izražavaju umjereno povjerenje u spremnost CERT tima u odbrani kritične infrastrukture od kibernetičkih napada, što opet sugeriše da građani razumiju i prepoznaju više tehničku i stručnu ulogu CERT-a u prevenciji i zaštiti, dok istovremeno izražavaju veoma nisko povjerenje u institucionalne i političke mehanizme državne zaštite kritične infrastrukture. Navedeni kontekst je neuobičajen i nije standardan, ali je značajan je odražava stanje i širu društvenu stvarnost kada je u pitanju povjerenje građana prema institucijama. Ovaj nalaz može i treba biti polazna tačka za jačanje transparentnosti, saradnje i građenje povjerenja između državnih institucija i šireg građanstva. Rezultati navedene analize su prikazani na Slici 4. koja prikazuje prosječnu ocjenu povjerenja (95% CI - interval pouzdanosti). U izračunu korišten je Wilcoxon Signed-Rank Test zbog ordinalne prirode podataka i odstupanja od normalne distribucije. Rezultati su prikazani pomoću tačkastog dijagrama kako bi se vizuelno prikazala razlika u stepenu povjerenja u CERT tim i u državne institucije.



Slika 4: Prosječne ocjene povjerenja u CERT i državne institucije.
Izvor 8: Autorska obrada podataka (2025).

5. ZAKLJUČAK

Cilj provedenog istraživanja je bila pocjena nivoa svijesti, znanja i percepcije rizika u vezi s kibernetičkom sigurnošću operativnih i industrijskih kontrolnih sistema (OT/ICS) u Bosni i Hercegovini. Operativni i kontrolni sistemi su ključne komponente svih procesa u sektorima koji spadaju pod kritičnu infrastrukturu, te samim tim su vrlo često mete različitih hibridnih prijetnji i kibernetičkih napada. Ovo istraživanje je ujedno i prvo istraživanje koncipirano i provedeno u oblasti kibernetičke sigurnosti kritične infrastrukture u Bosni i Hercegovini i kao takvo od velike je važnosti i značaja za naučnu zajednicu. Ispitana javnost u Bosni i Hercegovini posjeduje visok nivo svijesti o ozbiljnosti kibernetičkih prijetnji, umjeren nivo znanja, ali nedovoljno tehničkog znanja na temu za OT/ICS sigurnosti. Ispitanici vjeruju u CERT tim, ali ne širem državnom institucionalnom okviru, što opet upućuje na potrebu izgradnje povjerenja između države i stručnih zajednica. Iako je CERT tim u trenutku vršenja ovog istraživanja u fazi uspostave, te nije finaliziran niti u potpunosti

operativan, javni stav je da postoji povjerenje u nacionalni CERT tim, te da građani i stručna javnost ispravno prepoznaje tehničke kapacitete i spremnost. Sa druge strane, postoji jaz između povjerenja u CERT tim i povjerenje u državne institucije, Profesionalci koji rade s kritičnom infrastrukturom tvrde da su edukacije koje su imali veoma korisne i relevantne za njihov svakodnevni rad. Analiza percepcije ozbiljnosti kibernetičkih prijetnji između IT stručnjaka i građana pokazala je da ne postoji statistički značajna razlika između ove dvije grupe, što upućuje da je svijest o kibernetičkim prijetnjama u kritičnom sektoru izvan stručne i naučne zajednice. Ispitanici koji su anonimno učestvovali u ovoj studiji, najugroženijim smatraju energetski sektor (48.3%), zatim finansijski (24.4%) i zdravstveni (15.1%). Također, veliki dio ispitanika tvrdi da teme vezane za OT/ICS kibernetičku sigurnost nisu dovoljno zastupljene u domaćim medijima (81.1%). Za jačanje nacionalne otpornosti Bosne i Hercegovini potrebna je kombinacija tehničkih mjera, kontinuirano edukovanje kadra, međusektorske saradnje između privatnog i javnog sektora i medijske kampanje koje promovišu važnost ICS/OT sigurnosti. Ova studija i rezultati ove studije se mogu posmatrati kao empirijska osnova za daljnji razvoj nacionalnih sigurnosnih strategija, programa i obuka koje imaju za cilj poboljšanje i jačanje sigurnosti, zaštite i otpornosti kritične infrastrukture Bosne i Hercegovine na kibernetičke prijetnje.

6. LITERATURA

1. Ahić, J., & Hodžić, K. (2025). China's Role in Bosnia and Herzegovina's Critical Infrastructure Development and Security. Kriminalističke Teme, 25(1–2), 25–37. https://doi.org/10.51235/kt.2025.25.1-2.25
2. Almedires, M., & Almaiah, M. (2021). Cybersecurity in Industrial Control System (ICS). 2021 International Conference on Information Technology, ICIT 2021 - Proceedings, 640–647. https://doi.org/10.1109/ICIT52682.2021.9491741
3. Ermin Solak. (2022). ENERGETSKA SIGURNOST- JUČER, DANAS, SUTRA. BEZBEDNOSNI IZAZOVI, RIZICI I PRETNJE 21. VEKA – MULTIDISCIPLINARNI PRISTUP Tematski Zbornik Radova. www.fpsp.
4. Eva Nagyfejeo, & Sarah Puello Alfonso. (2019). Cybersecurity Capacity Review Bosnia and Herzegovina. https://ssrn.com/abstract=3658404
5. Ha, D. T., Hoang, N. X., Hoang, N. V., Du, N. H., Huong, T. T., & Tran, K. P. (2022). Explainable Anomaly Detection for Industrial Control System Cybersecurity. IFAC-PapersOnLine, 55(10), 1183–1188. https://doi.org/10.1016/j.ifacol.2022.09.550
6. Jason D. Christopher. (2024). SANS 2024 State of ICS/OT Cybersecurity. www.sans.org/white-papers/five-ics-cybersecurity-critical-controls
7. Mark Bristow. (2021). A SANS 2021 Survey: OT/ICS Cybersecurity. www.cisa.gov/critical-infrastructure-sectors
8. Matthew J. Kirkland, Daniel Conte de Leon, & Stu Steine. (2021). vWaterLabs: Design and Characteristics of a Virtual Testbed for Water-focused ICS Cybersecurity Education.
9. Popovski, V., Krisafi, L., Nenezić, A., Turčalo, S., Emini, D., & Kovacevic, A. (2023). CRISIS PREVENTION AND CRITICAL INFRASTRUCTURE IN WESTERN BALKANS.

10. Ramezan, C., Coffy, P., & Lemons, J. (2023). Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for? Journal of Cybersecurity Education Research and Practice, 2024(1). https://doi.org/10.32727/8.2023.31
11. Simons Markusson, M. (2023). Consequence-based Detection of Cyberattacks in Operational Technology.
12. Smajić, M., & Bajramović, Z. (2023). RISKS AND VULNERABILITY OF CRITICAL INFRASTRUCTURE IN BOSNIA AND HERZEGOVINA-ASSESSMENT AND PROTECTION.

ASSESSMENT OF PUBLIC AWARENESS AND KNOWLEDGE OF CYBERSECURITY RISKS IN THE MANAGEMENT AND CONTROL SYSTEMS OF CRITICAL INFRASTRUCTURE IN BOSNIA AND HERZEGOVINA

Abstract: *this study represents the first empirical research in Bosnia and Herzegovina that analyzes the level of public awareness, knowledge, and risk perception related to cybersecurity within the management and control systems of critical infrastructure (Operational Technology – OT / Industrial Control Systems – ICS). Although technical and engineering protection measures are fundamental, the human factor—awareness, trust, and perception among the population—remains crucial for strengthening resilience and safeguarding critical infrastructure in Bosnia and Herzegovina. The research was conducted between September 1 and October 31, 2025, through an online questionnaire, resulting in 206 valid responses. Statistical data analysis was performed in RStudio using the R programming language for statistical computations. The results show that the public in Bosnia and Herzegovina correctly perceives the seriousness and importance of cybersecurity threats and possesses a relatively good level of general knowledge about critical infrastructure protection. Furthermore, the public expresses confidence in the capability, readiness, and expertise of the CERT BiH team (which is still not fully operational), while showing considerably less trust in institutional protection and preparedness. Most IT professionals operating in the field of critical infrastructure believe that cybersecurity training is highly beneficial, whereas the comparative analysis between the risk perception of IT experts and citizens did not reveal a statistically significant difference. The findings also emphasize the need to strengthen education and media visibility regarding the importance of cybersecurity for OT/ICS systems. The results of this study may serve as a starting point and foundation for developing national training programs and strategies aimed at enhancing the resilience of critical infrastructure in Bosnia and Herzegovina.*

Keywords: *cybersecurity, critical infrastructure, industrial control systems, operational technology, public awareness, Bosnia and Herzegovina*

PSIHOLOŠKO PROFILIRANJE POČINIOCA U FUNKCIJI SAVREMENE PREVENCIJE KRIMINALITETA

Maida Muratović, *BA. iur* PDS PF UNSA
maidamuratovic444@gmail.com

Sažetak: *može se reći da je psihološko profiliranje počinioca jedna od važnijih, ali istovremeno i najmanje korištenih savremenih metoda prevencije kriminaliteta u zemljama regiona. Iako se o ovoj temi sve češće govori u okviru kriminalističke psihologije i forenzičkih nauka, njena primjena u preventivne svrhe ostaje marginalna. Institucije sigurnosti i dalje su prvenstveno fokusirane na procesuiranje već počinjenih djela, dok se nedovoljno pažnje posvećuje ranom prepoznavanju rizičnih osobina, psiholoških devijacija i obrazaca ponašanja koji prethode kriminalnom djelovanju. Motiv za analiziranje ove teme leži u potrebi da bolje razumijemo ljude u našem okruženju i identifikujemo osobe čije bi karakteristike mogle ukazivati na kriminogeni potencijal, ujedno I cilj ovog rada jeste da se pisanjem o profilisanju kriminalne ličnosti pokuša spriječiti nasilje i smanjiti broj žrtava, a ne da se samo govori o kažnjavanju i povećanju broja zatvorenika. U savremenim društvima, posebno onima suočenim s porastom kriminaliteta, prirodno se nameće pitanje: da li je svako od nas potencijalni počinitelj? Naglasak nije na stigmatizaciji, nego na razlikovanju rizičnih i nerizičnih osobina, razumijevanju utjecaja okoline, stresa, trauma i predispozicija na ponašanje pojedinca. Veliki problem našeg društvenog konteksta jeste zanemarivanje psihološkog pristupa ličnosti. Policijske i zdravstvene strukture trebaju imati obrasce psiholoških karakteristika ljudi oko sebe kako bi prepoznale latentne počinioce, osobe s patološkim crtama ili one koje razvijaju obrasce što upućuju na moguće nasilje.*

Ključne riječi: *psihološko profiliranje, rizične osobine, prevencija kriminaliteta, patološke crte ličnosti, latentni počinioci, kriminalistička psihologija.*

1. UVOD

Psihološko profiliranje počinioca, iako teorijski dobro utemeljeno i detaljno obrađeno u savremenoj kriminologiji, psihologiji i forenzičkim naukama, u praksi zemalja regiona još uvijek zauzima skromno mjesto. Iako brojne studije, modeli i metodološki pristupi jasno ukazuju na njegovu vrijednost, institucionalna primjena ove metode ostaje ograničena, sporadična i često nedovoljno shvaćena. Međutim, kritičari ukazuju na nedostatak dosljedne naučne validacije za mnoge tehnike profiliranja (Eze SM, Alabi KJ, Ibrahim SO, et al. 2025; 9(1): 092-096.). Takav raskorak između teorijskog znanja i praktične realizacije otvara pitanje: zbog čega se jedan od najvažnijih savremenih instrumenata prevencije kriminaliteta ne koristi u mjeri u kojoj bi to moglo unaprijediti kriminalističke politike i zaštitu društva? Savremeno društvo suočeno je s kontinuiranim porastom različitih oblika kriminalnog ponašanja, od nasilničkih delikata, porodičnog nasilja i seksualnih napada, do maloljetničkog prestupništva, različitih oblika imovinskog kriminaliteta, pa i sve sofisticiranijih oblika organizovanog kriminala. U takvom okruženju postaje neophodno razumjeti kako djelo, tako i osobu koja ga izvršava. Ljudi ne postaju počinioci preko noći, dakle njihovo ponašanje oblikuje kompleksna kombinacija psiholoških predispozicija, emocionalnih konflikata, trauma, životnih iskustava i socijalnog okruženja. Upravo zato, poznavanje profila ličnosti

predstavlja dragocjen uvid u niz faktora koji prethode izvršenju krivičnog djela. Teorijski postulati psihološkog profiliranja polaze od pretpostavke da svako krivično djelo nosi psihološki potpis izvršioca, odnosno tragove ponašanja koji, pravilno analizirani, mogu ukazati na njegove karakteristike, motivaciju, mentalne obrasce i emocionalne dispozicije. Takvi obrasci, bilo da je riječ o načinu selekcije žrtve, izboru mjesta događaja, stepenu brutalnosti, načinu prikrivanja tragova ili specifičnim ritualnim radnjama, omogućavaju stručnjacima da oblikuju vjerodostojan psihološki portret koji može pomoći u prevenciji i identifikaciji počinilaca. Međutim, i pored jasno postavljenih teorijskih osnova, u praksi se i dalje bilježi nedostatak sistematskog pristupa profiliranju. Policijske, zdravstvene i druge nadležne institucije najčešće reaguju tek nakon izvršenog krivičnog djela, zanemarujući ranu detekciju osoba kod kojih se primjećuju rizične osobine ili obrasci ponašanja koji ukazuju na potencijalnu opasnost. Time se propušta dimenzija prevencije – pravovremeno prepoznavanje pojedinaca koji zbog psiholoških karakteristika, emocionalne nestabilnosti, socijalnih deficita ili devijantnih sklonosti mogu postati izvršioci težih oblika kriminalnog ponašanja. U društvu u kojem se sve češće postavlja pitanje „ko su ljudi oko nas i šta ih motiviše na nasilje?“, postaje neophodno preispitati postojeće pristupe sigurnosti i okrenuti se pravovremenoj identifikaciji rizičnih profila. Psihološko profiliranje, kao metoda koja povezuje naučno znanje o ljudskom ponašanju sa operativnim potrebama policije, nudi upravo takvu mogućnost. Njegova šira primjena mogla bi predstavljati značajan iskorak u modernizaciji preventivnih strategija, jačanju institucionalne efikasnosti i zaštiti ranjivih društvenih skupina. U tom kontekstu, ovaj rad nastoji naglasiti važnost psihološkog profiliranja kao savremenog instrumenta prevencije kriminaliteta, analizirati teorijske postulate na kojima metoda počiva, te ukazati na potrebu njenog snažnijeg implementiranja u institucijama nadležnim za sigurnost i mentalno zdravlje građana. Razumijevanje ličnosti počinioca može se posmatrati kao nužan korak ka sigurnijem društvu.

1.1. Psihološko profiliranje počinioca kao teorijski koncept i institucionalni izazov

Psihološko profiliranje učinioca krivičnog djela već decenijama predstavlja jednu od najkontroverznijih, ali i najintrigantnijih oblasti savremene kriminologije, psihologije i psihijatrije (Rašić, H., Kovačević, D., Žarković Palijan, T. (2012: 2, 277–292). Iako je u stručnoj i naučnoj literaturi detaljno obrađeno, te time postavljen čvrst teorijski temelj za njegovo razumijevanje i primjenu, stvarno korištenje ove metode u radu institucija – kako sigurnosnih, tako i medicinsko-psihijatrijskih – ostaje pitanje koje se i dalje otvara pred nadležnim organima. Više od šezdeset godina prakse kriminalističkog profiliranja prošlo je bez preciznih, sistematskih i strogih naučnih evaluacija (Snook, B., Cullen, R.M., Bennell, C., Taylor, P., & Gendreau, P. (2008). Uprkos tome, metoda se danas koristi u početnim fazama kriminalističkih istraga, posebno u situacijama kada policija još uvijek traga za identitetom učinioca. U takvim slučajevima koriste se sve raspoložive tehnike kako bi se izgradio vjerodostojan psihološki portret osobe koja je izvršila djelo (Baić, V., Deljkić, I. (2019). Na taj način, profiliranje pomaže u odgovoru na glavno pitanje: *šta nam krivično djelo govori o ličnosti onoga ko ga je počinio? (*Stefoff, R. (2011). Takav odgovor zahtijeva analizu prirode djela, načina njegovog izvršenja, selekcije žrtve, mjesta događaja i svakog specifičnog obrasca ponašanja koji je ostao zabilježen tokom izvršenja (Wrightsman, L. S., Greene, E., Nietzel, M. T., Fortune, W. H. (2002). Cilj je da se, na osnovu interpretacije

tragova ponašanja, izrade informacije o najvjerovatnijim osobinama nepoznatog počinioca. Teorijski model na kojem se profilisanje zasniva polazi od pretpostavke da prikupljeni podaci ukazuju na stabilne psihološke karakteristike osobe, kao i da se o njima može zaključivati na osnovu načina izvršenja krivičnog djela. Ova metoda nalazi svoju primjenu u različitim oblastima kriminalnog djelovanja, dakle od krvnih i seksualnih delikata, preko imovinskih krivičnih djela, pa sve do terorizma i organizovanog kriminaliteta (Ainsworth, P. B. (2000*).* Ipak, najviše se koristi u rasvjetljavanju djela čiji „modus operandi" ukazuje na emocionalno ili psihopatološko stanje učinioca, poput sadističkog nasilja, postmortalnog sakaćenja tijela ili ubistava bez jasne motivacije. Upravo u tim situacijama ponašanje ostavlja najjasnije psihološke tragove. Međutim, i pored bogate literature, detaljno razrađenih teorijskih modela i velikog broja studija slučaja, primjena psihološkog profiliranja u institucijama regiona je rijetka, nesistematična i često zavisi isključivo od entuzijazma pojedinih profesionalaca. Ono što ostaje kao otvoreno pitanje jeste zašto teorijska znanja nisu pretočena u praksu, te zbog čega se institucije, posebno policijske, tužilačke, medicinske i psihijatrijske, još uvijek ne koriste ovom metodom kao standardnim alatom prevencije i rasvjetljavanja najtežih oblika kriminala. Kočnica u realizaciji očigledno postoji, bilo da se radi o operativnim ili institucionalnim mehanizmima. Možemo uvidjeti da je literatura odavno postavila temelje: jasno definisane koncepte, razrađene modele i, nadasve, dokazanu korisnost profiliranja. Ono što nedostaje jeste institucionalna hrabrostm konačni mehanizam i strateški pristup da se ti modeli implementiraju u svakodnevni rad sigurnosnih struktura. Dok god se profilisanje bude posmatralo više kao teorijska zanimljivost nego kao praktičan alat, njegovi puni potencijali ostat će neiskorišteni – na štetu prevencije, efikasnosti istraga i sigurnosti društva u cjelini.

1.2. Historijski razvoj kriminalnog profiliranja kao temelj savremene primjene

Kriminalno profiliranje, iako kao sistematizirana i institucionalizirana metoda dobija puni značaj tek u drugoj polovini XX stoljeća, ima duboke historijske korijene koji svjedoče o dugotrajnom interesu za povezanost ličnosti i kriminalnog ponašanja (Šeparović, Zvonimir, 1981 ; 19-20). Upravo taj historijski kontinuitet pokazuje da savremeno profiliranje nije prolazni teorijski konstrukt, već rezultat postepenog razvoja mišljenja o unutrašnjim uzrocima kriminaliteta. Već u klasičnoj antici grčki filozofi nastojali su objasniti kriminalno ponašanje kroz unutrašnja moralna i psihološka stanja pojedinca. Sokratova ideja „bolesnog duha", Platonova podjela prestupnika na popravljive i nepopravljive te Aristotelovo insistiranje na individualnoj odgovornosti predstavljaju rane oblike razmišljanja koji kriminalitet stavljaju u direktnu vezu s ličnošću počinioca (Baggerman, J. Arianne; Dekker, Rudolf M.; Maschuch, Michael J., 2011; 250). Iako filozofska, ova razmatranja jasno pokazuju da se individua od samih početaka posmatra kao centralni nosilac kriminalnog ponašanja, što ostaje temelj savremenog profiliranja. Tokom srednjeg i ranog novog vijeka pokušaji klasifikacije kriminalaca poprimaju primitivne i često pseudoznanstvene oblike, poput profiliranja heretika i vještica, kao i kasnije fiziognomije i frenologije. Iako su ove teorije danas odbačene, one ukazuju na trajnu potrebu društva da kriminalitet tumači kroz lične karakteristike počinioca, a ne isključivo kroz pravne norme (Singer, M, Kovčo V, Cajner Mraović I, 2002; 65) Pravi naučni zaokret nastaje krajem XIX stoljeća razvojem psihologije kao samostalne naučne discipline. Radovi Wilhelma Wundta, a potom i psihoanalitičara poput Freuda, Adlera i Junga, otvorili su prostor za sistematsko proučavanje unutrašnjih

konflikata, emocija i strukture ličnosti u kontekstu kriminalnog ponašanja. U tom periodu javlja se i prvi pokušaj praktičnog profiliranja u slučaju Jacka Trbosjeka, čime je postavljen važan princip da krivično djelo nosi prepoznatljive tragove ličnosti počinioca. Kriminalno profiliranje kao priznati institut afirmira se tek nakon 1970-ih godina osnivanjem Behavioral Analysis Unit (BAU) pri FBI-u, čime dobija metodološki okvir i institucionalnu podršku. Od tada do danas ono postaje sastavni dio savremenih kriminalističkih istraga, naročito u anglosaksonskom pravnom krugu, dok se u Evropi razvija kroz koncepte istražne i geografske psihologije (Modus Operandi and 'Offender Profiling': 2002). Savremena primjena kriminalnog profiliranja sve više prevazilazi isključivo represivnu funkciju i usmjerava se ka razumijevanju kriminalnog ponašanja i njegovoj prevenciji. Historijski razvoj ove metode jasno pokazuje da se radi o institutu s čvrstim teorijskim kontinuitetom, koji se kroz vrijeme prilagođavao razvoju nauke i društva. Upravo zbog toga kriminalno profiliranje, uz daljnju znanstvenu nadogradnju, predstavlja legitiman i opravdan alat savremene prevencije kriminaliteta.

1.3. Pioniri kriminalnog profiliranja

Da bi se danas mogle uvoditi nove mjere, mijenjati pristupi i primjenjivati savremeni modeli prevencije kriminaliteta, neophodno je razumjeti odakle potiče sama ideja takvog djelovanja. Historijski posmatrano, još mnogo prije savremenih institucija i naučnih disciplina, ljudi su uočavali da ponašanja koja odstupaju od uobičajenog i društveno prihvatljivog zahtijevaju dodatnu pažnju i dublje razumijevanje. Takva ponašanja, bilo nekada ili danas, imaju potencijal da unište ne samo pojedinca koji ih ispoljava, već i širu društvenu zajednicu. Društvo se kontinuirano suočava s osobama koje, zbog određenih ličnih osobina, trauma, unutrašnjih konflikata ili poremećaja, ispoljavaju nasilničko i društveno negativno ponašanje. Smatrati da te osobe „imaju pravo" na takvo ponašanje, bez ikakvog pokušaja ranog prepoznavanja i prevencije, ne može se opravdati ni moralno ni profesionalno. Upravo iz tog razloga, suština kriminalnog profiliranja nije povećanje broja zatvorenika, već smanjenje broja žrtava. U tom kontekstu, važno je osvrnuti se na pionire koji su, svaki u okviru svog vremena i znanja, pokušavali objasniti vezu između ličnosti i kriminalnog ponašanja. Jedan od prvih bio je Cesare Lombroso (1836–1909), koji je smatrao da se kriminalci mogu razlikovati od ostalih ljudi na osnovu određenih fizičkih obilježja. Iako su njegove teorije danas opravdano kritikovane i u velikoj mjeri napuštene, Lombrosov značaj leži u činjenici da je kriminalitet prvi put sistematski povezao s osobinama pojedinca, a ne isključivo s pravnim normama. Time je otvorio prostor za razmišljanje o kriminalcu kao osobi sa specifičnim karakteristikama, što predstavlja jednu od osnovnih ideja savremenog profiliranja. Pravi zaokret ka praktičnoj primjeni profiliranja desio se sredinom XX stoljeća zahvaljujući James Brussel, psihijatru iz New Yorka i prvom poznatom kriminalnom profileru u Sjedinjenim Američkim Državama. U saradnji s policijom, Brussel je radio na složenim slučajevima serijskih bombaških napada, podmetanja požara i ubistava. Njegov najpoznatiji doprinos odnosi se na slučaj tzv. „Ludog bombaša", koji je godinama izbjegavao policiju postavljajući eksplozivne naprave na javnim mjestima. Analizom pisama, načina izvršenja i simbolike napada, Brussel je izradio psihološki profil koji je precizno opisivao ličnost počinioca – paranoičnu, pedantnu i duboko ogorčenu osobu s ličnim motivima osvete. Taj profil je, posredno, doveo do identifikacije i hapšenja Georgea Meteskyja, čime je po prvi

put jasno potvrđena operativna vrijednost psihološkog profiliranja u praksi (Alison, Laurence, ur. 2013) Svjestan ograničenja intuicije, Brussel je nastojao svoje metode učiniti sistematičnijim. U saradnji s agentima Federal Bureau of Investigation Howarda Tetena i Patricka J. Mullanyja, tokom 1970-ih godina učestvovao je u razvoju prvih formalnih obuka koje su dovele do osnivanja Jedinice za bihevioralne nauke, kasnije poznate kao Jedinica za bihevioralnu analizu (BAU) (Turvey, Brent E. 2002). Time je profiliranje po prvi put institucionalizirano i uključeno u zvanične kriminalističke procedure. Daljnji razvoj moderne metodologije obilježili su agenti FBI-a Robert K. Ressler i John Douglas, zajedno s forenzičkom medicinskom sestrom Ann Burgess, koji su tokom 1980-ih godina razvili bihevioralni intervju i sistematske procedure profiliranja kroz opsežne razgovore sa serijskim ubicama. Njihov rad omogućio je dublje razumijevanje obrazaca ponašanja i motiva najtežih nasilnih počinilaca. Prema tome, početkom 1990-ih godina britanski psiholog David Canter dao je veoma važan doprinos savremenom shvatanju profiliranja osnivanjem istraživačke psihologije. Za razliku od ranijih pristupa, Canter se zalagao za korištenje empirijskih, recenziranih istraživanja i statističkih metoda, čime je profiliranje dodatno udaljeno od spekulacija, a približeno naučno utemeljenoj praksi (Esherick, Joan. 2014). Razvoj kriminalnog profiliranja, od ranih filozofskih i bioloških pokušaja do savremenih interdisciplinarnih metoda, jasno pokazuje da se ne radi o prolaznom trendu, nego o kontinuiranom nastojanju da se kriminalno ponašanje razumije kako bi se preveniralo. Upravo ta historijska linija opravdava njegovu današnju primjenu, posebno u funkciji zaštite potencijalnih žrtava i smanjenja nasilja u društvu.

1.3.1. Da li je kriminalno profiliranje nužan alat savremenog krivičnog sistema

Kao i većina savremenih istražnih metoda koje se nalaze na granici više naučnih disciplina, kriminalno profiliranje kontinuirano izaziva podijeljena mišljenja u stručnoj i naučnoj javnosti. Dok ga jedni smatraju vrijednim analitičkim alatom koji može doprinijeti rasvjetljavanju najsloženijih oblika kriminalnog ponašanja, drugi mu zamjeraju nedostatak empirijske provjerljivosti i jasne metodološke standardizacije. Upravo zbog takvog dualnog položaja, pitanje opravdanosti i potrebe kriminalnog profiliranja ostaje jedno od temeljnih savremenih kriminoloških pitanja. Najčešći prigovori upućeni kriminalnom profiliranju odnose se na njegov navodno pseudoznanstveni karakter i otežanu mogućnost empirijske verifikacije rezultata. Pojedini autori ističu da profiliranje ne ispunjava stroge kriterije naučnih metode, budući da se često oslanja na interpretativne procjene i deduktivne zaključke, a ne na statistički provjerljive zakonitosti. U tom kontekstu, kriminalno profiliranje je čak poređeno s disciplinama poput astrologije, uz tvrdnje da njegovi zaključci često počivaju na općim i teško mjerljivim pretpostavkama (Gladwell, Malcolm, 2019; 91-118. Dodatne kritike dolaze iz studija koje ukazuju na slabu ili nejasnu povezanost između ponašanja na mjestu zločina i stabilnih karakteristika ličnosti počinioca, upozoravajući na opasnost preuveličavanja dometa profiliranja u istražnoj praksi. Drugi pravac kritike fokusiran je na pitanje stručnosti onih koji se bave profiliranjem. Istraživanja su pokazala da razlike u tačnosti profila između iskusnih profilera i osoba bez specijalizirane obuke nisu uvijek statistički značajne, što je dovelo do zaključaka da profiliranje može biti podložno subjektivnim interpretacijama i kognitivnim pristranostima (Pinizzotto, Anthony J.; Finkel, Norman J.1990; 215-233).Posebno je problematično to što su laici, oslanjajući se na socijalne

stereotipe, često skloni davanju uvjerljivih, ali netačnih profila, dok su čak i profesionalni profileri ponekad precjenjivali vlastitu preciznost. Međutim, uprkos ovim kritikama, važno je naglasiti da osporavanje potpune naučne preciznosti kriminalnog profiliranja ne znači nužno i njegovo odbacivanje kao korisnog istražnog sredstva. Brojne studije ukazuju na to da je osnovni problem u procjeni njegove vrijednosti upravo teškoća mjerenja „tačnosti" profila (Alison, Laurence; Smith, Matthew D.; Morgan, Keith, 2003; 185-195). Profiliranje ne proizvodi binarne rezultate koji se mogu lako provjeriti, već nudi skup vjerovatnih karakteristika koje služe kao orijentir u daljnjoj istrazi (Snook, Brent; Eastwood, Joseph; Gendreau, Paul; Goggin, Claire; Cullen, Richard M., 2007;437- 453). Upravo zbog toga, njegova vrijednost se ne ogleda u identifikaciji konkretnog počinioca, već u sužavanju kruga sumnjivih i boljem razumijevanju kriminalnog ponašanja. Empirijski podaci iz prakse FBI-a dodatno potvrđuju ovu tezu. Analiza slučajeva u kojima je profiliranje korišteno pokazala je da je u određenom broju predmeta ono direktno doprinijelo identifikaciji počinioca, dok je u znatno većem broju slučajeva imalo pomoćnu, ali ipak značajnu ulogu u vođenju istrage i strateškom odlučivanju (Stefoff, Rebecca, 2011). Pored toga, istražitelji i policijski službenici u velikoj mjeri percipiraju kriminalno profiliranje kao koristan alat, što govori u prilog njegovoj praktičnoj vrijednosti, bez obzira na metodološke nedostatke. Kada se pitanje kriminalnog profiliranja posmatra iz perspektive domaćeg i regionalnog konteksta, dolazi se do dodatnog sloja problema. Na prostoru Bosne i Hercegovine, ali i šireg regiona jugoistočne Evrope, kriminalno profiliranje gotovo da nema institucionalno utemeljenu primjenu. Iako se elementi psihološke procjene ličnosti pojavljuju u sudsko-psihijatrijskim i psihološkim vještačenjima, sistematsko korištenje profiliranja u preventivne ili istražne svrhe ostaje sporadično i zavisi od individualne inicijative pojedinih stručnjaka. Policijske strukture i tužilaštva primarno su usmjerene na represivno djelovanje nakon izvršenog krivičnog djela, dok se ranoj identifikaciji rizičnih obrazaca ponašanja posvećuje minimalna pažnja. Upravo u tom kontekstu kriminalno profiliranje može dobiti poseban značaj. Društva koja se suočavaju s porastom nasilnog kriminaliteta, porodičnog nasilja, maloljetničke delinkvencije i povratništva u kriminalu, imaju izraženu potrebu za alatima koji omogućavaju raniju intervenciju. Profiliranje, ako se koristi odgovorno i interdisciplinarno, može doprinijeti boljem razumijevanju ličnosti prestupnika, identifikaciji faktora rizika i razvoju preventivnih strategija usmjerenih na zaštitu društva, a ne isključivo na sankcionisanje posljedica. Savremeni pristupi kriminalnom profiliranju sve više naglašavaju potrebu njegove transformacije iz intuitivne i parcijalno empirijske metode u znanstveno utemeljen, interdisciplinaran analitički okvir. Autori koji su među najistaknutijim kritičarima profiliranja istovremeno zagovaraju njegovu reformu, a ne ukidanje, ukazujući na potrebu jasnijih metodoloških pravila, veće saradnje između psihologa, kriminologa i pravnika, te kontinuirane evaluacije prakse. Shodno navedenom, samo pitanje „treba li nam kriminalno profiliranje" ne može se posmatrati kroz binarnu dilemu korisno–nekorisno. Njegova vrijednost zavisi od načina primjene, nivoa stručnosti i institucionalnog okvira u kojem se koristi. Iako još uvijek ne postoje savršeni modeli za empirijsku provjeru njegove tačnosti, činjenica da se kriminalno profiliranje sve češće koristi u razvijenim pravnim sistemima, te da uživa podršku praktičara, ukazuje na njegov realni potencijal.

Za društva poput našeg, kriminalno profiliranje ne predstavlja luksuz, već mogući iskorak ka modernijem, preventivno orijentiranom sistemu sigurnosti. Uz holistički i interdisciplinarni

pristup, ono može prerasti iz „korisne opcije“ u nužan instrument savremene borbe protiv kriminaliteta.

1.4. Opravdanost primjene kriminalnog profilisanja

Faza modela	Željeni cilj	Uključene institucije	Primjeri primjene u BiH	Očekivani preventivni efekti
I. Rano prepoznavanje rizika	Sistematsko uočavanje ponavljajućih obrazaca ponašanja koji odstupaju od uobičajenog I normaliziranog, uključujući učestale prijetnje, porodične konflikte, nasilničnog ponašanja, zloupotrebu alkohola ili opojnih droga, izraženu impulzivnost, socijalnu izolaciju te školske izostanke i agresiju kod maloljetnika. Psihološki profil se koristi isključivo kao signal upozorenja i indikator potencijalnog rizika, a ne kao osnova za sankcionisanje ili stigmatizaciju pojedinca.	Policija (operativni sektor), centri za socijalni rad, škole, te bolnice (primarni, sekundarni i tercijarni nivo).	• Višestruke policijske intervencije zbog porodičnog nasilja bez prijave KD-a. • Maloljetnik s ponavljanim nasilnim ponašanjem u školi ili zajednici. • Osoba poznata policiji po prijetnjama ili agresivnom ponašanju, ali bez formalnog krivičnog postupka.	Pravovremeno prepoznavanje rizičnih situacija prije eskalacije u teška krivična djela; smanjenje iznenadnih nasilnih incidenata i povećanje ukupne sigurnosti zajednice.
II. Strukturirana procjena ličnosti	Uvođenje jedinstvenog, opisnog i stručno kontrolisanog obrasca procjene ličnosti koji obuhvata psihološke, socijalne i kriminogene faktore, poput emocionalne stabilnosti, nivoa samokontrole, porodičnih odnosa, prisustva stresora i prethodnog rizičnog ponašanja. Procjena nema dijagnostički niti represivni karakter, već služi smanjenju subjektivnosti i oslanjanja isključivo na intuiciju službenika.	Policija (analitički sektor), psiholog, psihijatar, kriminolog	• Analitička procjena povratnika u nasilju u porodici • Procjena rizika kod mladih uključenih u tuče, nasilničko ponašanje ili krađe. • Procjena osoba koje prijete ili pokazuju eskalaciju agresije, ali još nisu procesuirane.	Ujednačen, transparentan i stručan pristup procjeni rizika; smanjena mogućnost greške, pristrasnosti i proizvoljnog odlučivanja.
III. Preventivna intervencija	Na osnovu prethodne procjene primjenjuju se individualizirane, neinvazivne i proporcionalne mjere, kao što su savjetodavni razgovori, uključivanje porodice, upućivanje na psihološku ili socijalnu	Policija, centri za socijalni rad, zdravstvene ustanove, nevladin sektor, lokalna zajednica.	• Savjetodavni i nadzorni rad s nasilnikom u porodici prije eskalacije. • Uključivanje maloljetnika u preventivne i edukativne programe.	Smanjenje rizika ponavljanja nasilja i kriminalnog ponašanja; jačanje zaštitnih faktora i otpornosti pojedinca, preventivno sigurnosno odgajanje pojedinca, sklonog nasilničkom ili nekom

	podršku, te pojačani nadzor bez ograničavanja osnovnih prava. Fokus je na pomoći, stabilizaciji i prekidu kriminogenih obrazaca, a ne na kažnjavanju.		• Psihološka podrška osobama s izraženim stresnim reakcijama ili traumama.	drugom negativnom ponašanju. Model :"sigurnosni odgoj pojedinca od strane kriminologa"
IV. Praćenje i evaluacija	Kontinuirano praćenje efekata primijenjenih mjera kroz periodične revizije procjene rizika, sistematsko dokumentovanje postupanja i evaluaciju ishoda. Ova faza osigurava zakonitost, proporcionalnost, zaštitu ljudskih prava i transparentnost u radu institucija.	Sve uključene institucije	• Redovna revizija slučajeva porodičnog nasilja • Evaluacija maloljetnika uključenih u preventivne programe • Interna i eksternalna kontrola policijskog postupanja	Sprečavanje zloupotrebe modela; jačanje povjerenja javnosti u institucije; dokazivanje stvarne opravdanosti i efikasnosti primjene psihološkog profiliranja.

Tabela 1: Skica prijedloga modela preventivne primjene psihološkog profiliranja u BiH. Izvor: Prijedlog autora

Predloženi model preventivne primjene psihološkog profiliranja u Bosni i Hercegovini nastao je kao rezultat zapažanja autora ovog rada, koja su se formirala kroz pripravnički rad u ministarstvu unutrašnjih poslova, gdje se autor neposredno susretao s različitim profilima počinilaca krivičnih djela, ali i s osobama koje, iako formalno nisu procesuirane, pokazuju izražene obrasce društveno negativnog i rizičnog ponašanja. Upravo takvi susreti ukazuju na jednu od osnovnih slabosti savremenog sigurnosnog sistema, dakle činjenicu da se institucije najčešće aktiviraju tek nakon što je nasilje već eskaliralo i proizvelo štetne posljedice, dok se rani signali upozorenja često zanemaruju ili posmatraju izolovano. Prikazana tabela koncipirana je kao pokušaj odgovor na taj problem i predstavlja prijedlog za sistematizaciju preventivnog pristupa koji bi omogućio ranije, koordiniranije i stručnije djelovanje. Svaka od faza modela zasniva se na logici postupnosti, proporcionalnosti i interdisciplinarnosti, čime se nastoji izbjeći i represivni automatizam i neosnovana stigmatizacija pojedinaca.

Prva faza – ***rano prepoznavanje rizika*** – polazi od realne činjenice da nasilničko i kriminalno ponašanje rijetko nastaje iznenad i "preko noći". Brojni slučajevi nasilja u porodici, teških tjelesnih ozljeda, nasilničkog ponašanja, pa i ubistava, u praksi su prethodno bili praćeni ponavljanim prijetnjama, verbalnim sukobima, alkoholizmom, psihičkom nestabilnošću ili ranijim policijskim intervencijama bez prijave krivičnog djela. Ignorisanje tih obrazaca, bilo zbog nedostatka jasnog modela ili straha od „neutemeljenog postupanja", u konačnici dovodi do rasta broja žrtava. Iako nauka s pravom zahtijeva empirijsku provjeru svake teze, praksa pokazuje da čekanje potpunog naučnog konsenzusa u oblasti prevencije nasilja i nasilničkog ponašanja često znači zakasnjelu reakciju sistema. U tom smislu, psihološko profiliranje u prvoj fazi modela nema funkciju presuđivanja, već isključivo funkciju signalizacije rizika. Takav pristup u potpunosti je u skladu s principima savremene prevencije kriminaliteta, gdje se naglasak stavlja na prepoznavanje obrazaca ponašanja, a ne na etiketiranje ličnosti. Upravo zato su u gore izvedenoj skici jasno navedeni primjeri poput višestrukih policijskih

intervencija bez prijave krivičnog djela ili ponavljanog nasilnog ponašanja kod maloljetnika, jer se radi o realnim situacijama s kojima se institucije u BiH svakodnevno susreću.

Druga faza – ***strukturirana procjena ličnosti*** – predstavlja pokušaj da se praksa oslanjanja isključivo na intuiciju i subjektivnu procjenu zamijeni ujednačenijim i isključivo stručnijim pristupom. U domaćem kontekstu često se susreće situacija da slični slučajevi bivaju različito procijenjeni u zavisnosti od institucije, službenika ili lokalne prakse. Uvođenjem opisnog, stručno kontrolisanog obrasca procjene smanjuje se rizik od proizvoljnosti, a odluke se temelje na jasno definisanim indikatorima rizika i zaštitnim faktorima. Važno je naglasiti da se i u ovoj fazi izbjegava represivni pristup, čime se čuva osnovni princip presumpcije nevinosti i zaštite ljudskih prava.

Treća faza – ***preventivna intervencija*** – nosi najveću praktičnu vrijednost predloženog modela. U savremenim društvima, uključujući i Bosnu i Hercegovinu, sve je očiglednije da represija sama po sebi ne smanjuje dugoročno nasilje, naročito kada je riječ o maloljetnicima i osobama s izraženim psihosocijalnim problemima. Koncept preventivne intervencije, zasniva se na individualiziranom pristupu i uključivanju porodice, zajednice i stručnjaka iz različitih oblasti. Posebno mjesto u ovoj fazi zauzima model *„sigurnosnog odgoja pojedinca od strane kriminologa“,* koji se može posmatrati kao most između teorijskog znanja i praktičnog djelovanja. Kriminolog u ovom kontekstu ne djeluje kao represivni autoritet, već kao stručnjak koji pomaže pojedincu da razumije posljedice vlastitog ponašanja i razvije alternativne, društveno prihvatljive obrasce.

Četvrta faza – ***praćenje i evaluacija*** – uvedena je iz potrebe da se odgovori na legitimne kritike upućene psihološkom profiliranju, posebno one koje se odnose na mogućnost zloupotrebe i kršenja prava pojedinca. Kontinuirana evaluacija obradsca omogućava da se svaka primijenjena mjera preispita, dokumentuje, ali naravno po potrebi i koriguje. Ovim činom bi se osigurala transparentnost rada institucija, kao i jačanje povjerenje javnosti, što je naročito važno u društvu koje je osjetljivo na pitanja zloupotrebe ovlasti, a idealan primjer osjetljivosti društva jeste stanovništvo Bosne i Hercegovine Iako se mora priznati da još uvijek ne postoje dovoljno opsežna empirijska istraživanja koja bi u potpunosti potvrdila prediktivnu moć psihološkog profiliranja u preventivne svrhe, jednako je važno istaći da i samo nedjelovanje nosi svoje vlastite, vrlo konkretne posljedice. Porast broja žrtava nasilničkog ponašanja, naročito u porodičnom kontekstu i među mladima, predstavlja realan društveni problem koji zahtijeva odgovore sada, a ne tek nakon potpune naučne validacije svakog pojedinačnog instrumenta. Predloženi model, upravo zbog svoje postepenosti, proporcionalnosti i stalne evaluacije, nudi balans između naučne opreznosti i praktične odgovornosti. Na taj način, ovakvo predložena skica se ne može posmatrati kao konačno rješenje, već kao jedan početni okvir koji omogućava testiranje, prilagođavanje i daljnju naučnu evaluaciju preventivne primjene psihološkog profiliranja u Bosni i Hercegovini. Njena opravdanost leži u pokušaju da se smanji broj žrtava nasilja, unaprijedi institucionalna koordinacija i pomjeri fokus sa posljedica na uzroke kriminalnog ponašanja, čime se ostvaruje osnovni cilj savremene sigurnosne politike, a to jeste zaštita društva uz poštivanje dostojanstva pojedinca.

2. ZAKLJUČCI

Na osnovu cjelokupne teorijske analize, historijskog pregleda, kritičkog sagledavanja savremene prakse i razrade prijedloga modela preventivne primjene psihološkog profiliranja, može se izvesti nekoliko bitnih zaključaka:

1. Psihološko profiliranje ima teorijsko i historijsko utemeljenje, te se ne može posmatrati kao savremeni eksperiment ili prolazni trend. Njegov razvoj, od ranih filozofskih razmatranja do savremenih interdisciplinarnih modela, potvrđuje kontinuitet ideje da kriminalno ponašanje proizlazi iz prepoznatljivih obrazaca ličnosti i ponašanja, što opravdava njegovu današnju primjenu.
2. Savremeni sigurnosni sistemi, uključujući onaj u Bosni i Hercegovini, dominantno su reaktivno orijentisani, što znači da institucije djeluju tek nakon što je krivično djelo izvršeno, što u konačnici ne ide u korist sprječavanju žrtava, nego samo u postizanju sankcionisanja.
3. Iako psihološko profiliranje nema apsolutnu trenutnu empirijsku preciznost, analiza savremene literature i prakse pokazuje da nijedna preventivna metoda u oblasti kriminaliteta ne posjeduje potpunu prediktivnu sigurnost. Odsustvo potpune naučne validacije ne znači odsustvo praktične vrijednosti, naročito u kontekstu ranog prepoznavanja rizičnih obrazaca ponašanja.
4. Kriminalno ponašanje rijetko nastaje iznenada, već mu prethode ponavljajući obrasci poput prijetnji, nasilničkog ponašanja, eskalacije konflikata, svakog oblika nasilja u porodici, zloupotrebe opojnih supstanci i socijalne disfunkcije.
5. Predloženi model preventivne primjene psihološkog profiliranja pokazuje da je moguće uspostaviti proporcionalan i pravno prihvatljiv okvir, koji ne dovodi do stigmatizacije pojedinca niti kršenja ljudskih prava. Profiliranje se u tom modelu koristi kao signal upozorenja i analitička smjernica, a ne kao osnova za sankcionisanje ili dokazivanje krivnje.
6. Interdisciplinarni pristup, koji uključuje policiju, centre za socijalni rad, zdravstvene ustanove i lokalnu zajednicu, predstavlja kvalitetni početni uslov opravdane primjene profiliranja. Time bi se svakako smanjika subjektivnost pojedinačnih procjena i povećava stručna odgovornost institucija u donošenju odluka.
7. Preventivne intervencije zasnovane na individualiziranoj procjeni ličnosti imaju veći potencijal dugoročnog smanjenja nasilja od isključivo represivnih mjera, posebno kada je riječ o maloljetnicima i osobama s izraženim psihosocijalnim rizicima. U tom kontekstu, cilj sistema nije povećanje broja sankcionisanih lica, već prekid kriminogenih obrazaca ponašanja.
8. Zamišljeni model „sigurnosnog odgoja pojedinca od strane kriminologa“ predstavlja realno ostvarivu i društveno prihvatljivu preventivnu mjeru, koja povezuje teorijska znanja kriminologije s praktičnim radom na terenu.
9. Kontinuirano praćenje i evaluacija kreiranog obraca predstavljaju neophodnu korekciju primjene psihološkog profiliranja, čime se odgovara na legitimne kritike o mogućoj zloupotrebi, gdje bi takav mehanizam osigurava transparentnost, zakonitost i povjerenje javnosti u rad institucija.

10. Uspjeh psihološkog profiliranja kriminalnog ponašanja se treba mjeriti smanjenjem potencijalnih žrtava, a nikako samo u povećanju broja sankcionisanih počinilaca odnosno zatvorenika.

4. POPIS LITERATURE

1. Ainsworth, P. B. (2000). *Psychology and Crime: Myths and Reality*. Harlow: Pearson Education.
2. Alison, L. (ur.) (2013). *Zbirka slučajeva forenzičkih psihologa: Psihološko profiliranje i kriminalistička istraga*. London: Routledge.
3. Alison, L., Smith, M. D., & Morgan, K. (2003). Interpreting the accuracy of offender profiles. *Psychology, Crime & Law*, 9(2), 185–195.
4. Baggerman, J. A., Dekker, R. M., & Maschuch, M. J. (2011). *Controlling Time and Shaping the Self: Developments in Autobiographical Writing Since the Sixteenth Century*. Leiden: BRILL.
5. Baić, V., & Deljkić, I. (2019). *Kriminalistička psihologija*. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.
6. Burazer, M. (2019). Kriminalno profilisanje. *Hrvatski ljetopis za kaznene znanosti i praksu*, 26(1), 91–118.
7. Carson, D., & Bull, R. (ur.). *Handbook of Psychology in Legal Contexts*. Chichester: Wiley.
8. Eze, S. M., Alabi, K. J., Ibrahim, S. O., Yusuf, A. O., Hamzat, F. O., Abdulrauf, A., et al. (2025). Forenzička psihologija i kriminalističko profiliranje. *Journal of Forensic Science Research*, 9(1), 092–096.
9. Esherick, J. (2014). *Kriminalistička psihologija i profiliranje ličnosti*. Mason Crest.
10. Gladwell, M. (2007). Dangerous minds. *The New Yorker*, 4. studenog. Prema: Burazer, M. (2019).
11. Modus operandi and 'offender profiling': Some lessons on modern cognitive science for the law of evidence. (2002). *Cardozo Law Review*, 24, 193–285. Prema: Burazer, M. (2019).
12. Pinizzotto, A. J., & Finkel, N. J. (1990). Criminal personality profiling: An outcome and process study. *Law and Human Behavior*, 14(3), 215–233.
13. Rašić, H., Kovačević, D., & Žarković Palijan, T. (2012). Profiliranje počinitelja ubojstava. *Policija i sigurnost*, 2, 277–292.
14. Singer, M., Kovčo Vukadin, I., & Cajner Mraović, I. (2002). *Kriminologija*. Zagreb: Nakladni zavod Globus, str. 65. Prema: Burazer, M. (2019).
15. Snook, B., Cullen, R. M., Bennell, C., Taylor, P., & Gendreau, P. (2008). The criminal profiling illusion: What's behind the smoke and mirrors? *Criminal Justice and Behavior*, 35(10), 1257–1276.
16. Snook, B., Eastwood, J., Gendreau, P., Goggin, C., & Cullen, R. M. (2007). Taking stock of criminal profiling. *Criminal Justice and Behavior*, 34(4), 437–453.
17. Stefoff, R. (2011). *Criminal Profiling*. New York: Marshall Cavendish Corporation.
18. Šeparović, Z. (1981). *Kriminologija i socijalna patologija*. Zagreb: Pravni fakultet u Zagrebu, str. 19–20.

19. Turvey, B. E. (2002). *Kriminalno profiliranje: Uvod u analizu bihevioralnih dokaza*. San Diego: Academic Press.
20. Wrightsman, L. S., Greene, E., Nietzel, M. T., & Fortune, W. H. (2002). *Psychology and the Legal System* (5th ed.). Belmont: Wadsworth.
21. EBSCO Research Starter. Criminal personality profiling. Dostupno na: https://www.ebsco.com/research-starters/science/criminal-personality-profiling (pristupljeno: 10.12.2025).

PSYCHOLOGICAL PROFILING OF PERPETRATORS IN THE FUNCTION OF MODERN CRIME PREVENTION

Abstract: *It can be said that psychological profiling of offenders is one of the most important, yet at the same time one of the least used contemporary methods of crime prevention in the countries of the region. Although this topic is increasingly discussed within the fields of criminal psychology and forensic sciences, its application for preventive purposes remains marginal. Security institutions are still primarily focused on processing crimes that have already been committed, while insufficient attention is paid to the early identification of risk traits, psychological deviations, and behavioral patterns that precede criminal activity. The motivation for analyzing this topic lies in the need to better understand the people around us and to identify individuals whose characteristics may indicate criminogenic potential. At the same time, the aim of this paper is to use writing about criminal personality profiling to help prevent violence and reduce the number of victims, rather than merely focusing on punishment and increasing the prison population. In modern societies, especially those facing rising crime rates, a natural question arises: is each of us a potential offender? The emphasis is not on stigmatization, but on distinguishing between risky and non-risky traits, as well as on understanding the influence of environment, stress, trauma, and predispositions on individual behavior. A major problem in our social context is the neglect of the psychological approach to personality. Police and healthcare structures should possess frameworks of psychological characteristics of individuals in their environment in order to recognize latent offenders, persons with pathological traits, or those developing behavior patterns that may indicate potential violence.*

Key words: *psychological profiling, risk traits, crime prevention, pathological personality traits, latent offenders, criminal psychology.*

SAVREMENA MEDICINA U FUNKCIJI DOKAZIVANJA KRIVIČNIH DJELA

Prof.dr.sci. Adnan Pirić
piricadnan@gmail.com

Rusmir Prohan, dipl.krim.
rusmirprohan22@gmail.com

Sažetak: *Riječ medicina porijeklom je iz latinskog jezika i znači lijek (remedium), a upotrebljava se i izraz ars medicina kao umjetnost liječenja. Zasnovana je dva principa: teorijsko-istraživačkom i praktičnom, ili često nazvanim, kliničkim principom. Zaključena medicinska teorija se putem raznih edukacijskih procesa najčešće provodi u praktični oblik, što će dovesti do konačnog cilja. Sve navedeno čini medicinu spojem naučnog i praktičnog. Medicina kao naučna i praktična disciplina svoju ulogu u polju kriminalistike i krivičnog prava dokazuje kroz sudsko-medicinska vještačenja, čiji je permanentni zadatak otkrivanje i razjašnjavanje objektivnih činjenica kod počinjenih krivičnih djela: tjelesne povrede; utvrđivanje vremena i uzroka smrti, sudsko-medicinska obdukcija leševa; vještačenje dijelova tjela; toksikološka vještačenja; biološka traseologija; makrotragovi i kontaktni mikrotragovi drugog porijekla; genetika nasljeđivanja; postupak indentifikacije, i td... kod otkrivanja krivičnog djela i izvršioca. Razvojem medicine, a posebno Medicinske kriminalistike, uočljiva je njena preokupacija čovječijim životom, njegovom zaštitom i svim krivičnopravnim regulativama koje iz toga proizilaze. Iz navedenog proizilazi potreba za kontinuiranom saradnjom između medicinara, kriminalista i pravnika. Na primjenu forenzičke medicine, ukazuju nam zapisi koji datiraju još od prije 3.000 godina p.n.e., kod Hindusa, gdje je ljekar na dvoru vršio obdukcije, kako bi utvrdio tačan uzrok smrti ili verifikovao eventualne povrede od kojih je vladar podlegao. Takođe, davne (460-377) godine p.n.e. Hipokat je istraživao i pratio tok trudnoće kod žena i proučavao životnu sposobnost nedonoščadi. Mada usporenim hodom nauka je krčila svoj put, zauzimajući mjesto koje joj pripada.*

Ključne riječi*: Medicina, kriminalistika, pravo, otkrivanje, razjašnjavanje i dokazivanje.*

1. UVOD

Savremena medicina predstavlja važan segment forenzičke nauke, koja kombinuje medicinsko znanje kriminalističku i pravnu ekspertizu u cilju otkrivanja, razjašnjavanja i dokazivanja krivičnih djela i njihovih učinilaca. Savremena medicina ima vrlo značajnu, a ponekad i ključnu ulogu u kriminalistici i krivičnom, preciznije krivično-procesnom pravu, osobito forenzička medicina. Njena funkcija nije ograničena samo na liječenje povreda i bolesti, već i na analizu i tumačenje medicinskih nalaza. Savremena (forenzička) medicina, kao spoj medicine kriminalistike i krivičnog prava, doprinosi između ostalog, razjašnjavanju okolnosti nastanka smrti, identifikaciji žrtava, određivanju uzroka povreda, kao i analizi bioloških tragova na mjestu zločina. Obdukcija ili sudsko-medicinska ekspertiza omogućava utvrditi, da li je smrt bila nasilna (ubistvo, samoubistvo, zades) ili prirodna; analiza povreda – ljekari analiziraju vrstu, dubinu, smjer i način zadavanja udarca/povrede, što može pomoći u rekonstrukciji događaja ili identifikaciji oružja/oruđa; DNK analiza – pomoću savremenih

metoda identifikacije moguće je precizno povezati osumnjičene sa žrtvom ili mjestom događaja/zločina; toksiologija – ispitivanje prisustva alkohola, droga, otrova ili drugih supstanci u organizmu, može biti ključno za dokazivanje krivičnih djela izvršenih trovanjem ili silovanjem; psihijatrijsko vještačenje – određuje da li je osumnjičeni bio uračunljiv u trenutku izvršenja djela, te da li je sposoban za suđenje; identifikacija žrtava – kroz analizu otisaka prstiju, DNK, zubne kartoteke/evidencije i drugih biometrijskih podataka; savremene tehnologije u službi pravde; digitalna radiologija (virtuelna autopsija) – omogućava neinvazivno ispitivanje tijela pomoću CT i MRI tehnologije; forenzička genetika – pored klasične DNK analize, koristi se i analiza mitohondrijalne DNK, što je korisno kod starih i degradiranih uzoraka; biometrija i softver za prepoznavanje lica – koriste se u identifikaciji počinilaca i žrtava; telemedicina i mobilne forenzičke jedinice – omogućavaju brzu analizu i slanje nalaza sa terena u centralne laboratorije. Savremena medicinska nauka ima praktični značaj u pravosudnom sistemu, obzirom na činjenicu da medicinska dokumentacija, mišljenje vještaka i drugi nalazi često predstavljaju ključne dokaze u eventualno nastalom sudskom procesu. Objektivnost i stručnost medicinskih vještačenja imaju težinu u procesu otkrivanja, razjašnjavanja i dokazivanja krivičnih djela i njihovih počinilaca, naročito kod ubistava, seksualnih delikata, nasilja u porodici i saobraćajnih nesreća... i mnogih drugih.

2. SAVREMENA MEDICINA U FUNKCIJI DOKAZIVANJA KRIVIČNIH DJELA

Uloga medicine u krimiminalistici i krivičnom pravu (procesnom pravu) postaje sve značajnija, osobito u sferi razjašnjavanja i dokazivanja krivičnih djela i otkrivanja njihovih izvršilaca. Savremena medicina kao multidisciplinarna nauka spaja znanja iz oblasti biologije, hemije, genetike, psihijatrije i kriminalistike, krivičnog i (procesnog) prava u cilju prikupljanja, analize i interpretacije dokaza koji mogu imati odlučujući značaj u krivičnim postupcima koji se vode pred sudovima. Napredak u medicinskoj tehnologiji omogućio je sudskim organima efikasnije otkrivanje/razjašnjavanje istine i identifikaciju počinilaca, naročito kod teških krivičnih djela (ubistva, silovanja, trovanja i druga teška krivična djela i nasilja.. odr).

3. ULOGA SAVREMENE MEDICINE U PRAVOSUĐU

Savremena forenzička medicina primjenjuje se u različitim fazama krivičnog postupka – od uviđaja na mjestu zločina, preko sudsko - medicinskih obdukcija, ekshumacija, do vještačenja u sudskim procesima. Njen osnovni zadatak jeste da pomogne u utvrđivanju: a) uzroka i vremena smrti, b) načina i mehanizma povređivanja, c) identiteta žrtve i/ili počinioca, d) prisustva otrovnih, opojnih i psihoaktivnih supstanci, e) psihičkog stanja osumnjičenog u trenutku izvršenja djela. U svim tim segmentima, forenzički stručnjaci često daju stručno mišljenje koje sud koristi kao dokazni materijal.

3.1. Neke od najčešćih oblasti savremene medicinske ekspertize

3*.1.1. Obdukcija i utvrđivanje uzroka smrti uključujući upotrebu CT-a i MRI-ja*

Sudsko - medicinska obdukcija je osnovna metoda kojom se utvrđuje priroda smrti. Savremeni pristupi uključuju upotrebu CT-a i MRI-ja za tzv. „virtuelne autopsije“, koje se u

novije vrijeme često koriste u Njemačkoj, Švicarskoj, a i djelimično i u Hrvatskoj. CT (kompjuterizovana tomografija) u forenzici. CT koristi rendgenske zrake za pravljenje trodimenzionalnih slika unutrašnjosti tijela. Forenzička primjena mu je u: a) otkrivanje preloma kostiju, npr. lobanje, rebra**;** b) analiza metaka i projektila – identifikacija putanje metka**;** c) povrede unutrašnjih organa**;** d) koristi se prije klasične obdukcije kao dopuna ili alternative. Prednost mu je*:* brza, detaljna, neinvazivna vizualizacija kostiju i stranih tijela. Na nekoliko primjera u praksi su zabilježena istraživanja u kojima je CT (kompjuterizovana tomografija) korišćen u forenzičkoj namjeni — otkrivanje povreda, utvrđivanje uzroka smrti i kao dopuna klasičnoj obdukciji. Nekoliko korisnih primjera iz međunarodne prakse možemo vidjeti u tabeli 1. Ispod:

Metoda	***Predmet analize***	***Značaj CT-a***
"Postmortem CT and autopsy findings in nine victims of terrorist attack"	U napadu eksplozivnim napravama i oružjem, izvršene su CT snimke (PMCT) svih žrtava *prije* obdukcije. CT je otkrio povrede, raspodjelu gelera, putanje projektila, opekline, lomove kostiju itd.	CT je pomogao da se jasno identificiraju i dokumentuju povrede koje su poslije pri obdukciji bile bolje vidljive ili su snimci doprinosili boljoj interpretaciji.
"PMCT in investigation of homicides" (serija sličnih slučajeva)	U 16 slučajeva ubistava analizirana su CT snimanja prije obdukcija (ubodi, udarci oštrim predmetom, udarci tupim predmetom, mecima).	Otkrivanje lomova, praćenje rana, prisustvo zraka u tjelesnim šupljinama (npr. pneumothorax), putanja metaka – sve stvari koje CT može pokazati vrlo precizno, često bolje nego samo klasična obdukcija.
"Useful Evidence by Post-Mortem CT and Stereomicroscopy in Bone Injury — Palermo slučajevi"	Dva slučaja s kostima žrtava koje su bile izložene velikoj šteti — izgorele ili raskomadane. Kombinirana je upotreba PMCT i stereomikroskopije da se razluče toplotne povrede od traumatskih lomova.	PMCT je omogućio vizualizaciju lomova i oštećenja kostiju u 3D, što je pomoglo pri identifikaciji metoda povrede; stereomikroskopija je dopunila CT analizom, naročito u sitnim detaljima lomova.
"Postmortem CT Angiography Compared with Autopsy" (multicentrična studija)	U 500 leševa je urađena CT angiografija (koja oslikava krvne žile) plus klasična obdukcija. Upoređene nalaze su po organima (kost, vaskularni sistem, tkiva).	CT angiografija je otkrila više vaskularnih i koštanih povreda nego što ih je autopsija sama otkrila; posebno kod unutrašnjeg krvarenja i povreda krvnih sudova.

*Tablica 1. Primjeri iz međunarodne prakse korištenja **CT-a**, prilikom obdukcije*

CT — naročito postmortem (PMCT) — nije zamjena za klasičnu obdukciju, ali je velika dopuna, posebno u slučajevima gdje je: tijelo teško pristupačno ili oštećeno, porodica odbija obdukciju, potrebno brzo dobiti pregled povreda prije drugih analiza. CT angiografija (ubacivanje kontrasta i pregledi vaskularnih struktura) može otkriti unutrašnja krvarenja i vaskularne povrede koje obdukcija može previdjeti. Kod slučajeva traumatskih smrti (udarci, saobraćajne nesreće, pucnjava), CT može vrlo jasno pokazati lomove kostiju, putanje projektila, prostornu lokaciju povreda i pomoći u rekonstrukciji događaja. Digitalna dokumentacija CT snimaka (3D rekonstrukcija) je značajna za sud, jer vizuelni materijal često bolje ilustruje povrede, putanje metaka i lokacije lomova nego samo verbalni opis. U 2. Primjera ispod, dat je prikaz nekoliko primjera/slučajeva u vezi sa korištenjem CT-a u sudskoj praksi Bosne i Hercegovine:

*"U jednom primjeru iz prakse u Bosni I Hercegovini tužilac je tražio da vještak dopuni svoj nalaz i mišljenje, nakon što izvrši uvid u CT nalaz (naravno nakon što se pribavi nalaz CT-a**),** jer su postojale određene nedorečenosti/nesuglasice (medicinska dokumentacija*

je tvrdila da postoji prelomi kosti desnog gležnja, dok je RTG pokazao da sa sigurnošću nije moglo biti utvrđeno da je do preloma došlo). Stoga je tužilac smatrao nalaz CT je smatran relevantnim za razjašnjenje te situacije. Što je u konačnici i doprinjelo razjašnjavanju tih nedoumica". Ovo je jedan od primjera koji pokazuje da i sudovi u Bosni i Hercegovini koriste i priznaju CT nalaz kao važan dio/element medicinske dokumentacije koji može ispraviti ili dopuniti ranije vještačenje.

"*U drugom slučaju, riječ je o jednon optužnici protiv ljekara zbog propusta (povreda u saobraćajnoj nezgodi)***.** *Naime u Prijedoru je podignuta optužnica protiv ljekara za kojeg sumnjalo da nije uradio neophodne dijagnostičke pretrage pacijentice povrijeđene u saobraćajnoj nezgodi (među njima, CT glave, mozga i CT grudnog koša) zbog čega nisu uočene određene povrede (prelomi rebara, krvarenja u lobanji), što je razriješilo nedoumice"*. I ovaj drug primjer je dokaz da sudovi u Bosni i Hercegovini svakako smatraju da je CT često neophodan za pravilnu dijagnostiku povreda, posebno unutrašnjih i složenijih slučajeva.

3.1.2. MRI (magnetna rezonanca) u forenzici

MRI koristi magnetno polje i radio-talase za prikaz mekih tkiva, bez zračenja. Forenzička primjena mu je u: a) otkrivanje povreda mozga, kičme, mišića; b) detekcija gušenja ili moždanih trauma koje nisu vidljive izvana; c) procjena stanja srca, jetre, bubrega – korisno u sumnjivim smrtnim slučajevima. MRI (magnetna rezonanca) u forenzici koristi se za detaljnu analizu mekih tkiva bez upotrebe jonizujućeg zračenja, što je naročito korisno kada su povrede nevidljive izvana ili teško uočljive klasičnim obdukcijama ili RTG/CT pregledima. Najčešća upotreba MRI-a u savremenoj medicine, prilikom otkrivanja, razjašnjavanja i dokazivanja krivičnih djela je u sljedećem:

1. Otkrivanje unutrašnjih povreda**,** što podrazumjeva, najčešće, intrakranijalna krvarenja (npr. subduralni hematom), zatim oštećenje mozga kod trauma ili gušenja te povrede mišića i unutrašnjih organa koje nisu uočljive na spoljašnjem pregledu.
2. Ispitivanje uzroka smrti kod djece i dojenčadi jer, sudska MRI može otkriti znakove sindroma tresene bebe, male frakture lobanje, hematome. Ova primjena je od izuzetne koristi u slučajevima kada klasična obdukcija nije prihvatljiva (etika, religija npr…).
3. Analiza u slučajevima smrti gušenjem**,** kada nam MRI može pokazati edem pluća, otok mozga, natečenost jezika i sluznica — znake asfiksije; ili
4. Sudski predmeti povezani sa mučenjem ili batinanjem, što može da pomgne prilikom otkrivanja povreda dubokih slojeva tkiva, koje nisu odmah vidljive, kao što su unutrašnja krvarenja u mišićima, hematomi, ruptura tetiva itd. U tablici 2. Ispod, ukazano je na nekoliko prednosti MRI u sudsko medicinskoj forenzici:

Prednost	**Objašnejnje**
Bez zračenja	Sigurno za osjetljive slučajeve i trudnice
Detaljan prikaz mekih tkiva	Bolji od CT za mozak, mišiće, leđnu moždinu
Neinvazivna metoda	Koristi se i kada je obdukcija nepoželjna ili nedostupna
Može otkriti „nevidljive" povrede Idealno za slučajeve gušenja, zlostavljanja, utapanja	

Tablica 2. Prednosti MRI u sudsko medicinskoj forenzici

Kada govorimo o praktičnoj primjeni MRI kroz primjere iz međunarodne prakse, ovdje bi bi bilo veoma poželjno istaći neke od međunarodnih studija, kao što je: Studija: *Post-mortem MRI in detection of brain injuries in children, u kojem slučaju je MRI* identifikovao subduralne hematome, kontuzije i cerebralni edem kod umrle dojenčadi – sve što nije bilo lako uočiti klasičnim pregledom. Zatim primjer u kojem je MRI je omogućio dijagnozu zlostavljanja djece, što je bilo ključno za krivični postupak. Što se tiče Bosne i Hercegvoine, upotreba MRI u praktičnoj primjeni po pitanju sudsko medicinske forenzičke prakse nije na "zavidnom" nivou, međutim, važno je istaći da se MRI se rutinski koristi u kliničkom kontekstu za život pacijenata, ali se u forenzičkoj praksi još ne koristi sistemski kao postmortem alat (*virtopsy*)**.** Postoji potencijal za uvođenje u slučajevima: a) sumnjivih smrti; b) vjerskih prigovora na klasičnu obdukciju i u slučajevima c) dokumentovanja torture ili zlostavljanja. Generalno promatrajući, radiologija i 3D CT-a, MRI rekonstrukcija, kao Savremene metode poput digitalne autopsije (virtopsy), najčešća se primjenjuju u: a) rekonstrukcijama uzroka smrti; zatim b) Identifikacija povreda (npr. ulazno/izlazne rane od vatrenog oružja) ili c) virtualnoj obdukcija bez invazivnih postupaka (važna u slučajevima religijskih ili etičkih prepreka). Savremene metode kao što su CT, MRI i digitalna autopsija (virtopsy) značajno su unaprijedile forenzičku medicinu i omogućile neinvazivno razjašnjavanje uzroka smrti, što je posebno važno u slučajevima osjetljivih krivičnih djela (npr. ubistava, mučenja). Digitalna autopsija (Virtopsy) što u stvari pretstavlja kombinaciju CT + MRI + 3D rekonstrukcija + digitalna analiza (softverom), je potpuno neinvazivna metoda obdukcije, često se koristi kada, porodica odbija klasičnu obdukciju iz religijskih/etičkih razloga. Tijelo je značajno oštećeno ili opasno za fizički kontakt (npr. zarazne bolesti), a najčešće se primjenjuje, prilikom analiza povreda bez otvaranja tijela, procjena vremena smrti i kao forenzička dokumentacija (digitalni dosjei, 3D modeli važni za sudski postupak). Neizostavno je napomenuti da se ova metoda koristi se i u edukaciji, simulacijama i ponovnim analizama slučajeva.

Slika 1. primjer digitalne autopsije, poznate kao Virtopsy

Digitalna autopsija, poznata i kao Virtopsy, predstavlja suvremeni pristup obdukciji koji koristi napredne slikovne tehnologije poput računalne tomografije (CT), magnetske rezonancije (MRI) i 3D skeniranja za neinvazivnu analizu tijela preminule osobe. Ovaj pristup omogućava detaljno vizualiziranje unutarnjih i vanjskih ozljeda bez potrebe za fizičkim otvaranjem tijela, što je osobito korisno u slučajevima gdje je očuvanje integriteta tijela ključno ili kada je tradicionalna obdukcija nepraktična. Važno je istaći još nekoliko ključnih komponennti Virtopsy metode, kao što je: 3D optičko skeniranje: ovo skeniranje se koristi se za precizno dokumentiranje vanjskih obilježja tijela, uključujući ožiljke, modrice i

druge vanjske ozljede. Zatim Multislice spiralna CT (MSCT**)**: koja omogućava detaljno vizualiziranje unutarnjih struktura tijela, uključujući kosti, organe i prisutnost stranih objekata. Isto tako MRI**:** Pruža visokokvalitetne slike mekih tkiva, što je korisno za identifikaciju unutarnjih ozljeda ili bolesti. I post-mortem angiografija: koja koristi kontrastna sredstva za vizualizaciju krvnih žila, što pomaže u otkrivanju unutarnjih krvarenja ili vaskularnih ozljeda. Prednosti Virtopsy metode su: neinvazivnost što mogućava detaljnu analizu bez fizičkog otvaranja tijela. Objektivnost što nam omogućava da slikovne tehnologije smanjuju subjektivnost u interpretaciji nalaza. Dokumentacija koja omogućava da svi podaci budu digitalno pohranjeni, što olakšava kasniju analizu ili reviziju. Primjena u različitim kontekstima**,** što znači da se koristi se u forenzičkim istragama, medicinskim istraživanjima i obrazovanju. Ograničenja i izazovi: Tehnička ograničenja: Neke ozljede ili bolesti mogu biti teško uočljive pomoću slikovnih tehnologija. Trošak**:** Visoka cijena opreme i održavanja može biti prepreka za široku primjenu. Pravna prihvaćenost: U nekim jurisdikcijama, rezultati virtopsije možda neće biti prihvaćeni kao zamjena za tradicionalnu obdukciju u sudskim postupcima.

Primjena u Bosni i Hercegovini

Iako Virtopsy metoda pokazuje potencijal u forenzičkim istragama, njezina primjena u Bosni i Hercegovini još uvijek nije široko rasprostranjena. Nedostatak specijalizirane opreme i obuke može ograničiti njezinu implementaciju. Međutim, s obzirom na prednosti koje pruža, postoji mogućnost da će se u budućnosti razmotriti njezina uvođenja u forenzičke institucije u zemlji.

Primjeri iz prakse

Forenzički centri u Švicarskoj, Njemačkoj i SAD-u već redovno koriste virtopsy u krivičnim istragama. U BiH, CT i MRI se već koriste u nekim sudsko-medicinskim centrima, posebno u većim kliničkim centrima (UKC Sarajevo, Tuzla, Banja Luka), dok virtopsy još nije standardizovan ali je uvođenje moguće u saradnji s međunarodnim partnerima.

3.2. Forenzička genetika – DNK analiza

Najvažnije i najpouzdanije dostignuće moderne forenzike. Primjena:

a) identifikacija počinioca ili žrtve (DNK iz krvi, dlake, sluzi, kože itd.);

b) povezivanje osumnjičenih sa mjestom zločina;

c) isključenje nevinih osoba.

Tehnike:

a) STR analiza (short tandem repeats) (Short Tandem Repeat analysis) je savremena forenzička metoda analize DNK koja se koristi za identifikaciju osoba na osnovu ponavljajućih sekvenci DNK (kratkih tandemskih ponavljanja). Ova metoda je zlatni standard u forenzičkoj genetici širom svijeta, uključujući i Bosnu i Hercegovinu.

b) Y-STR za analizu muških DNK tragova Y-STR analiza je posebna vrsta DNK analize koja se fokusira na short tandem repeats (STR) koji se nalaze isključivo na Y hromosomu**,** tj. muškoj liniji nasljeđivanja.

Ova metoda je izuzetno korisna u forenzičkoj genetici, posebno kada je potrebno analizirati muške biološke tragove u mješovitim uzorcima. mtDNA analiza za stare i oštećene uzorke (posebno u ratnim zločinima) Mitohondrijska DNK nalazi se u mitohondrijima, a nasljeđuje se isključivo po majčinskoj liniji (majka → dijete). Svaka ćelija sadrži stotine do hiljade

kopija mtDNA, za razliku od samo dvije kopije nuklearne DNK. Zbog toga je otpornija na razgradnju i može se analizirati i kada je obična DNK neupotrebljiva. Forenzička genetika – DNK analiza je ključna metoda u savremenom krivičnom postupku, jer omogućava direktno povezivanje osumnjičenih s krivičnim djelom. U nastavku dajemo konkretan primjer iz prakse, na stvarnim postupcima u kojima je DNK igrao odlučujuću ulogu.

Metoda	Tehnička osnova	Forenzička primjena	Primjeri iz prakse (BiH/regija)
STR analiza DNK	Kratki tandem ponavljanja	Identifikacija počinioca ili žrtve	Identifikacija u ratnim zločinima (ICMP)
Y-STR analiza	DNK s Y-hromosoma	Muška komponenta DNK u mješanim uzorcima	Silovanja, DNK sjemene tečnosti
mtDNA analiza	Mitohondrijska DNK (po majci)	Stari/razgrađeni uzorci, identifikacija	Masovne grobnice – žrtve rata u BiH
NGS (sekvenciranje nove generacije)	Visoko-protočno sekvenciranje	Kompleksni uzorci, više osoba	Napredna analiza ratnih i masovnih zločina
Virtopsy (digitalna autopsija)	CT + MRI + 3D modeliranje	Neinvazivno utvrđivanje uzroka smrti	Smrt u pritvoru, religijski prigovori na obdukciju
3D lasersko skeniranje	Lidar/laserski skener	Rekonstrukcija mjesta zločina	Vizualizacija zločina za Sud BiH
Bihevioralna forenzika (AI)	Analiza mikroizraza, govora tijela	Procjena iskaza i sumnjivog ponašanja	Paravinja, nestanci osoba, ispitivanja
Toksikološka analiza (HR-MS)	Spektrometrija mase visoke rezolucije	Otkrivanje droga, otrova, lijekova	Smrti zbog fentanila, alkohol + lijekovi
Forenzička biometrija	Prepoznavanje lica, otisaka, hoda	Identifikacija sa video snimaka	Pljačke, ubistva – analiza nadzornih snimaka
Epigenetska analiza	Mjerenje DNK modifikacija	Starost, navike, stres profili	Istraživanja u razvoju – buduća primjena u BiH

Tablica 3. Prednosti DNK-a u sudsko medicinskoj forenzici

Mogu se koristiti u postupcima gdje je potrebno utvrditi:
a) da li je osumnjičeni bio uračunljiv
b) postoji li duševni poremećaj (npr. kod femicida, serijskih ubistava);
c) kognitivne sposobnosti svjedoka (posebno djece)

3.4. Biometrija i analiza ponašanja

Prepoznavanje lica, otisaka prstiju, dužice oka, pa čak i načina hoda. Koristi se u videoanalizi zločina (npr. napada, pljački)[1]. Kombinuje se sa vještačenjem digitalnih tragova (mobiteli, GPS, kamere. Analiza ponašanja se fokusira na proučavanje načina djelovanja osobe – kako se kreće, komunicira ili reagira – kako bi se identificirali sumnjivi ili kriminalni obrasci. Tehnike i primjene:
a) Profiliranje počinitelja, kombinacija psiholoških, socijalnih i kriminalističkih podataka. Cilj: predvidjeti moguće ponašanje počinitelja i profilirati njegovu ličnost.
b) Analiza video nadzora, praćenje neobičnog ponašanja, sumnjivih pokreta ili rutinskih odstupanja, upotreba algoritama za prepoznavanje abnormalnih obrazaca kretanja.
c) Analiza internetskog ponašanja, praćenje online aktivnosti, poruka, društvenih mreža, Identifikacija cyber-kriminala, prijetnji ili radikaliziranih osoba**.**

[1] U Bosni i Hercegovini su već zabilježeni slučajevi primjene ove metode identifikacije izvršioca i na osnovu, između ostalog, biometrijskog nalaza vještaka, doneseno je nekoliko pravomoćnih sudskih presuda.

d) Detekcija laganja i stresa**,** Kombinacija biometrijskih podataka (puls, glas, mikroizrazi lica) i ponašanja. Primjena u ispitivanjima ili sigurnosnim provjerama.

3.4.1. Integracija biometrije i analize ponašanja

Kombinacija ovih metoda omogućava sveobuhvatan pristup u otkrivanju krivičnih djela: Biometrija osigurava identitet počinitelja. Analiza ponašanja daje kontekst i motive**,** što pomaže u prevenciji i predviđanju kriminala. Na primjer:

a) automatska detekcija sumnjivih osoba na aerodromima ili u javnom prijevozu.

b) kombinacija nadzornih kamera i prepoznavanja lica u borbi protiv terorizma.

c) analiza online obrazaca komunikacije za otkrivanje pedofilije ili prevarantskih mreža.

U nastavku pregledna tablica, koja jasno prikazuje različite biometrijske metode **i** metode analize ponašanja u kontekstu otkrivanja krivičnih djela:

Metoda	**Opis / Tehnika**	**Prednosti**	**Ograničenja**	**Primjeri primjene u kriminalistici**
Iris / skeniranje oka	Prepoznavanje jedinstvenih uzoraka irisa ili mrežnice	Izuzetno precizno, teško za lažiranje	Skupo, osjetljivo na svjetlosne uvjete i udaljenost	Sigurnosni sistemi, kontrola pristupa u visokorizičnim objektima
Prepoznavanje lica	Analiza geometrije lica i ključnih točaka	Brzo prepoznavanje u javnim prostorima	Moguće pogreške kod maski, promjene izgleda ili osvjetljenja	Nadzor u javnim prostorima, identifikacija osumnjičenih
Glasovna identifikacija	Analiza frekvencijskih i tonalnih karakteristika glasa	Može raditi na daljinu, neinvazivno	Promjene glasa, buka okoline, imitacije	Telefonske prijetnje, online prijetnje
Analiza video nadzora	Praćenje pokreta i neobičnog ponašanja u javnim prostorima	Brza detekcija sumnjivih aktivnosti	Veliki volumen podataka, pogrešne detekcije	Aerodromi, javni prijevoz, sigurnost događaja
Analiza internetskog ponašanja	Praćenje online aktivnosti, komunikacije i društvenih mreža	Omogućava otkrivanje cyber-kriminala	Privatnost, šifrirane komunikacije	Cyber prevara, pedofilija, radikalizacija

Tablica 4. Prednosti biometrije u analizi ponašanja

3.5. Ostale savremene forenzičke metode

Prethodna elaboracija savremenih medicinskih dostignuća i njihovog značaja u kriminalistici i krivičnom pravu dokazuje nedvojbeno da savremena medicina, posebno u svom forenzičkom segmentu, predstavlja nezamjenjiv alat u borbi protiv svih oblika kriminala. U vezi s tim u nastavku ćemo dati kraći osvrt i na druge (ostale) savremene forenzičke metode značajne za krivični postupak.

3.5.1. Forenzička mikrobiologija

Koristi mikrobiom (bakterije) iz tijela da:

a) odredi vrijeme smrti (PMI – postmortem interval),

b) analizira tragove iz specifičnih tijela (npr. pluća, creva) radi otkrivanja infekcija, gušenja, utapanja itd.

Forenzička mikrobiologija je primjena mikrobioloških metoda i tehnika u kontekstu pravne i krivične istrage. Osim što se koristi za otkrivanje i identifikaciju patogena, ova disciplina pomaže u:
a) utvrđivanju uzroka smrti,
b) vremenu smrti (postmortalni interval – PMI),
c) identifikaciji mjesta zločina,povezivanju osumnjičenih s dokazima ili žrtvama i
d) istraživanju bioterorističkih napada.
- Primjena u kriminalistici:
a) Postmortalni mikrobni tragovi (mikrobiom smrti) nakon smrti, ljudski mikrobiom (npr. bakterije u crijevima, ustima, koži) počinje da se mijenja u predvidljivim fazama. Analizom promjena u mikrobnoj zajednici moguće je:
b) preciznije procijeniti vrijeme smrti, posebno kada su klasične metode nepouzdane.
b) razlikovati mjesto smrti od mjesta pronalaska tijela, jer mikrobiološka sredina može otkriti premještanje.

3.5.1.1. Forenzička analiza tla i okoliša

Bakterijske zajednice u tlu i vodi su različite u zavisnosti od lokacije. Mikrobiološkim poređenjem tragova tla na osumnjičenom (npr. obući) sa onima sa mjesta zločina može se utvrditi njihova povezanost. Ova metoda korištena je i u Bosni i Hercegovini u slučajevima krivičnih djela terorizma i nekih drugih teških krivičnih djela.

3.5.1.2. Bioterorizam i mikrobiološki napadi

Ovo je jedna od najvažnijih grana forenzičke mikrobiologije. U slučajevima namjernog puštanja patogena (npr. *Bacillus anthracis* – uzročnik antraksa), forenzička mikrobiologija koristi genetske metode za identifikaciju porijekla sojeva, čime se otkrivaju izvori i mogući počinioci.

3.5.1.3. Identifikacija osumnjičenih preko mikrobioma

Svaka osoba ima jedinstveni mikrobiom. Mikrobi sa kože, usta ili crijeva koji ostanu na površinama (npr. tastatura, telefon, odjeća) mogu se koristiti za identifikaciju prisustva određene osobe na mjestu zločina.
Napomena**:** Ova metoda je još u fazi istraživanja i nije široko prihvaćena u sudskoj praksi zbog nedostatka standardizacije.
Izazovi i pravna prihvatljivost**:** iako ima ogroman potencijal, postoje izazovi u primjeni forenzičke mikrobiologije u pravosudnom sistemu:
a) još uvijek nema standardizovanih protokola, posebno za mikrobiom,
b) potrebna je visoka stručnost za interpretaciju rezultata,
c) Prihvatljivost dokaza pred sudom može biti osporena zbog novosti metode.

3.5.1.4. Digitalna forenzika u analizi rana

Ovdje je vrlo korisno pomenuti sljedeće metode: 3D modelovanje rana radi poređenja s mogućim oružjem i Softverske simulacije udaraca.
Pravni značaj i validnost metoda:
a) metode moraju biti naučno validirane, da bi bili prihvaćeni kao dokaz na sudu,

b) DNK, toksikološke analize i radiološki nalazi imaju visoku dokaznu vrijednost i
c) metode poput "bite mark analysis" sve se rjeđe koriste zbog sumnjive tačnosti.

3.5.2. Metode analize u toksikologiji

Screening (pretraga prisustva supstanci):

a) imunotestovi (brzi testovi na droge i alkohol),

b) Tankoslojna hromatografija (TLC).

Konfirmatorne metode (tačne kvantifikacije):

a) GC-MS (gasna hromatografija s masenom spektrometrijom),

b) LC-MS/MS (tečna hromatografija s masenom spektrometrijom),

c) AAS (atomska apsorpciona spektrometrija) – za detekciju metala

Toksične doze i interpretacija nalaza:

a) važno je razlikovati prisustvo od toksične koncentracije**,**

b) neke supstance mogu biti prisutne, ali ne i uzrok smrti (npr. terapijske doze lijekova),

c) određene kombinacije droga (npr. alkohol + benzodiazepini) mogu imati sinergijski toksični efekat**.**

Posebni slučajevi trovanja u kriminalistici;

a) trovanje cijanidom **(**Smrt nastupa brzo. Detekcija je moguća iz krvi i tkiva. Tipičan miris gorkog badema (kod osjetljivih osoba),

b) trovanje ugljen-monoksidom (Često u slučaju požara ili loše ventilacije. Krv ima jarko crvenu boju zbog karboksihemoglobina).

c) Zloupotreba lijekova (zloupotreba lijekova za spavanje, sedativa, antidepresiva je sve češći uzrok nesreća i smrti).

d) "Date rape" droge (droge za silovanje) (supstance poput GHB, Rohypnol – brzo se metabolizuju i teško detektuju → analiza mora biti brza).

Toksikološki nalazi kao dokaz na sudu:

a) moraju biti izrađeni od strane ovlaštenih laboratorija**,**

b) Izvještaji uključuju: supstancu, koncentraciju, moguće djelovanje, uzrok smrti,

c) **v**ještaci toksikolozi tumače nalaze pred sudom.

4. ZAKLJUČAK

Savremena medicina značajno doprinosi efikasnijem krivičnom postupku. Forenzički metodi omogućavaju precizno utvrđivanje činjenica koje su često odlučujuće u dokazivanju krivice ili nevinosti. Tehnološki napredak i stalna edukacija stručnjaka iz oblasti forenzičke medicine čine ovu oblast ključnim segmentom u savremenom sistemu. Zemlje regiona, iako sa ograničenim resursima, sve više ulažu u forenzičke kapacitete, što doprinosi boljem funkcionisanju pravosuđa i jačanju vladavine prava. Savremena medicina, posebno u svom forenzičkom segmentu, predstavlja nezamjenjiv alat u borbi protiv svih oblika kriminala. Njena uloga nije samo pomoćna, već često presudna u otkrivanju istine i ostvarivanju pravičnosti krivičnog postupka. Kontinuirani razvoj tehnologije i obrazovanja u ovoj oblasti osigurava sve veću efikasnost u procesima otkrivanja, razjašnjavanja I dokazivanja krivičnih djela. Trenutna ograničena primjena pojedinih metoda zbog skupog postupka ne treba

obeshrabriti, a najbolji dokaz za to da je i DNK analiza nekada bila veoma rijetko korištena, a danas je gotovo svakodnevna, čak i za krivična djela manje važnosti i težine.

5. IZVORI I KORIŠTENA LITERATURA

1. ICMP.org. (2020). *Forensic Science and the Identification of Missing Persons*.
2. Zakon o krivičnom postupku RS, FBiH, RH – čl. 118–130 (vještačenje).
3. Javan, G. T., Finley, S. J., Can, I., et al. (2023). *The thanatomicrobiome: a missing piece of the microbial puzzle of death*. Frontiers in Microbiology.
4. Metcalf, J. L., et al. (2023). *A microbial clock provides an accurate estimate of the postmortem interval in a mouse model system*. eLife.
5. Madea, B. (2019). *Estimation of the time since death*. CRC Press.
6. Madea, B. (2019). *Estimation of the Time Since Death*. CRC Press.
7. Saukko, P., & Knight, B. (2004). *Knight's Forensic Pathology*.
8. Baselt, R. (2020). *Disposition of Toxic Drugs and Chemicals in Man*.
9. WHO & UNODC izvještaji o drogama i trovanjima.

MODERN MEDICINE IN THE FUNCTION OF PROVING CRIMINAL OFFENCES

Summary: *The word medicine originates from the Latin language and means medicine (remedium), and the expression ars medicina is also used as the art of healing. It is based on two principles: theoretical-research and practical, or often called, clinical principle. The concluded medical theory is most often implemented into a practical form through various educational processes, which will lead to the final goal. All of the above makes medicine a combination of the scientific and the practical. Medicine as a scientific and practical discipline proves its role in the field of criminology and criminal law through forensic medical examinations, whose permanent task is to discover and clarify objective facts in committed criminal offenses: bodily injuries; determining the time and cause of death, forensic medical autopsy of corpses; expert examination of body parts; toxicological expert examinations; biological traceology; macrotraces and contact microtraces of other origin; genetics of inheritance; identification procedure, etc. in detecting a criminal act and its perpetrator. With the development of medicine, and especially Medical Criminology, its preoccupation with human life, its protection and all the criminal law regulations that arise from it is noticeable. From the above, the need for continuous cooperation between physicians, criminologists and lawyers arises. The application of forensic medicine is indicated by records dating back to 3,000 years BC, among the Hindus, where the court physician performed autopsies in order to determine the exact cause of death or verify any injuries from which the ruler succumbed. Also, in the distant past (460-377) BC. Hippocrates researched and monitored the course of pregnancy in women and studied the viability of premature babies. Although science has been slowly making its way, taking its rightful place.*

Keywords: *Medicine, criminology, law, discovery, clarification and proof.*

PRAKTIČNA PRIMJENA OSINT METODA U ISTRAŽIVANJU ORGANIZIRANIH KRIMINALNIH GRUPA

Dr. Emir Muhić
emirmuhic@fkn.unsa.ba

Sažetak: *savremene organizirane kriminalne grupe (OKG) djeluju u prostoru koji je istovremeno fizički i digitalni, pri čemu njihovo kriminalno ponašanje generira značajne javno dostupne informacijske tragove. Iako digitalni prostor postaje centralno operativno okruženje savremenog kriminalnog djelovanja, metode prikupljanja obavještajnih podataka iz otvorenih izvora (OSINT) u praksi krim-obavještajnog rada, kao i u akademskim istraživanjima, ostaju nedovoljno konceptualizirane i rijetko razmatrane kao zaseban analitički pristup. Posebno je izražen nedostatak stručnih i naučnih radova koji OSINT sistematski sagledavaju kao operativni alat u istraživanju organiziranih kriminalnih grupa. Cilj ovog rada je prikazati praktičnu i analitičku upotrebu OSINT metoda u identifikaciji, mapiranju i praćenju OKG, sa fokusom na njihovu primjenu u različitim fazama istražnog postupka. U radu se identifikuju ključni OSINT izvori, relevantne analitičke metode i predlažu osnovni modeli primjene OSINT-a u krim-obavještajnom radu, s ciljem unapređenja razumijevanja i operativne upotrebe otvorenih izvora u suzbijanju organiziranog kriminala.*

Ključne riječi*: OSINT, organizirane kriminalne grupe, kriminalističko-obavještajni rad, analiza mreža*

1. UVOD

Organizirane kriminalne grupe (OKG) u savremenom sigurnosnom okruženju prolaze kroz kontinuirane strukturne i operativne transformacije, uslovljene razvojem digitalnih tehnologija i širenjem online komunikacijskih prostora. Kriminalno djelovanje više se ne odvija isključivo unutar zatvorenih fizičkih mreža i neposrednih kontakata, već se u značajnoj mjeri prepliće sa digitalnim okruženjem u kojem nastaju brojni javno dostupni informacijski i digitalni tragovi. Takvi tragovi, iako često nenamjerni, predstavljaju važan izvor podataka za analitičko sagledavanje strukture, dinamike i aktivnosti organiziranog kriminala. Tradicionalne kriminalističke metode i istražne radnje ostaju temelj suzbijanja organiziranog kriminala, ali su istovremeno opterećene proceduralnim, vremenskim i pravnim ograničenjima, kao i problemima koji mogu nastati njihovim neadekvatnim provođenjem. Posebno u ranim fazama postupanja, istražni organi se suočavaju sa nedostatkom strukturiranih informacija koje bi omogućile brzo prepoznavanje ključnih aktera, njihovih međusobnih odnosa i obrazaca djelovanja. U tom kontekstu, open source intelligence metode se nameću kao praktičan i fleksibilan alat koji omogućava inicijalnu analitičku pripremu bez neposredne primjene invazivnih mjera. OSINT podrazumijeva sistematsko prikupljanje i analizu informacija iz javno dostupnih izvora, uključujući društvene mreže, javne registre, medijske sadržaje i druge otvorene digitalne platforme. Kada se primjenjuje planski i metodološki, OSINT omogućava identifikaciju društvenih mreža, obrasce ponašanja i indikatora kriminalnih aktivnosti koji mogu ostati nevidljivi kroz klasične operativne kanale. Članovi organiziranih kriminalnih grupa, kroz javno eksponiranje načina života, poslovnih aktivnosti ili društvenih veza, često ostavljaju informacijske fragmente koji se mogu

analitički povezati u širu sliku kriminalne strukture. Poseban značaj OSINT metode imaju u istraživanju organiziranog kriminala, gdje rana situaciona procjena i kvalitetna analitička priprema predstavljaju ključ za efikasno usmjeravanje daljih istražnih aktivnosti. OSINT može poslužiti za preliminarno mapiranje kriminalnih mreža, identifikaciju prioritetnih ciljeva, kao i za prepoznavanje finansijskih i imovinskih indikatora povezanih sa kriminalnim prihodima. Međutim, njegova stvarna vrijednost zavisi od pravilnog pozicioniranja unutar kriminalističko-obavještajnog ciklusa i integracije sa klasičnim istražnim metodama.

2. OPEN SOURCE INTELLIGENCE KAO ANALITIČKI I OPERATIVNI OKVIR

Savremeni kriminalistički i obavještajni rad sve se više oslanja na informacije koje nastaju izvan zatvorenih institucionalnih sistema, pri čemu digitalno okruženje proizvodi kontinuirani tok javno dostupnih podataka o pojedincima, organizacijama i društvenim procesima. Takvo okruženje zahtijeva razvoj metodoloških pristupa koji omogućavaju sistematsko prikupljanje, selekciju i analizu informacija koje su već prisutne u javnom prostoru, ali su često fragmentirane, nestrukturirane i bez neposredne analitičke vrijednosti. U tom kontekstu, OSINT se afirmiše kao okvir koji omogućava pretvaranje otvorenih informacija u smislen analitički uvid. Suštinski se OSINT definiše kao proces sistematskog prikupljanja, analiziranja i korištenja informacija koje su dostupne iz otvorenih i legalnih izvora, uključujući internetske stranice, javne registre, baze podataka, medijske sadržaje, društvene mreže, forume i druge oblike digitalne prisutnosti, bez korištenja invazivnih i penetracijskih metoda[2]. OSINT izvori podataka obuhvaćaju gotovo sve što možete pronaći na Internetu, od IP adrese do javnih državnih zapisa (EU4Justice, 2021). Ovakvo određenje ukazuje na širok spektar potencijalnih izvora, ali istovremeno nameće potrebu za jasnim metodološkim okvirom kako bi se izbjeglo nekritičko prikupljanje podataka bez analitičke svrhe. Ključna karakteristika OSINT-a je činjenica da se oslanja isključivo na informacije koje su javno dostupne, odnosno već se nalaze u online prostoru objavljene od autora ili posrednika, te su zakonito pribavljene, bez potrebe za posebnim ovlaštenjima, tajnim nadzorom ili upotrebom specijalnih tehničkih sredstava. OSINT je čisto pasivna metoda koja ne koristi penetraciju i aktivno izviđanje (Baker, 2023). Upravo ova pasivna priroda čini OSINT posebno pogodnim za rane faze krim-obavještajnog rada, u kojima je cilj razumijevanje konteksta, identifikacija aktera i mapiranje odnosa, a ne neposredno pribavljanje dokaznog materijala. OSINT se definiše kao obavještajni proizvod "nastao iz javno dostupnih informacija koje se prikupljaju, eksploatišu i distribuiraju na pravovremen način odgovarajućoj ciljnoj publici, s ciljem ispunjavanja specifičnog obavještajnog zahtjeva" (Lowentha & Clark, 2015). Ovakvo normativno određenje jasno pozicionira OSINT kao sastavni dio institucionalizovanog obavještajnog ciklusa, a ne kao neformalnu ili pomoćnu aktivnost. Unutar šireg OSINT okvira, poseban značaj imaju obavještajni izvori iz društvenih medija (Social Media Intelligence - SOCMINT), koji se fokusira na prikupljanje i analizu podataka generisanih kroz društvene mreže i digitalne komunikacijske platforme, čime se

[2] U ovom slučaju kontekst je na agresivne metode neovlaštenog pristupa štićenim sistemima i informacijama. Dakle, ukoliko se provode akivne operacije neovlaštenog proboja štićenih sistema, laički rečeno hakovanje, navedeno nije OSINT. Samo informacije i podaci koji su javno dostupni i aktivnosti i metode koje se mogu ponoviti od treće osobe i dovedu do istog podatka su OSINT.

otvara prostor za razumijevanje dinamičnih društvenih procesa u realnom vremenu. SOCMINT metode mogu uključivati pasivno „slušanje“ sadržaja (tzv. social media listening) i aktivno mapiranje korisničkih mreža.

3. Organizirane kriminalne grupe u digitalnom okruženju

2.1. Digitalni prostor i vidljivost kriminalnih mreža

Digitalizacija kriminalnih aktivnosti proizvela je paradoksalan efekat u kojem se istovremeno povećavaju i prikrivenost i analitička dostupnost određenih oblika organiziranog kriminala. Iako se internet često navodi kao najveći facilitator trgovine ljudima, on istovremeno pruža i mogućnost posmatranja trgovine ljudima koja ranije nije postojala, čineći mnoge aspekte ove pojave vidljivijima (Boyd, Casteel, Thakor, & Johnson, 2011). Upravo oslanjanje na internet kao primarnu komunikacijsku i koordinacijsku infrastrukturu dovodi do toga da kriminalne zajednice, uprkos nastojanjima da ostanu skrivene, proizvode raspršene digitalne tragove koji ostaju trajno prisutni u online prostoru. Korištenje online podataka prikupljenih sa web stranica, diskusionih grupa ili drugih foruma predstavlja rastući trend u istraživanjima devijantnog ponašanja (Durkin, Forsyth, & Quinn, 2006). Zbog kriminalne prirode ovih aktivnosti, prikrivene mreže se formiraju s ciljem olakšavanja operacija i izbjegavanja djelovanja organa za provođenje zakona. Sparrow (1991) te Xu i Chen (2005) zagovaraju primjenu mrežne analize u proučavanju prikrivenih i kriminalnih grupa. Analiza društvenih mreža (Social Network Analysis - SNA) pruža okvir, metode i alate za provođenje sofisticirane mrežne analize, omogućavajući empirijsko mjerenje i vizualizaciju različitih mreža, uključujući i tzv. tamne mreže (Mainas, 2012). Ovakva kombinacija digitalne vidljivosti i organizacijske zatvorenosti kriminalnih mreža ne predstavlja samo metodološki izazov za istražitelje, već ima i šire sigurnosne implikacije koje prevazilaze klasično krivičnopravno razumijevanje organiziranog kriminala. Upravo zbog toga, analiza digitalnih tragova, mrežnih struktura i online komunikacija ne može ostati ograničena na nivo pojedinačnih kriminalnih aktivnosti. To se mora posmatrati u kontekstu savremenih bezbjednosnih uslova u kojima se granice između kriminala, politike, ekonomije i informacija sve više brišu.

2.2. Organizirani kriminal kao hibridna prijetnja

U savremenim bezbjednosnim uslovima, hibridne prijetnje koje uključuju kriminalne radnje i aktivnosti, od krijumčarenja ljudi, narkotika i oružja, terorizma, dezinformacija do cyber napada, koriste digitalni prostor kao operativno okruženje. Na visokom nivou organizirane kriminalne grupe su zapravo hibridne prijetnje (Makarenko, 2010), i kao takve zaslužuju posebnu pažnju cjelokupnog sistema nacionalne sigurnosti. OKG postaju instrumenti takvih prijetnji, posebno u kontekstu globalnih kriza koje povećavaju institucionalnu ranjivost (EUROPOL, 2025). Zbog toga se organizirani kriminal ne može posmatrati isključivo kao autonomni oblik protivpravnog djelovanja usmjerenog na ostvarivanje finansijske koristi, već kao fleksibilan akter koji se prilagođava širim strateškim interesima i sigurnosnim poremećajima, a digitalne tehnologije postaju ključni resurs za upravljanje kriminalnim tržištima. Dakle, digitalni prostor se ne koristi samo za komunikaciju, već i za organizaciju distribucije narkotika (Mahnken, 2022), koordinaciju

krijumčarenja ljudi i oružja (Rhumorbarbe, i dr., 2017), upravljanje cyber kriminalnim aktivnostima (Jasper, 2020), kao i za prikrivanje i reintegraciju kriminalnih prihoda kroz sofisticirane oblike pranja novca koji uključuju online platne servise, kriptovalute i fiktivne digitalne poslovne modele. Na taj način, digitalna infrastruktura postaje produžetak kriminalne ekonomije (Biedron, 2024), omogućavajući kriminalnim grupama da istovremeno djeluju lokalno i transnacionalno, da koriste globalne platforme i legalne online servise kao logističke i finansijske čvorove, te da značajno smanje potrebu za fizičkom prisutnošću, čime se povećava otpornost njihove strukture na represivne mjere.

2.3. Struktura i digitalna organizacija OKG

Strukturno posmatrano, savremene OKG sve češće kombinuju hijerarhijske elemente sa mrežnim modelima organizacije (Libby & Corzine, 2011), što im omogućava veću fleksibilnost i bržu adaptaciju na promjene u operativnom okruženju. Ovakav hibridni model posebno dolazi do izražaja u digitalnom prostoru, gdje se ključni akteri mogu distancirati od neposrednog izvršenja kriminalnih aktivnosti, dok se operativni zadaci delegiraju kroz više slojeva posrednika i saradnika (Abello-Colak & Guarneros-Meza, 2014). Vođe se fizički distanciraju od kriminalnih operacija u izuzetnim slučajevima, bilo kao protumjera protiv otkrivanja ili zbog pritvora (EUROPOL, 2024, str. 26). Komunikacija se uvijek odvija u povjerljivim krugovima, pri čemu je svaki novi član provjeren i poznat vođama i njihovim zamjenicima (Lusthaus, 2019). Ovakva organizacija smanjuje direktnu izloženost centralnih aktera, ali istovremeno povećava zavisnost kriminalnih mreža od digitalnih komunikacijskih kanala i platformi koje povezuju geografski razdvojene segmente mreže, što digitalnu infrastrukturu čini ključnim integrativnim elementom transnacionalnog kriminalnog djelovanja.

3. OSINT KAO OPERATIVNI ALAT U ISTRAŽIVANJU ORGANIZIRANIH KRIMINALNIH GRUPA

3.1. OSINT i mrežna analiza kriminalnih struktura

Analiza OKG u digitalnom okruženju zahtijeva metodološki pristup koji prevazilazi fokus na pojedinačne aktere i izolirane događaje, te se usmjerava na razumijevanje odnosa, uloga i dinamike unutar kriminalnih mreža. Umjesto linearne logike identifikacije počinioca i djela, ovakav pristup polazi od pretpostavke da se kriminalna efikasnost proizvodi kroz raspodjelu funkcija, povjerenja i komunikacijskih tokova unutar mreže, a ne kroz individualno djelovanje. Studije koje se oslanjaju na mrežne metode za ispitivanje dinamike kriminalnih grupa prikupile su podatke o mreži iz različitih izvora, uključujući: (1) terenska zapažanja, (2) policijske evidencije, (3) arhivirane materijale, (4) samoprocjene i (5) online podatke (Ouellet & Hashimi, 2019). Ovakva kombinacija izvora omogućava istražitelju da istovremeno posmatra formalne i neformalne aspekte kriminalnog djelovanja, ali i da uoči razlika između onoga što je institucionalno zabilježeno i onoga što se zaista odvija unutar mreže. U praktičnom analitičkom radu, ovakav pristup omogućava identifikaciju centralnih aktera sa visokom stepenom povezanosti, posrednika koji povezuju različite segmente mreže, kao i perifernih i teško vidljivih aktera koji obavljaju ključne logističke i finansijske funkcije. Ono što je bitno je da centralnost u mreži ne označava nužno hijerarhijski vrh. To zapravo

često ukazuje na operativne čvorove koji kontrolišu tok informacija, novca ili povjerenja između inače nepovezanih segmenata kriminalne strukture. Idealno bi bilo da podaci o mreži odražavaju cijelu populaciju od interesa; međutim, koga uključiti ili isključiti često je ograničeno praktičnim ograničenjima „ko je u podacima“, a ne teorijskim pitanjima „koga treba smatrati dijelom mreže“ (Ouellet & Hashimi, 2019). Ova ograničenja posebno dolaze do izražaja u digitalnom okruženju, gdje vidljivost aktera zavisi od njihove izloženosti otvorenim izvorima. S druge strane, akteri sa najvišim stepenom kontrole često ostaju skriveni iza slojeva posrednika i tehničkih barijera, odnosno održavaju visok nivo operativne sigurnosti.

3.2. Pozicija OSINT-a u krim-obavještajnom ciklusu

OSINT u savremenim istragama OKG ne predstavlja zasebnu ili alternativnu metodologiju, već funkcionalni dio krim-obavještajnog ciklusa koji dopunjuje i unapređuje klasične istražne i obavještajne metode (Staniforth, 2016). Njegova osnovna vrijednost ne leži u ekskluzivnosti izvora, već u brzini dostupnosti, širini obuhvata i mogućnosti inicijalnog mapiranja kriminalnog okruženja bez primjene prinudnih ili prikrivenih mjera. U tom smislu, OSINT najčešće djeluje kao ulazna tačka obavještajnog ciklusa, omogućavajući formulisanje početnih analitičkih pretpostavki i identifikaciju relevantnih aktera, događaja i veza koje se kasnije provjeravaju drugim metodama. Prema Fedralnom istražnom birou (FBI), obavještajni ciklus je proces od šest faza: zahtijeva, planiranja i usmjeravanja, prikupljanja, obrade i iskorištavanja, analize i produkcije i diseminacije (Goldman, 2011). Shodno navedenom Goldmanovom definisanju FBI ciklusa, OSINT omogućava sistematsko sagledavanje otvorenog digitalnog okruženja u kojem kriminalne grupe djeluju, uključujući medijske sadržaje, društvene mreže, javne registre i poslovne podatke. Ovi izvori omogućavaju identifikaciju obrazaca ponašanja, javno vidljivih veza i indikatora kriminalnih aktivnosti, posebno u ranim fazama istrage kada još ne postoji dovoljan stepen osnovane sumnje za primjenu posebnih istražnih mjera i radnji. Time OSINT smanjuje početnu informativnu prazninu i omogućava efikasnije usmjeravanje daljih istražnih aktivnosti. U analitičkoj fazi krim-obavještajnog ciklusa, OSINT podaci se integrišu sa informacijama pribavljenim iz policijskih evidencija, finansijskih istraga i drugih izvora, pri čemu dobijaju svoju punu vrijednost kroz kontekstualizaciju i povezivanje. OSINT u ovoj fazi ne funkcioniše kao dokazni materijal sam po sebi, već kao analitički resurs koji pomaže u razumijevanju strukture kriminalne mreže, uloga pojedinih aktera i dinamike njihovih odnosa. Njegova uloga je usmjeravajuća, a ne dokazna. Posebno je značajna njegova uloga u identifikaciji potencijalnih posrednika, logističkih čvorova i aktera koji izbjegavaju direktnu operativnu vidljivost. U fazi usmjeravanja i donošenja odluka, OSINT doprinosi procjeni prioriteta i rizika, omogućavajući nadležnim institucijama da racionalnije rasporede ograničene resurse.

3.3. Ključni OSINT izvori u istraživanju OKG

U istraživanju organiziranih kriminalnih grupa, OSINT izvori ne posmatraju se kao izolovani skupovi informacija, već kao međusobno povezani segmenti digitalnog ekosistema. Njihova integrisana analiza omogućava rekonstrukciju kriminalnih aktivnosti, odnosa i obrazaca djelovanja. Operativna vrijednost proizlazi iz dostupnosti, mogućnosti

kombinovanja i potencijala za dugoročnu analizu, a ne iz pojedinačne informativne ekskluzivnosti. Medijski izvori predstavljaju jedan od osnovnih OSINT segmenata (Yeboah-Ofori & Brimicombe, 2018), jer reflektuju javno vidljive aspekte kriminalnih aktivnosti, institucionalnih reakcija i društvenog konteksta u kojem OKG djeluju. Analiza medijskih sadržaja omogućava identifikaciju ponavljajućih narativa, geografske koncentracije kriminalnih događaja, kao i vremenskih obrazaca koji mogu ukazivati na eskalaciju ili prilagođavanje kriminalnih aktivnosti. Iako mediji često nude fragmentirane informacije, njihova vrijednost leži u longitudinalnom praćenju i upoređivanju izvještaja kroz vrijeme. Za razliku od medijskih izvještaja koji posreduju informacije kroz institucionalni i urednički filter, društvene mreže omogućavaju neposredniji uvid u društvene veze i obrasce samoprezentacije aktera. Društvene mreže i platforme za digitalnu komunikaciju predstavljaju posebno značajan OSINT izvor, jer omogućavaju uvid u javno vidljive veze, kontakte i oblike samoprezentacije aktera (Andrews, Brewster, & Day, 2018). Iako pripadnici OKG nastoje ograničiti svoju izloženost, digitalni tragovi se često pojavljuju indirektno, kroz članove šireg kruga saradnika, porodicu, poslovne partnere ili povezane subjekte. Analiza ovih izvora omogućava identifikaciju društvenih veza, indikatora životnog stila nesrazmjernog prijavljenim prihodima, kao i potencijalnih logističkih i komunikacijskih čvorova unutar kriminalne mreže. Dok društvene mreže pružaju uvid u socijalnu dimenziju i neformalne odnose, postoje i drugi podaci kao što su javni registri i poslovni podaci koji omogućavaju analizu formalnih ekonomskih struktura. Registri pravnih lica, vlasničke strukture, javno dostupni finansijski podaci i informacije o poslovnim transakcijama omogućavaju identifikaciju fiktivnih kompanija, paravan-struktura i povezanih poslovnih subjekata koji se koriste za prikrivanje kriminalnih prihoda (Moglie & Sorrenti, 2022). Njihova posebna vrijednost ogleda se u mogućnosti povezivanja formalno legalnih aktivnosti sa neformalnim ili kriminalnim tokovima, čime se otvara prostor za finansijske istrage i imovinske provjere. Digitalni tragovi vezani za online tržišta, forume i specijalizirane platforme pružaju dodatni sloj informacija o modusima operandi OKG, posebno u oblastima distribucije narkotika, cyber kriminala i ilegalnih usluga (Johnsen & Franke, 2018). Iako je pristup ovim izvorima često ograničen ili fragmentiran, njihova analiza omogućava uvid u strukturu ponude, komunikacijske obrasce i hijerarhiju unutar kriminalnih tržišta, kao i identifikaciju aktera koji obavljaju posredničke i logističke funkcije.

3.4. Metode OSINT analize relevantne za OKG

Operativna vrijednost OSINT-a u istraživanju OKG ne proizlazi iz samog prikupljanja otvorenih podataka, već iz njihove sistematske analize i međusobnog povezivanja u koherentan analitički okvir. S obzirom na fragmentiranost i heterogenost otvorenih izvora, analitički proces mora biti usmjeren na metode koje omogućavaju identifikaciju obrazaca, odnosa i odstupanja, umjesto oslanjanja na izolovane informacije ili pojedinačne nalaze koji rijetko imaju samostalnu operativnu vrijednost. U tom smislu, analitički proces često započinje analizom veza, koja omogućava mapiranje odnosa između aktera, organizacija, događaja i digitalnih identiteta (Costa, 2019; Schwartz & Rouselle, 2008). Korištenjem javno dostupnih podataka sa društvenih mreža, medija i registara moguće je rekonstruisati osnovnu strukturu kriminalnih mreža, identifikovati centralne aktere, posrednike i periferne članove, te uočiti obrasce komunikacije i saradnje. Ovakav početni uvid stvara osnovu za dalje analitičko

produbljivanje, naročito u kontekstu hijerarhijsko-mrežnih struktura OKG, u kojima formalne pozicije često ne odražavaju stvarni stepen uticaja. Nakon uspostavljanja relacijske strukture mreže, vremenska analiza omogućava sagledavanje dinamike kriminalnih aktivnosti kroz vrijeme (Leong & Sung, 2015). Praćenjem vremenskih obrazaca objava, transakcija, putovanja ili javno zabilježenih događaja moguće je identifikovati faze intenziviranja aktivnosti, periode zastoja ili prilagođavanja, kao i reakcije kriminalnih grupa na represivne mjere. U okviru tako definisanog relacijskog i vremenskog konteksta, analiza sadržaja omogućava dublji uvid u komunikacijske i simboličke aspekte kriminalnog djelovanja (Al-Zaidy, Fung, Youssef, & Fortin, 2012). Cilj nije samo identifikacija eksplicitnih kriminalnih poruka, već i prepoznavanje latentnih signala, kodiranog jezika, ponavljajućih narativa i indikatora pripadnosti određenim grupama ili mrežama (Muhić, 2024), što je posebno važno u ranim fazama istrage kada direktni dokazi još nisu dostupni. Analitički proces se dodatno produbljuje geografskom analizom OSINT podataka, kojom se relacijski i sadržajni nalazi smještaju u prostorni kontekst. Mapiranjem lokacija događaja, kretanja aktera, prebivališta, poslovnih adresa i drugih javno dostupnih geografskih indikatora moguće je identifikovati operativne čvorove, zone koncentracije kriminalnih aktivnosti i transnacionalne rute djelovanja. Na osnovu ovakvog mapiranja i analize mreža, nadležne institucije i istraživači mogu steći dublje razumijevanje unutrašnje dinamike kriminalnog ponašanja, što omogućava preciznije usmjeravanje preventivnih i represivnih mjera (Modise, 2025). Takva saznanja doprinose ciljanim intervencijama na ključnim lokacijama i čvorovima mreže, efikasnijoj raspodjeli resursa te unapređenju situacione prevencije kroz smanjenje prostornih i strukturnih prilika za kriminalno djelovanje (Modise, 2025). Ovaj pristup je naročito značajan u istraživanju OKG koje djeluju preko više jurisdikcija, gdje prostorna dimenzija predstavlja ključni element operativnog planiranja. U konačnici korelacijska analiza omogućava integraciju svih prethodnih nalaza kroz povezivanje podataka iz različitih OSINT izvora. Kombinovanjem informacija iz medija, društvenih mreža, registara i online tržišta moguće je potvrditi ili odbaciti analitičke pretpostavke, uočiti konzistentne obrasce i smanjiti rizik pogrešne interpretacije pojedinačnih podataka. Time se OSINT analiza zaokružuje kao iterativan proces u kojem se relacije, vrijeme, sadržaj i prostor posmatraju u međusobnoj povezanosti, čime se obezbjeđuje analitička pouzdanost i operativna primjenjivost nalaza.

4. PRAKTIČNA PRIMJENA OSINT-A U KONKRETNIM FAZAMA ISTRAŽIVANJA OKG

4.1. Identifikacija aktera i preliminarno mapiranje kriminalne mreže

U početnoj fazi istraživanja organiziranih kriminalnih grupa, OSINT se koristi kao primarni analitički alat za identifikaciju relevantnih aktera i formiranje preliminarne slike kriminalne mreže. U situacijama u kojima još ne postoji dovoljan stepen osnovane sumnje za primjenu prikrivenih ili invazivnih istražnih mjera, otvoreni izvori omogućavaju zakonito i proporcionalno prikupljanje početnih informacija o osobama, strukturama i aktivnostima koje mogu biti povezane sa organiziranim kriminalom. Proces identifikacije aktera započinje sistematskim prikupljanjem već prethodno navedenih javno dostupnih podataka iz medijskih izvještaja, društvenih mreža, javnih registara i poslovnih baza podataka. Analizom ovih izvora moguće je identifikovati imena, pseudonime, nadimke, firme, organizacije i digitalne

identitete koji se učestalo pojavljuju u vezi sa određenim kriminalnim aktivnostima ili događajima (Muhić, 2024). Posebna pažnja posvećuje se ponavljanju istih aktera u različitim kontekstima, kao i njihovoj povezanosti sa već poznatim kriminalnim strukturama ili osobama iz šireg kriminogenog miljea. Nakon inicijalne identifikacije aktera, OSINT omogućava preliminarno mapiranje odnosa unutar potencijalne kriminalne mreže kao što su centralne figure, pomagači, saradnici, podgrupe i tako dalje (Xu & Chen, 2005). Korištenjem javno vidljivih veza sa društvenih mreža, i drugih otvorenih izvora moguće je uspostaviti osnovnu relacijsku strukturu između aktera, uključujući porodične, poslovne, društvene i logističke veze. Korištenje društvenih mreža naročito pomaže i otkriva stvarne socijalne dinamike promatrane grupe. Ovakvo mapiranje nije potpuno, već ima za cilj identifikaciju osnovnih čvorova, posrednika i periferije mreže. U ovoj fazi posebno je važno naglasiti da centralnost aktera u preliminarnoj mrežnoj slici ne mora nužno odražavati njihov stvarni hijerarhijski položaj ili stepen kontrole. Naprotiv, visoka vidljivost pojedinih aktera u otvorenim izvorima često ukazuje na operativne ili komunikacijske uloge, dok stvarni centri odlučivanja mogu ostati skriveni iza slojeva posrednika i indirektnih veza.

4.2. Praćenje aktivnosti i promjena u strukturi

Nakon inicijalne identifikacije aktera i preliminarnog mapiranja kriminalne mreže, OSINT se koristi za kontinuirano praćenje aktivnosti i uočavanje promjena u strukturi organizirane kriminalne grupe. U ovoj fazi fokus se pomjera sa statične identifikacije aktera na dinamičko posmatranje ponašanja, odnosa i prilagođavanja mreže u realnom vremenu ili kroz duže vremenske periode. Cilj nije samo registrovanje novih informacija, već razumijevanje načina na koji OKG reaguje na unutrašnje i spoljašnje pritiske. Praćenje aktivnosti putem OSINT-a obuhvata analizu vremenskih obrazaca objava, poslovnih promjena, javno zabilježenih kretanja, medijskih izvještaja i drugih digitalnih tragova koji ukazuju na intenziviranje, smanjenje ili transformaciju kriminalnih aktivnosti. Promjene u učestalosti komunikacije, pojavljivanje novih aktera, nestanak ranije aktivnih profila ili iznenadne izmjene poslovnih struktura mogu ukazivati na reorganizaciju mreže, prilagođavanje represivnim mjerama ili prelazak na nove kriminalne modalitete (Muhić, 2024). Poseban značaj u ovoj fazi ima praćenje promjena u relacijama između aktera. OSINT omogućava uočavanje slabljenja ili jačanja pojedinih veza, pojavu novih posrednika ili pomjeranje operativnih uloga unutar mreže. Ovakve promjene često prethode važnijim događajima, poput eskalacije kriminalnih aktivnosti, promjene logističkih ruta ili pokušaja prikrivanja tragova kroz restrukturiranje mreže.

4.3. Analitička validacija i podrška operativnim odlukama

U fazi analitičke validacije, OSINT se koristi za provjeru, dopunu i kontekstualizaciju prethodno formiranih analitičkih pretpostavki o strukturi, akterima i aktivnostima organizirane kriminalne grupe. Nakon inicijalnog mapiranja i kontinuiranog praćenja promjena, otvoreni izvori omogućavaju upoređivanje novih podataka sa postojećom analitičkom slikom, čime se smanjuje rizik pogrešne interpretacije i donošenja odluka na osnovu parcijalnih ili zastarjelih informacija. Analitička vrijednost OSINT-a u ovoj fazi proizlazi iz njegove sposobnosti da poveže različite vrste podataka u koherentnu cjelinu. Korištenjem korelacijske analize moguće je uporediti informacije iz medijskih izvještaja,

društvenih mreža, poslovnih registara i drugih otvorenih izvora sa podacima prikupljenim klasičnim istražnim metodama. Ovakav pristup omogućava potvrđivanje ili odbacivanje radnih hipoteza, identifikaciju kontradikcija i uočavanje obrazaca koji nisu bili vidljivi u ranijim fazama istrage. Poseban značaj OSINT-a u ovoj fazi ogleda se u podršci operativnom odlučivanju. Analizirani podaci mogu ukazivati na promjene u ponašanju ključnih aktera, pomjeranje operativnih čvorišta ili prilagođavanje kriminalne mreže institucionalnom pritisku. Na osnovu takvih nalaza moguće je preciznije odrediti operativne prioritete, procijeniti rizike i odabrati optimalan trenutak za primjenu formalnih istražnih ili represivnih mjera. OSINT u ovoj fazi ne služi kao dokazni materijal u užem procesnom smislu, već kao analitička podrška koja omogućava donošenje informisanih odluka. Njegova uloga je da pruži širi kontekst i smanji neizvjesnost u složenom operativnom okruženju u kojem djeluju OKG, posebno u slučajevima sa izraženom transnacionalnom dimenzijom i visokom adaptivnošću kriminalnih struktura.

5. ANALITIČKI IZAZOVI I OGRANIČENJA OSINT PRISTUPA PREMA OKG

U globalnom krim-obavještajnom kontekstu, OSINT je važan segment prikupljanja informacija o djelovanju organiziranih kriminalnih grupa. Kao što je već ranije obrađeno, on nosi širok spektar informacija i može nadopuniti tradicionalne metode obavještajnog rada, ali istovremeno nosi i značajne analitičke izazove i ograničenja. Iako su podaci iz otvorenih izvora lako dostupni, njihov kvalitet i pouzdanost često su upitni. Za razliku od klasičnih obavještajnih podataka prikupljenih tajnim ili službenim kanalima, otvoreni izvori mogu sadržavati neprovjerene ili namjerno obmanjujuće informacije. Još prije dvije decenije, u obavještajnim krugovima vladala je skepsa prema OSINT-u upravo zbog "niske pouzdanosti izvora proizašle iz pogrešnih informacija, tajnih poruka, dezinformacija i besmislenog sadržaja" (Hulnick, 2010). Ova strukturalna nepouzdanost znači da analitičari ne mogu slijepo vjerovati svakoj otvorenoj informaciji. Internet i društvene mreže jesu bogat izvor podataka, ali ujedno predstavljaju i "plodno tlo za dezinformacije" (Liferaft, 2023). Državni i nedržavni akteri širom svijeta svjesno plasiraju lažne ili iskrivljene sadržaje u javni prostor kako bi zbunili istražitelje ili oblikovali javno mnijenje (Liferaft, 2023). Čak i dobronamjerni korisnici mogu nenamjerno širiti netačne informacije, što proizvodi buku i šumove signala u kojoj je teško razlučiti činjenice od spekulacija. Za analitičare koji promatraju otvorene izvore, ovakva nepouzdanost predstavlja ogroman izazov. Oslanjanje na neprovjerene podatke može ozbiljno iskriviti analitičke zaključke i navesti policijske rukovodioce na pogrešne odluke. U kontekstu suzbijanja organiziranog kriminala to bi značilo pogrešno usmjeravanje resursa protiv pogrešne osobe ili grupe uslijed lažne dojave. Stoga, analitičari moraju uložiti dodatne napore u provjeru i validaciju otvorenih podataka. Standardna preporuka je da se svaka bitna informacija iz otvorenih izvora unakrsno provjeri kroz više nezavisnih izvora prije nego što se ugradi u izvještaj. Samo podaci koje potvrđuje nekoliko pouzdanih izvora mogu se smatrati vjerodostojnima. Osim opasnosti od nenamjerne dezinformacije, postoji i aktivna prijetnja od namjernih obmana. Organizirane kriminalne grupe ponekad svjesno plasiraju lažne tragove u javnost putem društvenih mreža, foruma ili kontroliranih medija kako bi skrenule pažnju istrage. Ovo može dovesti do pogrešne atribucije ili da analitičari troše resurse prateći lažne tragove (Dekens, 2025). Primjer takve

varke bi bio kada kriminalna organizacija putem lažnih online profila preuzme odgovornost za neki zločin kojeg zapravo nije počinila, ili kada podmetne lažne informacije o svojoj strukturi i planovima u online komunikaciju očekujući da će obavještajne i sigurnosne službe to pokupiti. Moderni algoritmi pretrage i društvenih mreža mogu paradoksalno pojačati učinak dezinformacija. Jednom kad lažni narativ zadobije zamah, digitalni ekosistem često ga nastavlja širiti. Na primjer preporučuju se slični sadržaji i stvara se echo chamber efekat koji dodatno učvršćuje pogrešne uvjerenja (Dekens, 2025). Drugo važno ograničenje OSINT-a jeste varijabilna dostupnost informacija. Za razliku od klasificiranih obavještajnih podataka do kojih se dolazi posebnim sredstvima, otvoreni podaci su dostupni samo tamo gdje su javno objavljeni. Mnoge relevantne informacije o organiziranom kriminalu nisu javno dostupne. Pripadnici OKG svoja ključna djelovanja i komunikacije nastoje skriti od javnosti, koristeći zatvorene forume na dark webu, šifrirane komunikacijske kanale, ili operiraju u zemljama gdje su službeni registri netransparentni. Ova nekompletnost obavještajne informacije znači da se preko OSINT-a često dobije samo djelomičan mozaik o kriminalnoj grupi. Otvoreni izvori mogu pružiti indicije kao što su medijski naslovi i tekstovi o sumnjivim kompanijama, javne registracije firmi povezane sa pranjem novca, objave na društvenim mrežama članova kriminalnog miljea, procureli dokumenti i drugo. Međutim ti podaci rijetko pokrivaju cjelinu organizacije ili svih njenih aktivnosti. Čak i kada se OSINT koristi za mrežnu analizu kriminalnih grupa, postavlja se pitanje pouzdanosti te mrežne slike. Varijabilnost dostupnosti ogleda se i u jezično-geografskim barijerama. Organizirane kriminalne mreže djeluju transnacionalno, a relevantne otvorene informacije mogu biti na različitim jezicima, u lokalnim medijima ili zatvorenim grupama specifičnim za određenu zemlju/region. Analitičar koji ne poznaje taj jezik ili kulturološki kontekst može propustiti ključne informacije. Automatski prevod može pomoći, ali ne prikazuje uvijek nijanse žargona ili slenga kriminalnih grupa, pri čemu je isto bitno u posmatranju migrantskih OKG koje su sve više prisutne na prostoru Zapadnog Balkana. Atribucija u obavještajnom kontekstu odnosi se na određivanje odgovornosti ko stoji iza neke kriminalne aktivnosti ili mreže. OKG u kibernetičkom prostoru, sve češće koriste “false flag” taktike kako bi zavarale istražitelje. Napadači mogu ostaviti digitalne ili medijske tragove koji upućuju na neku drugu grupu, što istražitelja može navesti na zaključak da je, za kibernetički napad odgovorna ruska mafija, dok je počinitelj zapravo druga organizacija (Galeotti, 2014). S obzirom na navedena ograničenja, OSINT treba posmatrati isključivo kao dopunski alat tradicionalnim metodama prikupljanja obavještajnih podataka, a ne kao njihov surogat. Klasične metode poput ljudskih izvora (HUMINT), tajnog nadzora, prisluškivanja komunikacija (SIGINT), forenzičke analize ili prikrivene operacije i dalje su nezamjenjive za dublje penetriranje u strukturu OKG-a. Otvoreni izvori mogu pružiti prvi sloj informacija ili kontekst, ali rijetko će sami po sebi razotkriti čitavu sliku kriminalnog pothvata. Jedan od primjera neuspješne OSINT istrage je ona o bombaškom napadu u Bostonu 2013. godine gdje su internetske zajednice (korisnici Reddita, 4chana i drugih platformi) uključile se u otvorenu istragu nastojeći pomoći policiji. Stotine samoprozvanih OSINT stručnjaka počeli su pregledavati javno dostupne fotografije i snimke s mjesta događaja u potrazi za sumnjivim licima. Ovaj *crowdsourcing* pristup ubrzo je krenuo u pogrešnom pravcu. Na temelju kolektivne analize slika, korisnici Reddita su pogrešno identificirali jednog mladića, studenta Sunila Tripathija, kao osumnjičenog napadača (Walker, 2013). Tripathi je bio student koji nije imao veze s

napadom, ali je neosnovano označen kao terorista od interent korisnika jer jer je fizički sličio na napadača i imao sličan ruksak. Ova javna OSINT istraga dovela je do širenja njegovog imena po društvenim mrežama i medijima. Policija je kasnije demantovala te navode i potvrdila da Tripathi nije bio uključen, a da su pravi počinitelji braća Tsarnaev otkriveni analizom snimaka nadzornih kamera od strane policije i sigurnosnih službi i svjedočenja građana.

6. ZAKLJUČAK

Savremeno djelovanje organiziranih kriminalnih grupa sve je izraženije povezano sa digitalnim operativnim okruženjem u kojem se kriminalne aktivnosti, odnosi i organizacijske strukture djelimično reflektuju kroz javno dostupne informacijske tragove. U takvim okolnostima, open source intelligence dobija sve veći značaj kao analitički alat koji omogućava ranu identifikaciju aktera, preliminarno mapiranje kriminalnih mreža i praćenje njihovog prilagođavanja promjenjivim bezbjednosnim i represivnim uslovima. Ipak, uprkos toj objektivnoj potrebi, OSINT u krim-obavještajnoj praksi i akademskim istraživanjima ostaje nedovoljno sistematiziran i često marginaliziran u odnosu na klasične istražne metode, posebno kada je riječ o njegovoj operativnoj primjeni u istraživanju organiziranog kriminala. Analizom ključnih OSINT izvora, relevantnih analitičkih metoda i konkretnih faza istražnog postupka oni mogu značajno doprinijeti smanjenju početne informativne praznine, preciznijem usmjeravanju istražnih prioriteta i dubljem razumijevanju dinamike kriminalnih mreža. Istovremeno postoje i ograničenja uključujući selektivnu vidljivost aktera, rizik pogrešne atribucije i uticaj analitičkih pristrasnosti.Navedeno potvrđuje da OSINT ne može biti posmatran kao samostalan istražni mehanizam, već isključivo kao komplementarni alat čija se puna vrijednost ostvaruje kroz integraciju sa HUMINT-om, finansijskim istragama i klasičnim policijskim metodama. Profesionalna i odgovorna upotreba OSINT-a zahtijeva visok stepen analitičke discipline, metodološku dosljednost i kontinuiranu validaciju nalaza kako bi se izbjegle površne interpretacije i operativne greške. Shodno svemu navedenom, sistemska primjena OSINT-a predstavlja neizostavan element savremenog krim-obavještajnog pristupa borbi protiv organiziranog kriminala, te da dalji razvoj ove oblasti zahtijeva veću institucionalnu pažnju, jasnije metodološke okvire i dodatna istraživanja usmjerena ka njegovoj praktičnoj i operativnoj upotrebi u kompleksnim, transnacionalnim istragama u uslovima kontinuirane digitalizacije kriminalnih struktura.

7. LITERATURA

1. Abello-Colak, A., & Guarneros-Meza, V. (2014). The role of criminal actors in local governance. *Urban Studies*, 3268-3289.
2. Al-Zaidy, R., Fung, B. C., Youssef, A. M., & Fortin, F. (2012). Mining criminal networks from unstructured text documents. *Digital Investigation*, 147-160.
3. Andrews, S., Brewster, B., & Day, T. (2018). Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online. *Security Informatics*.
4. Baker, R. (2023). *Deep Dive: Exploring the Real-World Value of Open Source Intelligence.* Wiley.
5. Bartlett, J., Miller, C., Crump, J., & Middleton, L. (2013). *Policing in information age.* Demos.

6. Biedron, S. R. (2024). *Cybercrime in the Digital Age (Master's thesis).* Oxford: University of Oxford.
7. Boyd, D., Casteel, H., Thakor, M., & Johnson, R. (2011). *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the U.S.* Microsoft Research.
8. Costa, J. (2019). *Social network analysis in combating organised crime and trafficking.* Basel Institute on Governance.
9. Dekens, N. (05. 09 2025). *The 13 Biggest OSINT Investigation Challenges*. Preuzeto od Shadow Dragon: https://shadowdragon.io/blog/what-are-the-common-struggles-of-osint-investigations/
10. Durkin, K., Forsyth, C. J., & Quinn, J. F. (2006). Pathological internet communities: A new direction for sexual deviance research in a postmodern era. *Sociological Spectrum*, 595-606.
11. EU4Justice. (2021). *Kratki vodič za OSINT.* Sarajevo: EU4Justice.
12. EUROPOL. (2024). *DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS.* Luxembourg: Publications Office of the European Union.
13. EUROPOL. (2024). *Encrypted app intelligence exposes sprawling criminal networks across Europe*. Preuzeto od EUROPOL: https://www.europol.europa.eu/media-press/newsroom/news/encrypted-app-intelligence-exposes-sprawling-criminal-networks-across-europe
14. EUROPOL. (2025). *EU-SOCTA: The changing DNA of serious and organised crime.* Luxembourg: Publications Office of the European Union: EUROPOL.
15. Galeotti, M. (2014). *Global Crime Today: The Changing Face of Organised Crime.* London: Routledge.
16. Goldman, J. (2011). *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats.* Scarecrow Press.
17. Hulnick, A. S. (2010). The Dilemma of Open Sources intelligence: Is OSINT Really Intelligence? U L. K. Johnson, *The Oxford Handbook of National Security Intelligence* (str. 229–241). Oxford.
18. Jasper, S. (2020). *Russian Cyber Operations.* Washington DC: Georgetown University Press.
19. Johnsen, J. W., & Franke, K. (2018). Identifying Central Individuals in Organised Criminal Groups and Underground Marketplaces. *Computational Science – ICCS*, (str. 379–386).
20. Leong, K., & Sung, A. (2015). A review of spatio-temporal pattern analysis approaches on crime analysis. *International E-Journal of Criminal Sciences*.
21. Libby, N. E., & Corzine, J. (2011). Criminal Organizations: Traditional Adversaries and New. U J. A. Scherer, & J. P. Jarvis, *The Future of Law Enforcement: A Consideration of Potential Allies and Adversaries* (str. 47-61). Quantico, VA: Proceedings of the Futures Working Group.
22. Liferaft. (12. 09 2023). *OSINT Analysts: 9 Mistakes That Can Sabotage Investigations*. Preuzeto od Liferaft: https://liferaftlabs.com/blog/osint-analysts-9-mistakes-that-can-sabotage-investigations
23. Lowentha, M. M., & Clark, R. M. (2015). *The Five Disciplines of Intelligence Collection.* CQ Press.
24. Lusthaus, J. (2019). Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy. *IEEE European Symposium on Security and Privacy Workshops*, (str. 474-480). Stockholm, Sweden.
25. Mahnken, J. K. (2022). Digital Transformations in Drug-Related Crime. *Historical Social Research*, 261-290.

26. Mainas, E. D. (2012). Analysis of Criminal and Terrorist Organisations as Social Network Structures: A Quasi-Experimental Study. *International Journal of Police Science and Management*, 264-282.
27. Makarenko, T. (2010). The Crime-Terror Continuum: Tracing the Interplay Between Transnational. *Global Crime* , 129-145.
28. Modise, J. M. (2025). Mapping Crime Place Networks: A Spatial Analysis of Criminal Activity. *International Journal of Innovative Science and Research Technology*, 2326-2336.
29. Moglie, M. L., & Sorrenti, G. (2022). Revealing "Mafia Inc."? Financial Crisis, Organized Crime, and the Birth of New Enterprises. *The Review of Economics and Statistics*, 142–156.
30. Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, godina 4., broj 2.*, 314-339.
31. Ouellet, M., & Hashimi, S. (2019). Criminal Group Dynamics and Network Methods. *Methods of Criminology and Criminal Justice Research* , 47-65.
32. Rhumorbarbe, D., Werner, D., Gilliéron, Q., Staehli, L., Broséus, J., & Rossy, Q. (2017). Characterising the online weapons trafficking on cryptomarkets. *Forensic Science International*, 16-20.
33. Schwartz, D. M., & Rouselle, T. (2008). Using social network analysis to target criminal networks. *Trends in Organized Crime*, 188–207.
34. Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 251-274.
35. Staniforth, A. (2016). Police Use of Open Source Intelligence: The Longer Arm of Law. *Advanced Sciences and Technologies for Security Applications*, 21-31.
36. Walker, P. (19. 04 2013). *Boston bombing identification attempts on social media end in farce*. Preuzeto od The Guardian: https://www.theguardian.com/world/2013/apr/19/boston-bombing-suspects-reddit-social-media
37. Xu, J. J., & Chen, H. (2005). CrimeNet explorer: a framework for criminal network knowledge discovery. *ACM Transactions on Information Systems*, 201 - 226.
38. Xu, J., & Chen, H. (2005). Criminal network analysis and visualization. *Communications of the ACM*, 100 - 107.
39. Yeboah-Ofori, A., & Brimicombe, A. (2018). Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*.
40. Zhilla, F. (2024). Decrypting the Balkan underworld. A theoretical analysis of encrypted communication in organized crime. *Jus & Justicia*, 7-22.

PRACTICAL APPLICATION OF OSINT METHODS IN THE INVESTIGATION OF ORGANIZED CRIMINAL GROUPS

Abstract: *contemporary organized criminal groups (OCG) operate in a space that is both physical and digital, where their criminal activities generate significant publicly available information traces. Although the digital space has become a central operational environment of modern criminal activity, open source intelligence (OSINT) methods remain insufficiently conceptualized in criminal-intelligence practice and are rarely addressed as a distinct analytical approach in academic research. There is a particular lack of professional and scientific studies that systematically examine OSINT as an operational tool in the investigation of organized criminal groups. The aim of this paper is to present the practical and analytical use of OSINT methods in the identification, mapping, and monitoring of OCGs, with a focus on their application across different phases of the investigative process. The paper identifies key OSINT sources, relevant analytical methods, and proposes basic models for the application of OSINT in criminal-intelligence work, with the goal of improving the understanding and operational use of open sources in combating organized crime.*

Keywords*: OSINT, organized crime groups, criminal intelligence, network analysis*

SPECIFIČNOSTI ONLINE GROOMINGA I KRIMINOLOŠKE IMPLIKACIJE DIGITALNOG OKRUŽENJA

Aldina Bjelić, MA
aldinabjelic@hotmail.com

Sažetak: ***r****ad analizira specifičnosti online groominga kao procesnog i manipulativnog oblika seksualne eksploatacije djece, s posebnim naglaskom na psihološke, kriminalne i digitalne dimenzije ovog fenomena. U teoretskom dijelu prikazane su faze manipulacije, tipologije počinilaca i obrasci ponašanja koji omogućavaju izgradnju prividno sigurnog odnosa između djeteta i groomera. Posebna pažnja posvećena je digitalnom okruženju koje svojim tehničkim karakteristikama, anonimnošću i infrastrukturom više platformi omogućava fragmentiranost tragova i otežava rekonstrukciju komunikacijskog toka. Analizirani su i strukturni faktori rizika, uključujući emocionalnu ranjivost djece, algoritamsku logiku digitalnih servisa i ograničene institucionalne kapacitete za prevenciju. Zaključuje se da je online grooming kompleksan fenomen koji zahtijeva interdisciplinarni pristup, jačanje digitalne pismenosti i razvoj preventivnih strategija koje uvažavaju psihološke, tehnološke i društvene komponente rizika.*

Ključne riječi: *online grooming, seksualna eksploatacija djece, digitalna ranjivost, digitalni tragovi*

1. UVOD

Online grooming predstavlja jedan od najsuptilnijih i najopasnijih oblika seksualne eksploatacije djece u digitalnom okruženju, budući da počinioci djeluju kroz proces postepenog uspostavljanja emocionalne veze, sticanja povjerenja i manipulacije koja žrtvu vodi ka seksualiziranom sadržaju ili fizičkom susretu. Za razliku od tradicionalnih oblika nasilja nad djecom, online grooming se odvija u prostoru koji omogućava prikrivanje identiteta, višestruke lažne prezentacije i kontinuirano pomjeranje komunikacije između platformi, što počiniocima daje značajnu prednost u izgradnji odnosa koji na prvi pogled ne djeluje prijeteće. Takva dinamika stvara kriminološki specifičan problem u kojem je granica između prividno bezopasne komunikacije i manipulativnog procesa teško uočljiva, kako za dijete tako i za odrasle koji kasnije učestvuju u identifikaciji i procjeni rizičnih obrazaca. Poseban izazov predstavlja činjenica da je online grooming proces, a ne jednokratni čin, zbog čega njegovo prepoznavanje zahtijeva analizu sekvenci poruka, promjena u tonu komunikacije i postupnog uvođenja seksualiziranih elemenata. Digitalna okolina dodatno komplikuje ovaj proces jer fragmentira komunikacijske tragove i otežava utvrđivanje namjere počinioca, što za pravosudne institucije predstavlja jedno od najkompleksnijih pitanja u fazi dokazivanja. Sudovi se često suočavaju s problemom tumačenja radnji koje se naizgled odvijaju u „sivoj zoni“, odnosno između zakonski kažnjivog ponašanja i komunikacije koja još nije eskalirala prema eksplicitnoj eksploataciji. Upravo zbog toga online grooming postaje pravno-procesni izazov u kojem se sudski epilog ne oslanja samo na postojanje nedvosmislenog sadržaja, nego i na sposobnost da se dokaže manipulativna priroda komunikacije i njena usmjerenost ka seksualnoj eksploataciji. Time se otvara prostor za

detaljniju kriminološku i pravnu analizu koja omogućava bolje razumijevanje mehanizama grooming, ali i ograničenja postojećih pravnih rješenja.

2. POJMOVNO ODREĐENJE ONLINE GROOMINGA

U literaturi se pojam seksualnog grooming najčešće koristi da označi proces u kojem odrasla osoba postupno priprema dijete i njegovu okolinu za seksualnu zloupotrebu, kroz kombinaciju emocionalne manipulacije, izgradnje povjerenja i normalizacije neprimjerenog ponašanja. Jedna od najčešće citiranih definicija naglašava da je grooming niz povezanih radnji kojima počinilac "priprema dijete i njegov socijalni kontekst" kako bi se olakšalo izvršenje seksualnog zlostavljanja, pri čemu se manipulacija odvija u fazama i traje određeno vrijeme, a ne predstavlja izolovan događaj (Kloess, Beech, & Harkins, 2014). Također, online chat orkestrira osoba koja se bavi groomingom na takav način da se na kraju sve pretvori u raspravu o seksu. Osoba koja se bavi groomingom često će slati pornografiju djetetu i podsticati seksualizirane tekstualne poruke ili poruke u chat sobama (Sorell, 2016). Ponekad će osumnjičeni biti zainteresiran za seksualno iskustvo djeteta i ponudit će mu da ga nauči seksualnim tehnikama. O'Connell (2003) dodatno ističu da grooming obuhvata i sistematsko testiranje granica, procjenu ranjivosti djeteta i suptilno smanjenje otpora kroz komplimente, poklone i pseudopriateljski odnos, što stvara okvir u kojem dijete doživljava počinioca kao „posebnu" osobu, a ne kao prijetnju. Pojam online grooming razvijen je kako bi se označila ista vrsta manipulativnog procesa, ali posredstvom informaciono-komunikacijskih tehnologija, prvenstveno interneta i digitalnih komunikacijskih platformi. Savremena istraživanja ga definišu kao proces u kojem odrasla osoba koristi internet tehnologije da inicira i razvije dinamiku seksualne persvazije i viktimizacije djeteta, s ciljem dobijanja seksualnog sadržaja ili organizovanja fizičkog susreta (Reneses, Riberas-Gutiérrez, & Bueno-Guerra, 2024). U tom smislu online grooming nije samo virtualna komunikacija, nego strukturirani niz interakcija u kojem se mijenjaju ton, sadržaj i intenzitet poruka. Na konceptualnom nivou online grooming se uobičajeno posmatra kao sastavni dio šire kategorije online seksualne eksploatacije i zloupotrebe djece (CSEA)[3], zajedno sa proizvodnjom, razmjenom i posjedovanjem materijala seksualnog zlostavljanja djece (CSAM), živim prenosima zlostavljanja i online seksualnom ucjenom. Međunarodne organizacije poput ECPAT-a[4] i Ured za borbu protiv droga i kriminala Ujedinjenih nacija (UNODC) ističu da je zajednička karakteristika ovih fenomena upotreba digitalnih tehnologija za uspostavljanje, održavanje ili produbljivanje odnosa moći u kojem je dijete dovedeno u stanje seksualne iskorištenosti, bilo kroz kontakte uživo, bilo kroz proizvodnju i

[3]Pojmovi Child Sexual Abuse Material (CSAM) i Child Sexual Exploitation and Abuse (CSEA) često se pogrešno koriste kao sinonimi, iako označavaju različite domene viktimizacije. CSAM se odnosi isključivo na bilo koji vizualni ili tekstualni materijal koji prikazuje seksualno zlostavljanje ili seksualiziranu eksploataciju djeteta, uključujući fotografije, video snimke, livestream sadržaje, crteže i digitalne manipulacije stvarnih ili fikcionalnih likova. Takvu definiciju koriste INTERPOL, Europol i ECPAT, pri čemu je naglasak na materijalu kao dokazu počinjenog zlostavljanja. CSEA je širi koncept koji obuhvata sve oblike seksualnog zlostavljanja i eksploatacije djece, uključujući kontaktne oblike nasilja, online grooming, seksualnu ucjenu, trgovinu djecom radi seksualne eksploatacije i produkciju CSAM-a. Drugim riječima, CSAM je proizvod, dok je CSEA proces i širi fenomen u kojem se pojavljuju mnogi modaliteti viktimizacije, a CSAM predstavlja samo jedan od njihovih izraza.

[4]ECPAT je akronim za End Child Prostitution in Asian Tourism, odnosno organizacije koja se bori za okončanje dječije prostitucije u azijskom turizmu.

dijeljenje seksualiziranog sadržaja (ECPAT, 2020; UNODC, 2020; ECPAT 2022). U tom okviru grooming zauzima specifično mjesto, jer je usmjeren upravo na pripremu terena za eksploataciju. Navedena priprema terena se ogleda u stvaranju psiholoških i situacionih uvjeta koji omogućavaju kasnije zlostavljanje. Normativno posmatrano, online grooming je prepoznat i u ključnim međunarodnim instrumentima zaštite djece od seksualne eksploatacije. Konvencija Vijeća Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja poznato kao Lanzarote konvencija uvodi posebno krivično djelo „navođenja djeteta na susret u seksualne svrhe“ (Council of Europe, 2015). Navedeno krivično djelo se vrši putem informaciono-komunikacijskih tehnologija i eksplicitno konstatuje da je riječ o fenomenu koji je u praksi poznat kao grooming. Model zakona Međunarodnog centra za nestalu i zlostavljanu djecu (ICMEC) (2017) dodatno precizira da online grooming obuhvata svako namjerno uspostavljanje kontakta sa djetetom putem informaciono-komunikacijskih tehnologija u svrhu pripreme ili olakšavanja seksualne zloupotrebe ili proizvodnje materijala seksualnog zlostavljanja djece. Ovakav pristup snažno utiče na nacionalna zakonodavstva, koja sve češće kriminaliziraju ne samo izvršenje zlostavljanja, nego i fazu digitalnog „pripremanja“ žrtve. Savremena istraživanja (Chiang & Grant, 2017; Wefers, i dr., 2024) naglašavaju da je za pojmovno razumijevanje online groominga ključno njegovo procesno i razvojno obilježje. Umjesto da se definiše isključivo prema pojedinačnim porukama ili sadržajima, grooming se prepoznaje kao tok komunikacije u kojem počinilac kombinira emocionalnu podršku, dijeljenje prividno intimnih informacija, postupno pomjeranje teme prema seksualnosti i normalizaciju sve eksplicitnijih sadržaja.

2. KRIMINALNE I PSIHOLOŠKE SPECIFIČNOSTI ONLINE GROOMINGA

Online grooming predstavlja procesnu i namjernu manipulaciju djeteta u cilju stvaranja emocionalne, psihološke i situacijske podložnosti seksualnoj eksploataciji. Kriminalna specifičnost ovog fenomena počiva na činjenici da se počinilac ne oslanja na fizičku prisilu, nego na postupno uspostavljanje odnosa koji djetetu djeluje sigurno, poznato i privlačno. U većini slučajeva počinilac kreira lažni identitet ili prilagođava svoj online nastup očekivanjima djeteta, čime se stvara iluzija vršnjačke komunikacije ili „posebnog prijateljstva“. Takva vrsta prezentacije omogućava mu pristup emocionalnim teškoćama, nesigurnostima ili trenucima ranjivosti koje dijete spontano dijeli u digitalnom prostoru. Psihološki aspekt groominga najjasnije se vidi kroz fazni model manipulacije koji je razvila Rachel O’Connell (2003), čiji su nalazi postali osnova za većinu kriminoloških i operativnih analiza ovog fenomena. Prema ovom modelu grooming se odvija kroz nekoliko uzastopnih faza koje imaju jasan psihološki cilj, a to su: Prva faza (Friendship Forming Stage) koja se odnosi na inicijalni kontakt u kojem počinilac nastoji djelovati ljubazno, radoznalo i podržavajuće. Druga faza (Relationship Forming Stage) podrazumijeva jačanje emocionalne veze kroz intenzivniju komunikaciju, razmjenu „povjerljivih“ informacija i stvaranje dojma da je odnos poseban i drugačiji od drugih. Treća faza (Risk Assessment Stage) predstavlja trenutak u kojem počinilac procjenjuje koliko je dijete spremno na dalje korake, ispituje da li roditelji nadziru komunikaciju, sugeriše načine skrivanja razgovora i provjerava da li dijete već ima iskustva sa sličnim sadržajem. Četvrta faza (Exclusivity Stage) uključuje emocionalno „vezivanje“ djeteta kroz izjave o posebnosti odnosa, ljubavi, povjerenju i povjerljivosti. Peta faza (Sexual Stage) predstavlja trenutak u kojem se uvodi seksualizirani

sadržaj, najčešće postepeno, kroz dvoumljive komentare, insinuacije, „šale“, a potom kroz eksplicitne zahtjeve. Šesta faza (Conclusion Stage) obuhvata prelazak na direktnu eksploataciju, bilo kroz razmjenu seksualiziranog materijala, bilo kroz organiziranje fizičkog susreta. Uspješno djelo, odnosno grooming, podrazumijeva vještu manipulaciju djeteta i njegove okoline kako bi se seksualno zlostavljanje moglo lakše počiniti bez otkrivanja (van Dam, 2006). Ova manipulacija nije spontana ili neorganizirana, nego predstavlja niz planskih radnji kojima počinilac sistematski utiče na percepciju djeteta i odraslih u njegovoj blizini. Počinitelj nastoji stvoriti sliku pouzdane i dobronamjerne osobe, čime se smanjuje vjerovatnoća da će njegovo ponašanje biti prepoznato kao prijetnja ili devijantno. Počinioci koji koriste grooming često to rade pod maskom ljubaznosti, šarma i spremnosti da pomognu (van Dam, 2001). U istraživanju DeHart i saradnika (2016), izvršena je tipologizacija online seksualnih prestupnika u četiri kategorije: počinioce orijentisane na cyberseks (*Cybersex offenders*), počinioce koji kombiniraju cyberseksualna ponašanja s planiranjem susreta (*Cybersex/schedulers*), počinioce čija je primarna namjera zakazivanje kontakta uživo (*Schedulers*) i počinioce koji nastoje kupiti seksualni pristup djetetu (*Buyers*). Pored faznog modela manipulacije, u literaturi se razvijaju i različite tipologije počinilaca koje dodatno objašnjavaju motivacijske i ponašajne razlike među groomerima. Lanning (2010) razlikuju preferencijalne i situacione počinioce, pri čemu prvi pokazuju stabilan i dugotrajan seksualni interes prema djeci, dok se drugi uključuju u zlostavljanje usljed okolnosti, oportuniteta ili emocionalnih frustracija. Autori poput Whittle i saradnika (2014) posebno ističu razliku između groomera koji putem interneta traže emocionalnu povezanost sa djetetom (intimacy-seeking) i onih koji su prvenstveno usmjereni na ostvarivanje fizičkog susreta (contact-driven), što je naročito relevantno u digitalnom okruženju. Upravo ovakav prikaz vlastite ličnosti omogućava im pristup situacijama u kojima dijete postaje emocionalno ili socijalno dostupnije, pri čemu ovo korelira sa O'Connellovim fazama. Kada se stvore prihvatljive okolnosti, počinitelj postepeno gradi odnos koji žrtva doživljava kao siguran i afirmativan, dok istovremeno prikriva svoju stvarnu namjeru. Oni strateški manipulišu žrtvom, njenom porodicom i zajednicom kako bi sakrili svoje devijantne namjere i izbjegli otkrivanje (Winters & Jeglic, 2017). Katz i Barnetz (2016) istraživali su grooming na uzorku od 95 djece uzrasta od 5 do 13 godina i utvrdili su da je 68,4% žrtava izjavilo kako je počinilac manipulirao njihovom porodicom. Takva strategija obuhvata i širenje povjerenja među odraslima koji mogu poslužiti kao zaštitni faktor, s ciljem da se smanji njihova sumnjičavost i poveća mogućnost nesmetanog kontakta s djetetom. Počinilac tako stvara društveni kontekst u kojem se njegovo prisustvo smatra benignim ili čak poželjnim. Ranjivost djece predstavlja jedan od ključnih faktora koji određuju vjerovatnoću ulaska u proces groominga. Istraživanja dosljedno pokazuju da djeca koja doživljavaju emocionalnu usamljenost, niže samopoštovanje ili potrebu za prihvatanjem predstavljaju posebno rizičnu skupinu, jer su sklonija razvijanju povjerenja prema nepoznatim osobama u digitalnom prostoru (Livingstone, Haddon, Görzig, & Ólafsson, 2011). Povišen rizik prisutan je i kod djece koja dolaze iz konfliktnih porodičnih sredina, imaju slab roditeljski nadzor ili izraženu potrebu za pažnjom i podrškom koju ne pronalaze u neposrednom okruženju. Online okruženje dodatno pojačava ove faktore, jer pruža osjećaj anonimnosti i kontrolisanog samoizražavanja, što djeci omogućava da grade odnose koji im se čine sigurnijim i otvorenijim nego u realnom životu. Whittle i saradnici (2013) ističu da djeca koja se osjećaju izolirano ili emocionalno

zanemareno češće prihvataju komunikaciju s nepoznatima i sporije prepoznaju manipulativne obrasce ponašanja. U takvim okolnostima groomer može precizno targetirati emocionalne potrebe djeteta, što olakšava izgradnju odnosa povjerenja i kasnije normaliziranje seksualizirane komunikacije.

3. DIGITALNO OKRUŽENJE I KRIMINALISTIČKE IMPLIKACIJE

3.1. Tehnike prikrivanja identiteta i digitalna infrastruktura groominga

Jedna od najizraženijih karakteristika digitalnog groominga jeste širok spektar tehnika prikrivanja identiteta. Počinitelji često koriste lažne profile, tuđe, generičke ili modificirane fotografije, privremene naloge i pseudonime, čime otežavaju identifikaciju i povezivanje različitih računa s istom osobom. Upotreba enkriptiranih aplikacija i *peer-to-peer* platformi koje nude poruke koje nestaju ili se automatski brišu dodatno smanjuje količinu dostupnih digitalnih tragova (Davidson & Gottschalk, 2011). Tehnološke inovacije dodatno komplikuju kriminalističku sliku. Razvojem alata za manipulaciju fotografija i videa, uključujući deepfake tehnologiju i AI-generirane profilne slike, groomeri sada mogu kreirati uvjerljive maske koji ne ostavljaju trag stvarne osobe. Takve slike se koriste za izgradnju vjerodostojnog digitalnog identiteta, posebno u okruženjima gdje se očekuje vršnjačka komunikacija. Osim vizualnog prikrivanja, počinitelji često mijenjaju jezički stil, korištenje slenga ili pravopisne obrasce kako bi imitirali govor djece i adolescenata. Specifičnost pojedinih platformi dodatno pogoršava kriminalističke izazove u praksi. Platforme poput Discorda, koje su posebno popularne među djecom i mladima, omogućavaju stvaranje zatvorenih grupa, tematskih kanala i privatnih razgovora u kojima se komunikacija odvija dinamično, intenzivno i često bez nadzora odraslih. U takvim digitalnim zajednicama groomer može lako identifikovati ranjivu djecu, bilo kroz posmatranje njihove komunikacije u grupama, bilo kroz ulazak u direktnu interakciju na osnovu zajedničkih interesa kao što su gaming, anime, umjetnost ili specifične subkulture (Ashcroft, Kaati, & Meyer, 2015). Dodatni problem nastaje kada groomer namjerno premješta komunikaciju na platforme koje nude bolju anonimnost, enkripciju ili veću kontrolu nad historijom poruka. Ovaj proces prelaska s jedne platforme na drugu, često nazivan *platform transition* ili *off-platform migration* (Chen & Jiang, 2025), predstavlja polaznu tačku za kasniju fragmentaciju digitalnih tragova. Groomer u početnoj fazi koristi platformu s otvorenom vidljivošću, poput Facebooka, Instagrama ili TikToka, a nakon uspostavljanja povjerenja komunikaciju prebacuje na servise s privremenim porukama kao što su Snapchat, Telegram ili Signal. Tokom ovih prelazaka groomer koristi prednosti tehničkih postavki platformi kako bi smanjio mogućnost nadzora, praćenja i rekonstrukcije komunikacijskog toka. Na taj način, manipulativni proces nije samo psihološki i komunikacijski, nego i tehnički strukturiran tako da kriminalističkim istražiteljima otežava identifikaciju počinitelja, prikupljanje dokaza i povezivanje digitalnih tragova u koherentan narativ.

3.2. Fragmentiranost digitalnih tragova i problemi rekonstrukcije komunikacijskog toka

Specifičnost digitalnih tragova u online groomingu ogleda se u njihovoj fragmentiranosti, isparljivost i zavisnosti od tehničkih karakteristika platforme. Ovakva isparljivost, odnosno volitalnost digitalnih tragova direktno je prepoznata kao jedan od ključnih problema u istraživanjima online seksualnih delikata (Heath, MacDermott, & Akinbi, 2023). U praksi to znači da istražitelji najčešće raspolažu tek fragmentima poruka, snimcima ekrana, parcijalnim zapisima ili podacima koji su vremenski i sadržajno neusklađeni. Praktični razmjeri online groominga vidljivi su u slučaju Aleksandra McCartneya iz Sjeverne Irske, koji je godinama koristio lažne identitete da manipulira i ucjenjuje maloljetne djevojčice širom više zemalja te je identifikovano oko 3.500 žrtava (Moses, 2024). Ovaj slučaj pokazuje kako kombinacija anonimnosti, višestrukih platformi i digitalnih tehnika prisile omogućava počinitelju dugotrajno izbjegavanje otkrivanja i eskalaciju zlostavljanja. Dizajn određenih platformi dodatno komplikuje forenzički rad. Tako Discord kao platforma dominantno korištena u gaming zajednicama omogućava stvaranje privatnih servera, zatvorenih kanala i prostora koji nadziru isključivo administratori, bez mogućnosti vanjskog nadzora. U tom okruženju groomer može koristiti brze, višesmjerne razgovore koji se odvijaju paralelno u više kanala, što stvara dodatnu složenost u kasnijem povezivanju digitalnih tragova. Forenzičke poteškoće dodatno se povećavaju kada groomer koristi kombinaciju sinhronih i asinhronih kanala komunikacije, kao što su glasovne poruke, video pozivi i tekstualni chatovi. Problem su i efemeralne, nestajuće poruke koje općenito počinitelju krivičnog djela omogućavaju da sakrije dokaze (Rashid & Mastorakis, 2025), pri čemu su istog svjesni groomeri. Navedeni formati često se ne pohranjuju na jednak način, a pojedine platforme uopšte ne čuvaju sadržaj poziva, poruka, audio-video sadržaja čime se gubi važan segment komunikacijske dinamike. Dodatni izazov predstavlja činjenica da digitalni tragovi ne odražavaju uvijek stvarni slijed događaja, jer groomer može manipulirati vremenom slanja poruka, koristiti VPN servise ili alate za prikrivanje lokacije, što stvara diskrepanciju između tehničkih podataka i stvarnog vremenskog toka interakcije.

4. FAKTORI RANJIVOSTI I OBRASCI ONLINE VIKTIMIZACIJE DJECE

Online grooming ne zavisi samo od strategija počinitelja i tehničkih karakteristika digitalnog okruženja, nego i od individualnih i socijalnih faktora koji oblikuju ranjivost djeteta. Brojna istraživanja ukazuju da djeca i adolescenti nisu jednako izloženi riziku ulaska u manipulativne interakcije, te da se povećana ranjivost može posmatrati kao rezultat kombinacije ličnih karakteristika, porodične dinamike i digitalne socijalizacije (Mitchell, Finkelhor, Jones, & Wolak, 2012). Groomer procjenjuje ove faktore već u ranim fazama komunikacije, te ciljano pristupa djeci koja pokazuju emocionalne potrebe, želju za pažnjom ili nedostatak stabilne podrške. Iz tog razloga razumijevanje ranjivosti ne predstavlja samo psihološki okvir, nego kriminološki element koji objašnjava zbog čega su neke skupine djece statistički češće izložene manipulativnim oblicima komunikacije. Online viktimizacija stoga nije jednokratan događaj, nego proces u kojem ranjivost djeteta i taktičke odluke počinitelja djeluju međusobno i istovremeno.

4.1. Individualni i psihosocijalni faktori ranjivosti djece

Individualni i psihosocijalni faktori predstavljaju jednu od najvažnijih determinanti rizika u online interakcijama. Istraživanja EU Kids Online (Livingstone, Haddon, Görzig, & Ólafsson, 2011) i radovi Whittle, Hamilton-Giachritsis i Beech (2013) pokazuju da djeca koja se osjećaju usamljeno, izolirano ili emocionalno zapušteno češće prihvataju komunikaciju s nepoznatim osobama na internetu. Niska razina samopoštovanja, potreba za potvrdom ili osjećaj nepripadanja vršnjačkoj grupi mogu stvoriti prostor u kojem dijete komunikaciju s groomerom doživljava kao izvor pažnje i emocionalne stabilnosti. Dodatni faktor ranjivosti predstavlja sklonost djece da dijele lične informacije i da digitalnu komunikaciju doživljavaju kao prostor u kojem mogu iskazati emocije bez straha od neposrednih posljedica. Studije Ybarra i Mitchell (2004) ukazuju da djeca s izraženijim internaliziranim problemima, poput anksioznosti i depresivnosti, češće razvijaju rizične online obrasce ponašanja, jer komunikaciju s nepoznatima percipiraju kao manje opasnu i potencijalno podržavajuću. Iako je istraživanje provedeno prije više od dvije decenije, njegov značaj nije umanjen, jer razvoj novih komunikacijskih platformi uključujući društvene mreže, forume i aplikacije sa visokim stepenom anonimnosti dodatno proširuje mogućnosti groomera da identifikuje ranjive korisnike. Servisi koji omogućavaju tematsko okupljanje mladih, privatne kanale i komunikaciju u stvarnom vremenu kreiraju okruženje u kojem se emocionalne slabosti djece lakše prepoznaju i ciljano iskorištavaju. U takvim okolnostima groomer prilagođava ton, sadržaj i dinamiku komunikacije tako da pojača osjećaj razumijevanja, prihvatanja i posebnosti odnosa. Kada dijete u groomeru prepozna emocionalni oslonac, proces viktimizacije postaje postepen i teško uočljiv, jer manipulacija ne djeluje prijeteće nego afirmativno. Ranjivost ne proizlazi samo iz deficita, nego i iz razvojnih specifičnosti dječije percepcije rizika. Adolescenti prirodno imaju smanjenu sposobnost procjene dugoročnih posljedica i izraženu potrebu za eksperimentisanjem (Yan & Brocksen, 2013; Maslowsky, Owotomo, Huntley, & Keating, 2019), što povećava vjerovatnoću ulaska u komunikacije koje se na početku čine bezopasnim. Dijete u digitalnom okruženju često nema jasnu predodžbu o tome kako se manipulacija razvija, niti razumijeva da grooming predstavlja proces u kojem se granice pomjeraju postepeno, a ne naglo. Zbog toga individualna ranjivost nije samo pitanje ličnosti ili odgoja, nego dio šireg obrasca u kojem se razvojne karakteristike djeteta uklapaju u manipulativne strategije online počinitelja.

4.2. Porodični i okolinski faktori rizika

Porodično okruženje predstavlja jedan od ključnih zaštitnih ili rizičnih faktora u online interakcijama djece, a njegova uloga posebno dolazi do izražaja u kontekstu groominga. Istraživanja dosljedno pokazuju da djeca koja odrastaju u emocionalno nestabilnim ili konfliktima opterećenim porodicama češće traže podršku izvan doma i sklonija su razvoju intenzivnih online odnosa sa nepoznatim osobama (Jeffery, 2024; Niklova, 2025). Nedostatak porodične stabilnosti, niska razina komunikacije i odsutnost emocionalne dostupnosti roditelja stvaraju ambijent u kojem dijete digitalni prostor percipira kao alternativni izvor pažnje i razumijevanja. Groomeri ciljano prepoznaju ovakve obrasce i koriste ih kao osnovu za postupno građenje odnosa koji zamjenjuje ono što dijete ne dobija u realnom okruženju. Hovanova (2025) naglašava da djeca koja provode vrijeme na internetu

bez jasnih pravila, bez nadzora ili bez otvorene komunikacije o digitalnim rizicima imaju znatno veću vjerovatnoću ulaska u rizične online interakcije. Problem nije samo u tehničkom nadzoru, nego u nedostatku povjerenja zbog kojeg dijete ne prijavljuje sumnjive kontakte roditeljima, već ih pokušava riješiti samo. U takvim situacijama groomer preuzima poziciju savjetnika ili emocionalnog oslonca (O'Connell, 2003), čime se smanjuje vjerovatnoća da će komunikacija biti otkrivena u ranoj fazi i povećava rizik od dalje manipulacije. Djeca iz porodica sa nižim socioekonomskim statusom često imaju ograničen pristup strukturiranim aktivnostima i sigurnim društvenim prostorima, pa veći dio socijalizacije ostvaruju putem interneta (Rouchun, Zongkui, Shuailei, Qingqi, & Chen, 2019). Digitalno okruženje u takvim slučajevima postaje dominantni prostor socijalnog učenja, u kojem djeca razvijaju prijateljske i povjerljive odnose bez adekvatnih mehanizama provjere ili zaštite (Bettencourt, 2014). Odsustvo nadzora i nedostatak digitalne pismenosti kod roditelja dodatno otežavaju prepoznavanje ranih znakova manipulacije. U porodicama gdje postoji hronični stres, višestruke obaveze, migracije, razvod ili nestabilni radni uslovi, djeca često provode značajan dio vremena u online prostoru bez strukture i nadzora. Ova situacija stvara otvoren prostor za groomera da se pozicionira kao stabilna, predvidiva i „sigurna" figura, što je posebno opasno u sredinama gdje je emocionalna podrška fragmentirana ili nedostupna. Empirijska istraživanja Ybarra i Mitchell (2004) pokazuju da djeca koja imaju slabiji odnos s roditeljima i nižu razinu percipirane podrške češće ulaze u interakcije s online strancima, pri čemu je rizik od manipulacije proporcionalan stepenu emocionalne izoliranosti.

4.3. Digitalna kultura i obrasci komunikacije kod djece i adolescenata

Digitalna kultura oblikuje način na koji djeca i adolescenti komuniciraju, izražavaju se i razvijaju odnose, pa samim tim utiče i na modalitete njihove ranjivosti. Istraživanja EU Kids Online projekta ukazuju da mladi doživljavaju digitalne platforme kao prostor u kojem mogu slobodnije izražavati emocije nego u offline okruženju, što rezultira brzim razvojem povjerljivosti i intenzivnih odnosa sa osobama koje ne poznaju u stvarnom životu (Towner, Grint, Levy, Blakemore, & Tomova, 2022). Ova kultura neposrednosti i emocionalne transparentnosti stvara uslove u kojima groomer može neprimjetno preuzeti ulogu osobe od povjerenja, jer se njegova komunikacija uklapa u norme koje mladi već prihvataju kao uobičajene. Valkenburg, Sumter i Peter (2011) naglašavaju da online okruženje olakšava proces samootkrivanja, pri čemu adolescenti često dijele informacije koje ne bi izrekli u offline kontaktu. Ovakav obrazac komunikacije otvara mogućnost za „brzu intimnost", fenomen u kojem emocionalna veza nastaje znatno brže nego što je razvojno uobičajeno, a razlika između vršnjačke komunikacije i manipulativnog pristupa postaje teško uočljiva. Groomer koristi ovu dinamiku tako što oponaša komunikacijske stilove karakteristične za vršnjačke odnose, te prilagođava ton i tempo interakcije očekivanjima djeteta. Digitalna komunikacija omogućava razvoj odnosa koji se odvijaju u kontinuiranom, gotovo neprekinutom toku, što ubrzava proces emocionalne vezanosti i otežava prepoznavanje granica. Uhls i saradnici (2024) navode da online interakcije zbog svoje stalne dostupnosti i ritma postaju poseban razvojni kontekst za adolescente, u kojem uče o odnosima, povjerenju i intimnosti. U nedostatku jasnih struktura i zaštitnih mehanizama, ova dinamika može postati okruženje visokog rizika u kojem djeca prihvataju manipulativne forme komunikacije kao dio uobičajenog digitalnog ponašanja.

5. STRUKTURNI FAKTORI RIZIKA I IMPLIKACIJE ZA PREVENCIJU

5.1. Strukturni faktori rizika u digitalnom okruženju

Fenomen online groominga ne može se posmatrati isključivo kroz individualne karakteristike počinioca ili žrtve, već zahtijeva razumijevanje šireg strukturnog okvira koji omogućava da manipulativni procesi nesmetano funkcionišu. Digitalno okruženje u kojem djeca i adolescenti svakodnevno borave oblikovano je arhitektonskim, tehnološkim i društvenim pravilima koja stvaraju pogodnu infrastrukturu za kontakte s nepoznatim osobama, uključujući one s namjerom seksualne eksploatacije. Ovakva struktura online prostora stvara ambijent u kojem groomer ne mora aktivno tragati za žrtvama, nego se često pozicionira unutar digitalnih zajednica u kojima se ranjiva djeca prirodno okupljaju, poput gaming platformi, kreativnih foruma ili interesnih grupa. Dodatni rizik proizlazi iz načina na koji su digitalne platforme dizajnirane da stimulišu što duže zadržavanje korisnika. Algoritmi koji preporučuju sadržaje zasnovane na prethodnim interakcijama doprinose formiranju „eho-komora" i specifičnih digitalnih kultura u kojima se djeca i adolescenti osjećaju prihvaćeno i razumijeno. Unutar takvih zajednica, gdje se podstiče visoka frekvencija komunikacije i razmjena ličnih informacija, groomer može neprimjetno procjenjivati emocionalne potrebe, obrasce ponašanja i potencijalne slabosti djece. Strukturni faktori rizika uključuju i digitalne navike djece, posebno njihovu sklonost da digitalni prostor doživljavaju kao sigurno mjesto za emocionalno izražavanje i povjeravanje (Towner, Grint, Levy, Blakemore, & Tomova, 2022). U kontekstu porodica koje se suočavaju s emocionalnim stresom, konfliktima ili nedostatkom vremena, djeca često prelaze u online okruženje tražeći podršku, razumijevanje ili pripadnost (Mustafa, Rose, & Ishak, 2020). U takvim situacijama groomer ima pristup djeci koja već osjećaju emocionalnu prazninu i pokazuju pojačanu potrebu za validacijom.

5.2. Operativne i institucionalne prepreke prevenciji online groominga

Prevencija online groominga ne zavisi isključivo od individualnog ponašanja djece, roditelja ili nastavnika, nego u velikoj mjeri od operativnih i institucionalnih kapaciteta društva da prepozna, adresira i ograniči ovaj oblik rizika. Jedan od ključnih problema predstavlja nedostatak specijaliziranih resursa i stručnjaka koji razumiju psihološke, tehnološke i sociokulturne aspekte groominga, budući da većina institucija i dalje funkcioniše prema tradicionalnim modelima zaštite djece koji nisu prilagođeni digitalnim formama manipulacije (Rughiniş, Vulpe, Ţurcanu, & Rosner, 2025). U takvim uslovima značajan broj slučajeva prolazi ispod radara, jer se rizične interakcije ne prepoznaju kao potencijalno opasne sve do trenutka kada se šteta već desi. Poseban izazov predstavlja ograničena saradnja institucija sa globalnim digitalnim platformama, koje posjeduju ključne podatke o korisnicima, komunikaciji i tehničkim tragovima. Razlike u zakonodavstvima, tehničkim standardima i politikama privatnosti dovode do situacije u kojoj nacionalne institucije često nemaju pravovremen pristup relevantnim informacijama. Ova fragmentacija odgovornosti rezultira sporim reakcijama, nedovoljno potpunim dokazima i izostankom sistemske prevencije. U mnogim društvima dodatni problem predstavlja i percepcija online rizika kao sekundarnog ili manje ozbiljnog u odnosu na fizičko nasilje. Takva percepcija utiče na prioritetizaciju resursa, brzinu reakcije i spremnost institucija da investiraju u savremene oblike digitalne zaštite djece. Rezultat je situacija u kojoj je preventivni sistem reaktivan

umjesto proaktivan (Maryam, Najafi, & Amirhasan, 2025), oslanjajući se na prijave i izuzetne slučajeve umjesto na kontinuirano praćenje obrazaca ponašanja i pravovremenu edukaciju. Dodatni problem predstavlja fragmentiranost institucionalnih nadležnosti u oblasti zaštite djece u digitalnom prostoru (Dymytriieva, 2024). Prevencija online groominga često se nalazi na podjeli između obrazovnog, socijalnog, policijskog i pravosudnog sistema, pri čemu nijedna institucija nema jasno definisanu vodeću ulogu u koordinaciji preventivnih aktivnosti. Ovakav model disperzije odgovornosti rezultira situacijom u kojoj se rizici prepoznaju parcijalno, informacije se ne razmjenjuju sistematski, a reakcije zavise od individualne procjene i angažmana pojedinaca unutar sistema, a ne od jasno uspostavljenih procedura. Nedostatak analitičkih i obavještajnih kapaciteta usmjerenih na prepoznavanje obrazaca online groominga je još jedan od ključnih probelam ovog fenomena (Milon-Flores & Cordeiro, 2022). Institucije se uglavnom oslanjaju na prijave, dok proaktivni modeli koji uključuju analizu ponašanja, digitalnih tragova i ponavljajućih obrazaca komunikacije ostaju slabo razvijeni ili u potpunosti izostaju. Time se propušta mogućnost rane identifikacije potencijalno opasnih interakcija koje još uvijek nisu rezultirale direktnom štetom, ali nose visok rizik eskalacije (Taylor, 2015).

5.3. Obrasci online groominga u savremenim digitalnim okruženjima djece i mladih

Savremena digitalna okruženja u kojima djeca i mladi svakodnevno borave ne predstavljaju samo tehničke platforme za zabavu, komunikaciju ili razmjenu sadržaja, već složene socijalne prostore u kojima se formiraju odnosi povjerenja, hijerarhije i osjećaj pripadnosti. Ta kombinacija interakcije, dostupnosti i prividne sigurnosti čini ih pogodnim za razvoj obrazaca online groominga koji su suptilni, postepeni i teško prepoznatljivi u ranim fazama. Grooming u ovim okruženjima rijetko se pojavljuje kao izolirani čin, već kao proces koji se odvija kroz niz svakodnevnih, naizgled benignih interakcija koje vremenom mijenjaju granice prihvatljivog ponašanja. Empirijska istraživanja potvrđuju da se online grooming ne može posmatrati kao linearna ili jednoobrazna aktivnost, već kao kompleksan i varijabilan proces koji uključuje niz prilagodljivih taktika i strategija, često teško prepoznatljivih u ranim fazama interakcije (Ali, Haykal, & Youssef, 2021). Obrasci seksualne manipulacije variraju od slučaja do slučaja, pri čemu pojedinačne interakcije same po sebi rijetko predstavljaju jasan indikator rizika. U nastavku će se posmatrati slučajevi grooming tri online platforme za komunikaciju koje najčešće koriste djeca, a to su Roblox, Discord i Reddit.

Roblox: U digitalnim prostorima zasnovanim na igri i saradnji, poput Roblox-a, grooming se često prikriva kroz zajedničke aktivnosti, razmjenu savjeta i mentorski odnos između starijih i mlađih korisnika. Funkcionalna logika igre, u kojoj su nagrade, napredovanje i socijalni status centralni motivatori, omogućava počiniocima da uspostave asimetričan odnos moći bez otvorene prisile. Djeca takve interakcije često ne doživljavaju kao rizične, jer su uklopljene u kontekst igre i percipirane kao dio normalne online socijalizacije. Dokumentovani sudski slučajevi ukazuju da su online igre poput Robloxa korištene kao inicijalna tačka za uspostavljanje kontakta, izgradnju povjerenja i privatnu komunikaciju s djecom, što je u pojedinim slučajevima rezultiralo višestrukim krivičnim djelima povezanima s online groomingom i seksualnom eksploatacijom maloljetnika (Turnnidge, 2025). Sudski nalazi potvrđuju da su počinioci koristili komunikacijske funkcije igre kako bi zaobišli nadzor i

nastavili interakciju izvan vidokruga roditelja i institucija, čime se značajno otežava rana detekcija ovakvih obrazaca ponašanja. Sudski postupci dodatno ukazuju na sistemske propuste u dizajnu i upravljanju platformom, posebno u pogledu neadekvatne moderacije in-game komunikacije, izostanka efikasne verifikacije dobi i tolerisanja prelaska komunikacije na vanjske aplikacije, što omogućava da se grooming razvija kroz naizgled benignu igru i socijalne interakcije (Miller, 2025). U pojedinim slučajevima, ovakvi obrasci su eskalirali u teške oblike fizičke eksploatacije maloljetnika, uključujući otmicu i višednevno zlostavljanje, pri čemu sudska dokumentacija potvrđuje da se ne radi o izoliranim incidentima, već o predvidivim posljedicama strukturnih slabosti platforme (Gagnon, 2025).

Discord: Slični obrasci uočavaju se i u komunikacijskim okruženjima zasnovanim na zatvorenim zajednicama, poput Discord-a, gdje struktura servera, hijerarhija uloga i ograničen pristup kanalima omogućavaju postupnu izolaciju potencijalnih žrtava. Analize online interakcija pokazuju da normalizacija seksualiziranog jezika, šala i sadržaja predstavlja jednu od ključnih taktika groominga, jer postupno mijenja percepciju prihvatljivog ponašanja kod djece i mladih. Ovakav pristup omogućava da se seksualna tematika uvodi indirektno, kroz grupni kontekst, umjesto kroz direktan pritisak (Pranoto, Gunawan, & Soewito, 2015). Izvještaji pokazuju da su komunikacijski servisi poput Discord-a bili povezani sa značajnim brojem krivičnih postupaka koji uključuju otmice djece, online grooming i distribuciju materijala seksualnog zlostavljanja djece. Prema dostupnim podacima, identifikovani su i brojni aktivni serveri posvećeni eksploataciji djece, dok je sama platforma priznala da postojeći mehanizmi detekcije obuhvataju tek dio stvarnog obima problema, što dodatno potvrđuje ograničenja trenutnih modela moderacije (Goggin & Ingram, 2023). Rizik predstavlja i činjenica da su manji i privatni serveri često slabo moderirani, što omogućava dugotrajno djelovanje bez institucionalnog nadzora. U takvom kontekstu, djeca i mladi se suočavaju s pritiskom zajednice da prihvate obrasce ponašanja koji bi u offline okruženju bili prepoznati kao neprihvatljivi. Organizirane online grupe, poput mreže poznate kao „764“, koriste komunikacijske platforme namijenjene djeci i mladima za sistematsko ciljanje ranjivih maloljetnika s ciljem ucjene, prisiljavanja na samopovređivanje i proizvodnju materijala seksualnog zlostavljanja djece (Fletcher, Tzani, & Ioannu, 2025). Djelovanje ovakvih grupa odvija se višekanalno i transplatformski, uz oslanjanje na zatvorene servere, psihološku manipulaciju i dugotrajni nadzor žrtava, što značajno otežava ranu detekciju i institucionalnu intervenciju (Fletcher, Tzani, & Ioannu, 2025). Sudski postupci pokrenuti protiv Discord-a ukazuju na to da je platforma u pojedinim slučajevima omogućila online grooming i seksualnu eksploataciju maloljetnika usljed nedostatka osnovnih zaštitnih mehanizama, uključujući efikasnu verifikaciju dobi, proaktivnu moderaciju i roditeljske kontrole. Tužbeni navodi dodatno ističu da se moderacija u velikoj mjeri oslanja na samoprijavljivanje korisnika, dok su maloljetnici izloženi neograničenim privatnim komunikacijama i eksplicitnim kanalima, što značajno povećava rizik od manipulacije i zlostavljanja (Singleton Schreiber, 2025).

Reddit: Anonimna i tematski strukturirana digitalna okruženja, kakva karakteriše Reddit, dodatno komplikuju prevenciju online groominga. Istraživanja komunikacije između maloljetnika i počinilaca pokazuju da eskalacija online groominga može nastupiti izuzetno

brzo. U pojedinim dokumentovanim slučajevima, već nakon nekoliko dana online interakcije dolazi do uspostavljanja povjerenja i pristanka djece na dijeljenje privatnih fotografija, što dodatno komplikuje mogućnosti pravovremene institucionalne intervencije (Nikolovska, 2020). Anonimnost omogućava groomerima da se predstave kao empatični sagovornici, savjetnici ili osobe koje dijele slična iskustva, posebno u zajednicama koje se bave ličnim problemima, emocionalnim krizama ili identitetskim pitanjima. Grooming se u tim slučajevima često odvija kroz diskurs podrške i razumijevanja, pri čemu se povjerenje gradi prije nego što se započne sa postepenim pomjeranjem komunikacije u privatne poruke. Takvi obrasci omogućavaju izgradnju emocionalne zavisnosti prije nego što se započne sa eksplicitnijim oblicima seksualne manipulacije (Ali, Haykal, & Youssef, 2021; Quayle, 2020). Empirijska analiza tematskih zajednica na Reddit-u pokazuje da se platforma često koristi kao prostor za razmjenu iskustava o seksualnom zlostavljanju djece, ali i za identifikaciju, prijavljivanje i neformalno mapiranje sumnjivih online ponašanja i potencijalnih predatora. Iako takve zajednice doprinose podizanju svijesti, nalazi ukazuju i na to da se informacije o grooming obrascima, rizičnim platformama i sumnjivim akterima često dijele izvan institucionalnih kanala, što potvrđuje postojanje paralelnog, neformalnog sistema reakcije na online rizike (Simhadri & Ringenberg, 2023). Dokumentovani slučajevi iz prakse ukazuju da su mehanizmi moderacije na platformama poput Reddita u pojedinim situacijama reagovali sa značajnim zakašnjenjem, čak i kada se radilo o dijeljenju seksualno eksplicitnog materijala koji uključuje maloljetnike. U jednom takvom slučaju, žrtva je bila primorana samostalno identificirati i prijavljivati sadržaj u više zajednica, dok su institucionalni i moderatorski odgovori bili fragmentirani i nedovoljno efikasni, što je omogućilo dugotrajniju dostupnost nezakonitog materijala (Fingas, 2021). Ovakvi obrasci su posebno teško uočljivi jer ne uključuju otvorene oblike seksualizacije u ranim fazama, već se oslanjaju na emocionalnu vezanost i zavisnost.

6. ZAKLJUČAK

Online grooming predstavlja jedan od najsloženijih i najteže prepoznatljivih oblika seksualne viktimizacije djece, upravo zbog svoje procesne i relacijske prirode. Umjesto neposredne prisile ili fizičkog kontakta, grooming se zasniva na postepenoj izgradnji emocionalne veze, psihološkoj manipulaciji i sistematskom pomjeranju granica prihvatljivog ponašanja, pri čemu dijete postepeno gubi sposobnost da prepozna rizik i ugroženost. Analiza kriminalnih, psiholoških i komunikacijskih obrazaca pokazuje da grooming gotovo uvijek prolazi kroz više faza u kojima se namjera počinioca prikriva prividom brige, razumijevanja i bliskosti, što ovaj oblik eksploatacije čini posebno podmuklim i otpornim na ranu detekciju. Digitalno okruženje dodatno pojačava navedene rizike, ne samo zbog anonimnosti i brzine komunikacije, nego i zbog same arhitekture savremenih digitalnih platformi koje omogućavaju fragmentaciju identiteta, nestabilnost digitalnih tragova i istovremeno korištenje više komunikacijskih kanala. Korištenje pseudonima, višestrukih profila i privremenih naloga omogućava počiniocima da kontinuirano prilagođavaju svoj digitalni identitet, otežavajući pouzdanu identifikaciju i praćenje njihovog djelovanja. Istovremeno, funkcionalnosti poput nestajućih poruka, privatnih kanala i preusmjeravanja komunikacije na vanplatformske aplikacije dodatno smanjuju trajnost i dostupnost relevantnih digitalnih dokaza. Ovakvi tehnički i organizacijski uslovi stvaraju ozbiljne kriminalističke i forenzičke

izazove, jer otežavaju rekonstrukciju kompletnog toka komunikacije i onemogućavaju cjelovit uvid u razvoj manipulativnog odnosa kroz vrijeme. Strukturni faktori rizika igraju ključnu ulogu u nastanku i razvoju online groominga, jer oblikuju kontekst unutar kojeg se manipulativni odnosi mogu razvijati gotovo neprimjetno. Emocionalna ranjivost djece, porodični stres, nedostatak adekvatnog nadzora, ali i algoritamske logike digitalnih platformi, komercijalni interesi i ograničeni institucionalni kapaciteti ne djeluju izolirano, već čine međusobno povezan sistem u kojem se rizik kumulativno povećava. U takvom sistemu pojedinačne slabosti se nadovezuju jedna na drugu, stvarajući prostor u kojem groomeri mogu dugotrajno djelovati bez ranog uočavanja ili pravovremene intervencije. Efikasni preventivni modeli moraju obuhvatiti razvoj digitalne pismenosti koji ide dalje od osnovnih sigurnosnih savjeta i uključuje razumijevanje manipulativnih obrazaca i emocionalnih strategija koje počinioci koriste. Istovremeno, nužno je jačanje profesionalnih, analitičkih i operativnih kapaciteta institucija koje se bave zaštitom djece, kao i uspostavljanje funkcionalne i obavezujuće saradnje s tehnološkim kompanijama. Razvoj javnih politika koje prepoznaju procesnu prirodu manipulacije, umjesto fokusiranja isključivo na pojedinačne incidente, predstavlja ključni korak ka izgradnji održivog sistema prevencije koji može odgovoriti na stvarne rizike digitalnog okruženja.

7. LITERATURA

1. Ali, S., Haykal, H. A., & Youssef, E. Y. (2021). Child Sexual Abuse and the Internet—A Systematic Review. *ARENA OF TECHNOLOGIES*.
2. Ashcroft, M., Kaati, L., & Meyer, M. (2015). A Step Towards Detecting Online Grooming -- Identifying Adults Pretending to be Children. *European Intelligence and Security Informatics Conference*, (str. 98-104).
3. Bettencourt, A. (2014). *Empirical Assessment of Risk Factors: How Online and Offline Lifestyle, Social Learning, And Social Networking Sites Influence Crime Victimization.* Bridgewater State University, BSU Master's Theses.
4. Chen, L., & Jiang, Y. (2025). Social media as a counter-public sphere? Chinese feminist activism empowered by hashtags. *Feminist Media Studies*.
5. Chiang, E., & Grant, T. (2017). Online grooming: moves and strategies. *Language and Law*, 103-141.
6. Council of Europe. (2015). *Opinion on Article 23 of the Lanzarote Convention and its explanatory note.* Council of Europe.
7. Davidson, J., & Gottschalk, P. (2011). Characteristics of the Internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies*, 23-36.
8. DeHart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2016). Internet sexual solicitation of children: a proposed typology of offenders based on their chats, emails, and social network posts. *Journal of Sexual Agression*.
9. Dymytriieva, O. I. (2024). STATE POLICY OF CHILD PROTECTION IN CYBERSPACE AS A PRIORITY OF HUMAN SECURITY: A RETROSPECTIVE OF FORMATIO. *Global Prosperity*.
10. ECPAT. (2020). *Summary paper on Online Child Sexual Exploitation.* Bangkok: ECPAT International.

11. ECPAT International and WeProtect Global Alliance. (2022). *Child Sexual Abuse and Exploitation Online: Survivors Perspectives.* WeProtect Global Alliance.
12. Fingas, J. (25. 04 2021). *Reddit sued for failing to pull child sexual abuse content*. Preuzeto od Yahoo!Tech: https://tech.yahoo.com/general/article/reddit-lawsuit-over-child-sexual-abuse-content-175310256.html
13. Fletcher, R., Tzani, C., & Ioannu, M. (2025). Danger on Discord: How 764 prey on and extort minors. *Assessment and Development Matters*, 59-63.
14. Gagnon, K. (04. 08 2025). *13-Year-Old Groomed, Kidnapped Through Roblox: Family Sues Gaming Giant*. Preuzeto od Milberg: https://milberg.com/news/13-year-old-groomed-kidnapped-through-roblox-family-sues-gaming-giant/
15. Goggin, B., & Ingram, D. (22. 06 2023). *'It's horrifying': Discord CEO on child abuse issues after NBC News investigation*. Preuzeto od NBC News: https://www.nbcnews.com/tech/social-media/discord-ceo-child-safety-ai-server-deepfake-rcna90676
16. Heath, H., MacDermott, Á., & Akinbi, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation*.
17. Hovanová, M. (2025). A MODEL OF RISKY BEHAVIOR ON SOCIAL NETWORKS THROUGH PARENTAL ATTACHMENT AND PARENTAL MEDIATION. *Journal of Psychological and Educational Research*, 90-107.
18. International Centre for Missing & Exploited Children. (2017). *Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review.* International Centre for Missing & Exploited Children.
19. Jeffery, C. P. (2024). 'Trust us! We know what we are doing!' Parent-adolescent digital conflict in Australian families. *Journal of Children and Media*, 472-488.
20. Katz, C., & Barnetz, Z. (2016). Children's narratives of alleged child sexual abuse offender behaviors and the manipulation process. *Psychology of Violence*, 223–232.
21. Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online Child Sexual Exploitation. *Trauma, Violence & Abuse*, 126-140.
22. Lanning, K. V. (2010). *Child Molesters: A Behavioral Analysis.* National Center for Missing & Exploited Children.
23. Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU Kids Online: final report 2011*. London: LSE.
24. Maryam, D., Najafi, T. A., & Amirhasan, N. (2025). Iran's legislative response to the victimization of children in cyberspace: a criminal policy perspective. *Publicationes Universitatis Miskolcinensis, Sectio Juridica Et Politica*, 199–219.
25. Maslowsky, J., Owotomo, O., Huntley, E. D., & Keating, D. (2019). Adolescent Risk Behavior: Differentiating Reasoned And Reactive Risk-taking. *Journal of Youth and Adolescence*, 243–255.
26. Miller, R. V. (19. 12 2025). *Roblox Child Sex Abuse Lawsuit*. Preuzeto od Lawsuit Information Center: https://www.lawsuit-information-center.com/roblox-sex-abuse-lawsuit.html

27. Milon-Flores, D. F., & Cordeiro, R. L. (2022). How to take advantage of behavioral features for the early detection of grooming in online conversations. *Knowledge-Based Systems*.
28. Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012). Prevalence and characteristics of youth sexting: a national study. *Pediatrics*.
29. Moses, C. (26. 10 2024). *U.K. Man Who Posed as a Girl to Extort Teens Online Gets 20 Years in Prison*. Preuzeto od The New York Times: https://www.nytimes.com/2024/10/26/world/europe/catfish-northern-ireland-manslaughter.html
30. Mustafa, M. Y., Rose, N. N., & Ishak, A. S. (2020). Internet Addiction and Family Stress: Symptoms, Causes and Effects. *Journal of Physics: Conference Series*.
31. Niklova, M. (2025). Current Threats to the Family – Current Issues and Problems. U A. M. Kochanowicz, M. Witkowski, & D. Jorg, *FAMILY DYNAMICS in a Changing World: Support, Challenges, and Adaptation* (str. 157-166). WSB University, Poland.
32. Nikolovska, M. (2020). *The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children.* Jyväskylän yliopisto, Doctoral thesis.
33. O'Connell, R. (2003). *A Typology of Child Cybersexploitation and Online Grooming Practices.* Cyberspace Research Unit, University of Central Lancashire.
34. Pranoto, H., Gunawan, F. E., & Soewito, B. (2015). Logistic Models for Classifying Online Grooming Conversation. *ScienceDirect*, 357 – 365.
35. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum*, 429–447.
36. Rashid, E., & Mastorakis, N. E. (2025). Elimination and Analysis of Ephemeral Messages in Android Social Media Apps: A Forensic Perspective. *International Journal of Computers*, 94-102.
37. Reneses, M., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2024). "He Flattered Me". A Comprehensive Look Into Online Grooming Risk Factors: Merging Voices of Victims, Offenders and Experts Through In Depth Interviews. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*.
38. Rouchun, D., Zongkui, Z., Shuailei, L., Qingqi, L., & Chen, G. (2019). Family socioeconomic status and the parent-child relationship: Children's Internet use as a moderated mediator. *Current Psychology*, 4384–4393.
39. Rughiniş, R., Vulpe, S.-N., Ţurcanu, D., & Rosner, D. (2025). Balancing act: Europeans' privacy calculus and security concerns in online CSAM detection. *Frontiers in Big Data*.
40. Simhadri, S. S., & Ringenberg, T. (2023). Child Sexual Abuse Awareness and Support Seeking on Reddit: A thematic Analysis. *WWW '23 Companion: Companion Proceedings of the ACM Web Conference 2023*, (str. 267 - 271). Austin, TX, USA.
41. Singleton Schreiber. (16. 09 2025). *Lawsuit Filed Against Discord for Enabling Child Sexual Exploitation*. Preuzeto od Singleton Schreiber:

https://www.singletonschreiber.com/newsroom/pressreleases/lawsuit-filed-against-discord-for-enabling-child-sexual-exploitation
42. Sorell, T. (2016). Online Grooming and Preventive Justice. *Crime, Law and Philosophy*.
43. Taylor, J. (2015). Online investigations: protection for child victims by raising awareness. *ERA Forum*, 349–358.
44. Towner, E., Grint, J., Levy, T., Blakemore, S.-J., & Tomova, L. (2022). Revealing the self in a digital world: A systematic review of adolescent online and offline self-disclosure. *Current Opinion in Psychology*.
45. Turnnidge, S. (23. 10 2025). *Man who groomed kids on Roblox and Fortnite jailed*. Preuzeto od BBC: https://www.bbc.com/news/articles/cglgx09z82ko
46. Uhls, Y. T., Wal, A. v., Ellison, N., Collier, A., Subrahmanyam, K., & Valkenburg, P. M. (2024). Adolescents' Online Communication Practices in a Digital World. U D. A. Christakis, & L. Hale, *Handbook of Children and Screens* (str. 215–221). Springer.
47. UNODC. (2020). *Online child sexual exploitation and abuse*. Preuzeto od UNODC: https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html
48. Valkenburg, P. M., Sumter, S. R., & Peter, J. (2011). Gender differences in online and offline self-disclosure in pre-adolescence and adolescence. *British Journal of Developmental Psychology*, 253-269.
49. van Dam, C. (2001). *Identifying Child Molesters: Preventing Child Sexual Abuse by Recognizing the Patterns of Offenders.* New York: Haworth Press.
50. van Dam, C. (2006). *The Socially Skilled Child Molester: Differentiating the Guilty From the Falsely Accused.* New York: Haworth Press.
51. Wefers, S., Dieseth, T., George, E., Øverland, I., Jolapara, J., McAree, C., & Findlater, D. (2024). Understanding and Deterring Online Child Grooming: A Qualitative Study. *Sexual Offending: Theory, Research, and Prevention*.
52. Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). "Under His Spell": Victims' Perspectives of Being Groomed Online. *Social Sciences*, 404-426.
53. Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior*, 135-146.
54. Winters, G. M., & Jeglic, E. L. (2017). Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molesters. *Deviant Behavior*, 724-733.
55. Yan, J., & Brocksen, S. (2013). Adolescent risk perception, substance use, and educational attainment. *Journal of Risk Research*, 1037-1055.

SPECIFICS OF ONLINE GROOMING AND CRIMINOLOGICAL IMPLICATIONS OF THE DIGITAL ENVIRONMENT

***Abstract**: the paper analyzes the specific features of online grooming as a process-based and manipulative form of child sexual exploitation, with a special focus on the psychological, criminal, and digital dimensions of this phenomenon. The theoretical section presents the stages of manipulation, offender typologies, and behavior patterns that enable the creation of a seemingly safe relationship between the child and the groomer. Special attention is given to the digital environment which, through its technical features, anonymity, and multi-platform infrastructure, allows the fragmentation of traces and makes the reconstruction of the communication flow more difficult. Structural risk factors are also analyzed, including children's emotional vulnerability, the algorithmic logic of digital services, and limited institutional capacities for prevention. The paper concludes that online grooming is a complex phenomenon that requires an interdisciplinary approach, stronger digital literacy, and the development of preventive strategies that take into account psychological, technological, and social risk factors.*

***Keywords:** online grooming, child sexual exploitation, digital vulnerability, digital traces*

UPUTE ZA AUTORA

Časopis objavljuje radove iz oblasti kriminalistike, kriminologije i prava. Radovi koji zadovoljavaju kriterije, upućuju se na recenziju. Postupak recenziranja je anoniman za autore i recenzente. Ukoliko dostavljeni rad ne spada u oblast Časopisa, isti će biti vraćen autoru. Za prihvaćene priloge se ne plaćaju autorski honorari, niti se naknađuju bilo kakvi drugi troškovi. Jezici na kojima se primaju radovi su: bosanski, hrvatski, srpski, crnogorski (u latiničnom ili ćiriličnom pismu) i engleski jezik. Radovi se dostavljaju isključivo u elektronskoj formi na e-mail adresu:centarkkpi@gmail.com. Maksimalna dužina izvornih, preglednih i stručnih radova može biti jedan tabak ili 16 stranica A4 formata, ili 35.600 karaktera. Redakcija izuzetno može odlučiti da, na prijedlog glavnog urednika, objavi rad obimniji od standardnog obima.

1. Maksimalna dužina ostalih vrsta radova, može biti do 8 stranica A4 formata ili pola autorskog tabaka, ili najviše do 17.800 karaktera.
2. Radu se dodaju sažeci do 150 riječi, na jednom od jezika Časopisa i na engleskom jeziku.
3. Radu se dodaje do 5 ključnih pojmova na jednom od jezika Časopisa i na engleskom jeziku.
4. Pogodni radovi se upućuju na recenziju, a radovi koji se ocijene nepogodnima vraćaju se autorima.
5. Kako bi bio objavljen u Zborniku, svaki rad mora dobiti dvije pozitivne recenzije. U slučaju da je jedna recenzija pozitivna, a jedna negativna, rad se upućuju na treću recenziju.
6. Odluku o prihvaćanju ili neprihvaćanju rada za objavu, te njegovoj kategorizaciji, na prijedlog glavnog urednika, donosi redakcija.
7. Imena recenzenata nisu dostupna autorima. Nakon obavljene recenzije, primjedbe recenzenata se dostavljaju autorima radi usvajanja ili odbijanja. Ukoliko prihvate primjedbe, autori će u roku od 8 dana dostaviti ispravljeni rad.
8. Recenzenti ne znaju ime autora. Autor će prilikom izrade rada izbjeći svoju posrednu identifikaciju kroz tekst rada.
9. Recenzenti svoje recenzije dostavljaju na posebnom obrascu koji dobivaju zajedno sa tekstom za recenziju.
10. Prikazi, osvrti, zabilješke i ostali radovi koji nisu naučni ili stručni se, ne recenziraju. Odluku o njihovom eventualnom ispitivanju i objavljivanju donosi glavni urednik.
11. Radovi koji se dostavljaju Zborniku moraju biti lektorisani. Autori prihvaćaju prava redakcije da lektorisani rad objavi bez daljnjih konsultacija s autorima. Ukoliko za to postoji opravdana potreba, konsultacija se može obaviti sa autorima, na osnovu odluke glavnog urednika.
12. Autori dopuštaju Zborniku korištenje njihovih radova za objavljivanje u bilo kojoj formi (printanoj, online ili sl.). Zbornik zadržava i sva druga prava vezana za objavljivanje, ukoliko nije drugačije ugovoreno sa autorom.
13. Radovi koji su upućeni za objavljivanje u Časopisu, neće i ne mogu biti dostavljeni na objavljivanje u drugoj publikaciji. Nakon što budu objavljeni u Časopisu, radovi u

drugoj publikaciji (uključujući i svaki drugi oblik objavljivanja i distribucije) mogu biti objavljeni isključivo nakon prethodno pribavljenog odobrenja od glavnog urednika.

14. Časopis će objavljivati i sažetke stručnih i naučnih članaka domaćih autora objavljenih u stranim indeksiranim časopisima, ukoliko takvi sažeci budu dostavljeni od autora.

STANDARDI ZA OBLIKOVANJE TEKSTA PRILOGA

1. Tekst rada se dostavlja kao Microsoft Word dokument, uz korištenje Times New Roman fonta veličine 12 pt., uz mogućnost korištenja bold, italic i drugih modifikacija.
2. Naslov rada se piše New Times Roman fontom, boldirano i veličine 14. pt.
3. Podnaslovi se pišu Times New Roman fontom, boldirano i veličine 12. pt. Numeriranje podnaslova je obavezno. Autor određuje samostalno način označavanja. Razmak između redova je 1,0.
4. Početak pasusa mora biti uvučen za pet slovnih mjesta u odnosu na lijevu marginu ili odvojen duplim proredom.
5. Prvi put upotrijebljena kratica ili akronim se označavaju u zagradi iza riječi ili skupine riječi koju označavaju. Prethodna odredba važi i za skraćeno označavanje propisa.
6. Prvi put citiran pravni propis mora biti označen brojem za "fusnotu" i naveden prema broju službenog glasila u kome je objavljen.
7. Napomene se pišu fontom 10. Napomene se nalaze na dnu teksta ("Fusnote").
8. Svaka od četiri margine mora biti veličine 2,5 cm.
9. Na prvoj strani rada nalazi se puno ime i prezime svakog autora, akademska ili druga titula, institucija u kojoj radi – ako je zaposlen. Pored osobnih podataka, na prvoj stranici se nalazi i naslov rada.
10. Na drugoj stranici se daje sažetak i spisak ključnih riječi u skladu s tačkom I, 10 i 11.
11. Spisak obuhvaća korištenu literature po abecednom redu prezimena prvog autora, spisak konsultovanih web-stranica, spisak tabela i popis shema – ako su korištene. Spisak literature sadrži korištene zakone i druge izvore, koji će biti navedeni po kategorijama.

Radovi koji ne budu izrađeni u skladu sa ovim uputama biti će vraćeni autorima !

Redakcija Časopisa

CENTAR ZA KRIMINALISTIČKA, KRIMINOLOŠKA I PRAVNA ISTRAŽIVANJA

.....

SJEDIŠTE REDAKCIJE ČASOPISA
Ul. Školska 23, 72270 Travnik
