ONLINE SEKSUALNA EKSPLOATACIJA DJECE: METODE POČINILACA I ODGOVORI SIGURNOSNIH AGENCIJA

DOI: *10.70329/2744-2403.2025.5.10.8*

Pregledni rad

Aldina Bjelić, MA[1]

Sažetak:

Online seksualna eksploatacija djece predstavlja jedan od najbrže rastućih oblika cyber kriminala, potaknut dinamičnim razvojem digitalnih tehnologija, globalnom povezanosti i širokom dostupnošću komunikacijskih platformi. Počinioci koriste raznovrsne metode kojima ciljaju ranjivu populaciju djece, uključujući grooming, sextortion, socijalni inženjering, kreiranje lažnih identiteta i distribuciju materijala seksualnog zlostavljanja putem enkriptiranih kanala, peer-to-peer mreža i darknet servisa. Tehnološki faktori poput end-to-end enkripcije, kriptovaluta, anonimizacijskih mreža i generativne umjetne inteligencije dodatno otežavaju detekciju i omogućavaju počiniocima visok stepen operativne sigurnosti. Sigurnosne agencije odgovaraju razvojem specijaliziranih timova, jačanjem digitalno-forenzičkih kapaciteta, međunarodnom saradnjom i oslanjanjem na OSINT i SOCMINT metode u identifikaciji počinilaca i praćenju kriminalnih mreža. Ipak, izazovi poput nedostatka kadra, tehničkih barijera, fragmentiranih nadležnosti i brzine tehnoloških promjena i dalje ograničavaju efikasnost institucionalnog odgovora. Pravne i političke mjere, uključujući Budimpeštansku konvenciju i Lanzarote konvenciju, pružaju okvir za djelovanje, ali u praksi ostaje značajan jaz između normativnih zahtjeva i operativnih mogućnosti. Rad naglašava da borba protiv online seksualne eksploatacije djece zahtijeva kombinaciju preventivnih mjera, tehnoloških inovacija, multisektorske saradnje i jačanja kapaciteta sigurnosnih institucija. Zaštita djece u digitalnom prostoru predstavlja ne samo pravni i društveni prioritet nego i ključni faktor ukupne sigurnosne stabilnosti.

Ključne riječi*: cyber kriminal, grooming, sextortion, darknet, OSINT*

[1] aldinabjelic@hotmail.com

1. Uvod

Online seksualna eksploatacija djece predstavlja jedan od najsloženijih i najbrže rastućih izazova savremenog digitalnog okruženja. Razvoj informacijsko-komunikacijskih tehnologija, široka dostupnost interneta i masovna upotreba pametnih telefona otvorili su nove prostore interakcije u kojima djeca provode sve veći dio svakodnevnog života. U takvom ambijentu, tradicionalni obrasci viktimizacije poprimaju nove digitalne dimenzije, a počinioci koriste specifične tehnike prilagođene online okruženju kako bi identifikovali, manipulirali i eksploatisali djecu. Ovaj fenomen dobija na ozbiljnosti jer internet omogućava širok spektar anonimnih i teško detektabilnih aktivnosti koje nadilaze geografske granice i izmiču tradicionalnim oblicima nadzora i kontrole. Istovremeno, globalni porast slučajeva online seksualne eksploatacije djece ukazuje na rastući jaz između brzog tehnološkog napretka i institucionalne sposobnosti da se na adekvatan način zaštiti najranjivija populacija. Sigurnosne i druge agencije suočene su s izazovima poput enkriptiranih komunikacijskih kanala, decentraliziranih mreža, kriptovaluta i generativne umjetne inteligencije, koji dodatno otežavaju identifikaciju počinilaca i procesuiranje krivičnih djela. Iako postoje međunarodni standardi, pravni okviri i specijalizirane jedinice koje se bave ovim oblikom kriminala, njihova efikasnost često zavisi od tehničke opremljenosti, kapaciteta za digitalnu forenziku i nivoa međunarodne saradnje. Uzimajući u obzir navedene okolnosti, cilj ovog preglednog rada je sistematizirati savremene spoznaje o metodama koje online počinioci najčešće koriste, analizirati institucionalne i sigurnosne odgovore, te ukazati na ključne izazove koji oblikuju mogućnosti efikasne prevencije i represije. Namjera je ponuditi jasan i sveobuhvatan pregled literature i praksi koje mogu poslužiti stručnjacima, istraživačima i donositeljima odluka u unapređenju politika zaštite djece u digitalnom prostoru.

2. Definisanje cyber eskploatacije djece

Cyber eksploatacija djece predstavlja skup kriminalnih radnji koje uključuju korištenje informaciono-komunikacijskih tehnologija radi seksualnog iskorištavanja maloljetnih osoba, distribucije ili proizvodnje materijala seksualnog zlostavljanja, manipulacije, iznude ili drugih oblika nedozvoljenog postupanja nad djecom. Prema Lanzarote konvenciji Vijeća Evrope (2007), seksualno iskorištavanje djece obuhvata sve radnje u kojima se dijete koristi u svrhu seksualnog zadovoljstva druge osobe, bez obzira na to odvija li se čin u fizičkom ili digitalnom prostoru. Digitalni prostor omogućava da se ove radnje odvijaju bez fizičkog kontakta, pri čemu počinioci koriste anonimnost, tehničku zaštitu i globalnu dostupnost interneta kako bi izbjegli nadzor i odgovornost. Internet tehnologija omogućava spajanje udaljenih, širenje vijesti i informacija, ali se u navedenom krije i mogućnost manipulacije umom i načinom razmišljanja

svakog misaonog bića (Muhić, 2025).U savremenoj literaturi i praksi najčešće se koristi termin online seksualna eksploatacija djece, odnosno *Online Child Sexual Exploitation*, koji prema izvještajima Europola (2025) obuhvata grooming, sextortion, regrutaciju djece za seksualne aktivnosti putem interneta i distribuciju materijala seksualnog zlostavljanja djece. S tim u vezi, poseban akcenat stavlja se na CSAM (Child Sexual Abuse Material), odnosno materijal koji vizualno prikazuje seksualno zlostavljanje djeteta. Interpol i ECPAT (2018) predlažu sve češću upotrebu termina CSEM (Child Sexual Exploitation Material), naglašavajući da fokus nije samo na prikazu zlostavljanja, nego na eksploataciji koja stoji iza nastanka takvog sadržaja.

Jedan od najznačajnijih elemenata cyber eksploatacije je grooming, proces manipulativne izgradnje povjerenja između počinioca i djeteta. Whittle i saradnici (2014) definišu grooming kao ciljanu, faznu i psihološki usmjerenu strategiju kojom počinilac stvara emocionalnu vezu sa žrtvom, pripremajući je na seksualiziranu komunikaciju ili susret. Grooming se danas dominantno odvija na društvenim mrežama, online igrama i chat aplikacijama, gdje počinilac može nesmetano komunicirati, bez neposrednog nadzora odraslih. Sextortion predstavlja drugi ključni modalitet eksploatacije, a Wolak i saradnici (2018) definiraju ga kao oblik iznude u kojem počinilac zahtijeva dodatne seksualne sadržaje, novac ili druge koristi, prijeteći objavljivanjem stvarnog ili manipuliranog materijala koji prikazuje dijete u seksualiziranom kontekstu. Ovaj oblik kriminala postaje sve prisutniji zbog mogućnosti obrade slika i videa, uključujući deepfake tehnologiju, koju UNODC (2015) identifikuju kao rastući izazov za identifikaciju žrtava i dokazni postupak. Razumijevanje cyber eksploatacije djece zahtijeva poznavanje tehnoloških faktora koji omogućavaju da počinioci djeluju uz minimalan rizik. Izvještaji Europola i Interpola pokazuju da enkriptirane aplikacije, anonimne mreže poput Tora, kriptovalute i peer-to-peer sistemi omogućavaju visok stepen digitalne sigurnosti počinioca, dok istovremeno otežavaju istrage sigurnosnih agencija. UNODC upozorava i na porast sintetičkih vizualnih materijala generiranih umjetnom inteligencijom, koji se koriste u svrhe manipulacije, ucjene ili distribucije, čime se dodatno zamagljuju granice između stvarnog i kreiranog sadržaja. Stoga se cyber eksploatacija djece može jasno definisati tek kada se posmatra kroz tri međusobno povezana aspekta - krivična ponašanja koja se manifestuju u digitalnom prostoru, tehnološka sredstva koja omogućavaju anonimnost i širenje materijala, te psihološko-manipulativne strategije kojima se počinioci služe u komunikaciji sa žrtvama. Tek kombinacija ovih elemenata omogućava adekvatno prepoznavanje rizika, pravilnu kategorizaciju pojavnih oblika i izgradnju institucionalnih mehanizama za prevenciju i suzbijanje ovog oblika kriminaliteta.

3. Metode počinilaca online seksualne eksploatacije djece

Metode koje počinioci koriste u online seksualnoj eksploataciji djece kontinuirano se razvijaju paralelno s razvojem komunikacijskih tehnologija, digitalnih platformi i novih mogućnosti za prikrivanje identiteta. Za razliku od tradicionalnih oblika zlostavljanja, koji zahtijevaju fizičku prisutnost i direktan kontakt, online okruženje omogućava počiniocima da djeluju transnacionalno, anonimno i uz minimalne rizike otkrivanja. Europol u svojim IOCTA izvještajima (2022-2025) naglašava da je najveća prijetnja upravo dinamičnost metoda, koje se brzo prilagođavaju promjenama sigurnosnih protokola i nadzornih mehanizama.

3.1. Grooming kao centralni obrazac ponašanja

Grooming predstavlja jedan od najkompleksnijih i najopasnijih oblika online manipulacije djece, a njegovo razumijevanje zahtijeva analizu dinamičnih i međusobno povezanih faza kroz koje počinitelji nastoje ostvariti psihološku kontrolu nad djetetom. Tipologija koju je razvila O'Connell (2003) jedna je od najutjecajnijih i najdetaljnijih u ranoj fazi istraživanja ovog fenomena, te predstavlja temelj za savremene modele koji objašnjavaju kako se komunikacijski obrasci, manipulativne strategije i tehnološki faktori uklapaju u proces eksploatacije. Ipak, kasniji radovi pokazuju da se grooming ne odvija uvijek linearno te da počinitelji znatno ubrzavaju pojedine faze. Zbog toga je danas nužno posmatrati grooming kao fluidan, prilagodljiv i višedimenzionalan proces koji se oblikuje u skladu s motivacijom počinitelja, karakteristikama djeteta i specifičnostima digitalnog okruženja. O'Connell (2003) je dala naredne faze groominga koje je potrebno razmotriti zarad efikasnijeg shvatanja problema u vezi sa istraživanjem ove vrste krivičnog djela, a samim time i procesuiranjem.

Faza formiranja prijateljstva

Prema O'Connell (2003), proces najčešće počinje fazom uspostavljanja prijateljstva, u kojoj počinitelj ulazi u prvi kontakt s djetetom, bilo predstavljajući se kao vršnjak, bilo otvoreno kao odrasla osoba. Cilj je procijeniti djetetovu otvorenost za komunikaciju i uspostaviti osnovni osjećaj poznanstva. U ovoj fazi počinitelj postavlja uvodna pitanja o dobi, interesima, školskim obavezama ili hobijima, te često traži fotografije djeteta kako bi potvrdio njegov identitet ili provjerio odgovara li fizički njegovim preferencijama. Dumitriu, Dudu i Nanău (2024) napominju da se već u ovoj fazi može prepoznati selekcija žrtve, jer počinitelji biraju djecu koja pokazuju znake ranjivosti ili potrebe za potvrdom.

Faza formiranja veze

Ova faza predstavlja produbljivanje prvog kontakta i stvaranje emocionalne bliskosti. Počinitelj se predstavlja kao podrška, povjerljiv sagovornik ili „najbolji prijatelj", a razgovori se šire na teme koje uključuju porodične odnose, školske

probleme, uspjehe, nesigurnosti i svakodnevne izazove (O'Connell, 2003). Cilj ove faze je stvaranje privida emocionalne sigurnosti. Prema Whittle i drugim (2013), počinitelji tokom ove faze aktivno prate emocionalna stanja djeteta kako bi prepoznali trenutke ranjivosti i iskoristili ih za jačanje veze. Cano, Fernandez i Alani (2014) ističu da ova faza odgovara prvoj etapi Olsonove teorije luring komunikacije, poznatoj kao *Deceptive Trust Development*, u kojoj počinitelj namjerno stvara atmosferu povjerenja i zajedničke identifikacije.

Faza procjene rizika

Nakon uspostavljanja osnovnog odnosa, počinitelji prelaze na procjenu rizika otkrivanja. O'Connell (2003) pokazuje da počinitelji postavljaju pitanja poput: „Ko sve koristi računar?", „Jesu li roditelji trenutno kod kuće?", „Da li imaš telefon koji koristiš samo ti?", s ciljem da utvrde stepen nadzora i sigurnost daljnje komunikacije. Ova faza je ključna jer određuje intenzitet i smjer narednih postupaka. Chiang i Grant (2017) napominju da suvremeni groomeri često ne čekaju duže razdoblje da bi procijenili rizik, već tu fazu obavljaju u ranim minutama razgovora, što omogućava brzu procjenu mogućnosti manipulacije i izbjegavanje nadzora.

Faza eksluzivnosti

U ovoj fazi počinitelj uvodi narative o posebnom odnosu, međusobnoj tajnosti i emocionalnoj povezanosti. Tipični izrazi uključuju tvrdnje da dijete može vjerovati samo njemu, da ga odrasli ne razumiju ili da su njih dvoje „posebni" i „povezani na način koji drugi ne mogu razumjeti". Cilj je izolirati dijete od drugih izvora podrške i stvoriti odnos zavisnosti. Prema Dumitriu i saradniciima (2024), ova faza odgovara mehanizmima izolacije i psihološke kontrole, koji se pojavljuju i kod offline zlostavljanja. Ova faza također priprema dijete za normalizaciju seksualizirane komunikacije tako što pojačava osjećaj lojalnosti i emocionalne obaveze prema počinitelju.

Seksualna faza

Nakon što je postignut određeni stepen povjerenja i izolacije, počinitelj prelazi na postepeno ili naglo seksualiziranje komunikacije. Pitanja koja uvode seksualne teme mogu biti vrlo suptilna („jesi li imao/la simpatiju?"), ali i direktna („da li se diraš?"). Također, počinitelj može tražiti eksplicitne slike, predlagati upotrebu kamere ili detaljno opisivati seksualna ponašanja. Chiang i Grant (2017) ukazuju da savremeni groomeri često uvode seksualni sadržaj znatno ranije nego što O'Connell-ov model sugerira, ponekad već u prvim minutama komunikacije, što predstavlja veliki izazov za tradicionalne modele detekcije. Kloess, Hamilton-Giachritsis i Beech (2017) dodatno razlikuju groomere koji koriste *indirektni pristup*, postepeno povećanje seksualizacije od onih koji koriste *direktni pristup*, bez prethodne emocionalne pripreme.

Faza izvođenja seksualnih fantazija

O'Connell (2003) dodaje završnu fazu u kojoj počinitelj pokušava navesti dijete na seksualno eksplicitne radnje, bilo online ili offline. To uključuje vođenje djeteta kroz simulirane seksualne scenarije, izvođenje eksplicitnih radnji pred kamerom ili predlaganje fizičkog susreta. Chiang i Grant (2017) potvrđuju da se u suvremenim slučajevima ova faza može pojaviti veoma rano, zbog ubrzane dinamike komunikacije i činjenice da počinitelji često djeluju iz pedofilskih zajednica na darknetu gdje se razmjenjuje znanje i "savjeti" o optimalnim strategijama eksploatacije.

Dinamičnost, preklapanja i ubrzavanje faza

Iako je O'Connell-in model bio pionirski i ostaje najdetaljniji opis faznog pristupa, moderni empirički radovi (Chiang & Grant, 2017; Kloess et al., 2017) pokazuju da se grooming u savremenom online okruženju odvija mnogo brže i da faze nisu ni približno linearne.
Studije otkrivaju da:

- sve faze mogu nastupiti unutar prvog sata komunikacije
- seksualizacija može biti prisutna već u prvim porukama
- faze se često preklapaju
- groomeri mogu preskakati čitave faze ako procijene da je dijete ranjivo
- digitalne platforme omogućavaju brzu eskalaciju, naročito uz enkriptirane aplikacije

Dumitriu i saradnici (2024) potvrđuju da grooming treba posmatrati kao adaptivni proces koji zavisi od motivacije počinitelja, ranjivosti žrtve i konteksta komunikacije, a ne kao fiksni slijed koraka.

3.2. Online seksualna iznuda

Online seksualna iznuda predstavlja jedan od najagresivnijih i najštetnijih oblika tehnologijom posredovane seksualne eksploatacije djece, a u posljednjoj deceniji dobila je status prioritetne prijetnje u izvještajima Europola i međunarodnih organizacija. Iako se u javnom diskursu dugo poistovjećivala s groomingom ili širim kategorijama online seksualnog nasilja, današnja istraživanja jasno ukazuju da se radi o zasebnom i izrazito destruktivnom obrascu ponašanja. Najjednostavnije rečeno, sextortion uključuje situaciju u kojoj počinitelj prijeti da će objaviti, distribuirati ili poslati seksualno eksplicitne slike ili videozapise djeteta ako ono ne ispuni određene zahtjeve, bilo seksualne, emocionalne ili materijalne prirode. Ta osnovna struktura prisile čini temelj fenomena koji, prema nalazima Finkelhora i saradnika (2020), pogađa oko 3,5% mladih prije

punoljetstva, pri čemu je stvarna prevalencija vjerovatno znatno veća zbog izuzetno niskog nivoa prijavljivanja.

Za razliku od groominga, koji se dominantno temelji na stvaranju emocionalne bliskosti i postepenom urušavanju granica, online seksualna iznuda počiva na naglom i radikalnom narušavanju ravnoteže moći u trenutku kada počinitelj dođe u posjed seksualnog materijala djeteta. Açar (2016) ovaj oblik eksploatacije definira kroz tri ključna elementa, a to su digitalni prostor kao okruženje djelovanja, posjedovanje kompromitirajućeg materijala i upotrebu tog materijala kao sredstva ucjene. Tek kada su ta tri elementa ispunjena, može se govoriti o sextortion-u kao specifičnoj formi online seksualnog nasilja. Ova formulacija posebno je korisna jer razgraničava seksualnu iznudu od groominga, sextinga, cyberbullyinga i drugih digitalnih rizika. Istraživanja ukazuju da inicijalni materijal najčešće nastaje kroz dobrovoljno slanje slika u kontekstu romantičnog odnosa, prijateljstva ili očekivane intimnosti. Wolak i saradnici (2018) pokazuju da je 75% maloljetnih žrtava svjesno poslalo prvi materijal, ali pod pritiskom ili emocionalnom manipulacijom, dok više od 60% počinitelja dolazi iz kruga poznanika, vršnjaka ili bivših partnera. Ovi nalazi ozbiljno narušavaju stereotip o „strancu-predatoru“ i ukazuju da se veliki broj incidenata odvija unutar postojećih odnosa moći među adolescentima. Istovremeno, suvremeni oblici iznude sve češće uključuju i nepoznate počinioce, uključujući kriminalne grupe koje putem lažnih profila iniciraju razmjenu intimnih slika, brzo eskaliraju komunikaciju i potom zahtijevaju novac, dodatne eksplicitne materijale ili druge oblike poslušnosti (Ray & Henry, 2024).

Modaliteti pribavljanja materijala uveliko variraju, ali se u literaturi mogu prepoznati tri dominantna obrasca (Açar, 2016). Prvi se odnosi na iznudu unutar postojećih odnosa, najčešće među adolescentima, gdje intimne fotografije postaju alat kontrole nakon sukoba ili prekida. Drugi se povezuje s predatorskim ponašanjem u kojem se grooming tehnike koriste samo kao početna faza za pribavljanje vizualnog materijala, nakon čega slijedi brza eskalacija prijetnji. Treći obrazac uključuje tehnički sofisticirane metode, poput hakovanja računa ili kamera, iako se u praksi javljaju znatno rjeđe nego što se pretpostavlja, jer zahtijevaju znanja koja većina počinitelja nema (Açar, 2016). Ipak, IoT uređaji i funkcija „live streaminga“ otvaraju nove rizike, posebno u kontekstu praksi snimanja bez pristanka. Dinamika iznude posebno je opasna zbog činjenice da prijetnje ne služe samo kao sredstvo kontrole, već i kao faktor psihološke destabilizacije žrtve. Tipično, počinitelj prijeti javnim objavljivanjem materijala, slanjem roditeljima, prijateljima ili nastavnicima, kreiranjem lažnih profila ili slanjem materijala školskim zajednicama. Studije pokazuju da mnogi počinioci prijetnje ponavljaju kroz mjesece i da, u slučajevima maloljetnih žrtava, nerijetko potiču djecu na samopovređivanje ili samoubistvo kako bi dodatno učvrstili kontrolu (Wolak et al., 2018). Upravo takve eskalacije ukazuju da sextortion nije samo digitalni fenomen, već oblik psihološkog i emocionalnog nasilja sa

ozbiljnim posljedicama po mentalno zdravlje žrtve. Psihološke posljedice seksualne iznude izrazito su teške, a literatura potvrđuje trajne efekte poput depresije, intenzivne anksioznosti, osjećaja krivnje i srama, povlačenja iz socijalnih kontakata i ozbiljnih samodestruktivnih misli (Ray & Henry, 2024). Zabilježeni su slučajevi u kojima su djeca promijenila školu, prekinula obrazovanje ili pokušala samoubistvo kako bi pobjegla od prijetnji koje nisu znala kako zaustaviti. Ključno je što većina žrtava ne traži pomoć jer polovina maloljetnika u studiji Wolaka i saradnika (2018) nikada nije prijavila incident, iz straha od osude, nevjerice, reakcije roditelja ili gubitka reputacije. Time se stvara začarani krug u kojem se iznuda nastavlja upravo zato što je nevidljiva.

3.3. Proizvodnja i distribucija CSAM: tehnološki infrastruktura, kriminalne dinamie i izazovi za istrage

Savremena proizvodnja i distribucija materijala seksualnog zlostavljanja djece (CSAM) odvija se u digitalnom prostoru koji karakterišu brzina, anonimnost i globalni domet. Tehnološki napredak posljednjih dvadeset godina fundamentalno je promijenio kriminalne procese, čineći nastanak i širenje CSAM jednostavnijim i operativno sigurnijim za počinitelje. Lee i saradnici (2020) naglašavaju da današnje online okruženje spaja tri ključne dimenzije relevantne za razumijevanje fenomena su zakonski okvir, distribucijske kanale i tehničke mehanizme detekcije. Ove dimenzije oblikuju cjelokupnu infrastrukturu u kojoj počinitelji djeluju, a ujedno postavljaju jasna ograničenja pred istražne organe. Kriminalni proces počinje u fazi proizvodnje, koja se danas odvija u širokom rasponu kontekstaod direktnog kontaktnog zlostavljanja u intrafamilijarnim okvirima, do potpunog online iskorištavanja putem web kamera i digitalnih uređaja. Sistematski pregled Calea i suradnika (2021) pokazuje da se značajan dio CSAM proizvodi u okruženjima gdje počinitelj ima neposredan pristup djetetu. U više od polovine slučajeva počinitelj je član porodice žrtve ili blizak poznanik, što potvrđuju i nalazii Gewirtz-Meydan i saradnika (2018) koji ukazuju da su porodica, bliski partneri roditelja i osobe iz neposrednog okruženja najčešći proizvođači sadržaja. Paralelno, sve je više slučajeva u kojima se CSAM producira isključivo online, bez fizičkog kontakta, putem direktnog nagovaranja djece da pred kamerom izvode seksualizirane radnje (McManus, Long, Alison, & Almond, 2015). Ovaj oblik predstavlja relativno novu kategoriju digitalnih zločina, potaknutu ekspanzijom aplikacija sa video-komunikacijom i niskom procjenom rizika kod počinitelja.

Distribucija CSAM materijala zauzima centralno mjesto u savremenom ekosistemu seksualne eksploatacije djece, a odvija se kroz tri dominantna kanala: otvoreni web, P2P mreže i dark web. Na otvorenom webu CSAM se pojavljuje u dva konteksta: u direktnim kontaktima počinitelja i djece putem društvenih mreža, i u formi nestrukturiranih, privremeno dostupnih materijala koji izmiču

moderaciji. Cale i saradnici (2021) ističu da je upravo otvoreni web prostor u kojem se odvija najveći dio početnih kontakata između djece i počinitelja, posebno na platformama kao što su Facebook, Instagram, Snapchat i različite aplikacije za razmjenu videa. U tom segmentu dominiraju fenomeni grooming, seksualiziranog uvjeravanja i prikupljanja inicijalnih fotografija koje kasnije prelaze u kriminalne mreže. Ova interakcija pokazuje stalnu povezanost između proizvodnje i distribucije kroz sadržaj nastao tokom grooming koji je često je polazna tačka za širu razmjenu. P2P mreže predstavljaju drugi sloj distribucije i omogućavaju globalno dijeljenje velikih datoteka bez centralnog posrednika. Bissias i saradnici (2016) procjenjuju da je u određenom trenutku više od 800.000 korisnika na globalnom nivou učestvovalo u dijeljenju CSAM na P2P mrežama, dok Bouhours i Broadhurst (2011) ukazuju da se značajan dio razmjene dešava lokalno i u jezičkim i kulturnim grupama povezanih korisnika. Ove mreže posebno karakterišu ogromni volumeni podataka, česta razmjena višegodišnjeg sadržaja, te fragmentiranost datoteka koja otežava identifikaciju originalnog materijala. Policijske agencije u brojnim zemljama izvještavaju o tome da P2P mreže generiraju obim rada koji nadmašuje njihove tehničke i kadrovske kapacitete, što potvrđuje i Johansson (2019) u svojoj studiji o švedskom policijskom kontekstu.

Najorganiziraniji i najopasniji sloj distribucije razvija se na dark webu. Ngo, Gajula, Thorpe i McKeever (2024) analizirali su više od 353.000 objava na osam dark web foruma i identificirali preko 10.000 aktivnih CSAM autora koji koriste ove platforme za razmjenu materijala, komunikaciju, savjetovanje o metodama izbjegavanja detekcije i stvaranje zatvorenih zajednica. Autori bilježe i specifične kriminalne obrasce kao što su razmjena ekskluzivnih materijala, korištenje kodiranog žargona, primjenu sofisticiranih operativnih sigurnosnih mjera i jasno strukturirane hijerarhije u kojima se status stiče obimom doprinosa. Ove strukture predstavljaju digitalni ekvivalent organiziranih kriminalnih mreža i značajno otežavaju infiltraciju i prikupljanje dokaza. Istraživanja takođe pokazuju da su platforme kao što su Tor i I2P glavni pristupni kanali, uz dodatno korištenje enkripcije, kriptovaluta i decentraliziranih hosting servisa koji dodatno otežavaju rad istražnih agencija.

Sve ove dinamike stvaraju ozbiljne operativne izazove za istrage. Leclerc i saradnici (2022) navode da policijski istražitelji širom svijeta ističu nedostatak specijalizirane obuke, tehničkih resursa i analitičke podrške kao najveće prepreke efikasnom procesuiranju slučajeva. Problemi se kreću od tehničke zastarjelosti opreme i nedostatka digitalnih forenzičara, do nedovoljne saradnje s globalnim društvenim mrežama i pravnih ograničenja koja usporavaju pristup podacima. Johansson (2019) dodatno ukazuje da mnoge policijske organizacije tretiraju CSAM kao kriminal nižeg prioriteta, što dovodi do preopterećenosti istražitelja, dugih zastoja u procedurama i slabog institucionalnog odgovora u odnosu na obim štete.

3.4. Tehnike identifikacije žrtava i počinitelja

Identifikacija žrtava i počinitelja u slučajevima online seksualnog zlostavljanja djece predstavlja ključnu kariku između "digitalnog traga" i klasičnog krivičnog postupka. Pritom se isprepliću tri ravni- forenzička analiza vizuelnog sadržaja, automatizirane tehnike detekcije i klasifikacije CSAM-a, te operativno-istražne metode usmjerene na traganje za konkretnim osobama iza ekrana. Savremena literatura pokazuje da nijedna od ovih komponenti nije dovoljna sama za sebe, već da se najveći učinak postiže kombiniranjem više pristupa, uz jasno definisanu institucionalnu podjelu uloga i odgovornosti.

3.4.1. Forenzička analiza i klasifikacija slikovnog materijala

Osnovni preduvjet za identifikaciju žrtava i počinitelja jeste uopće prepoznati da određeni materijal predstavlja seksualnu zloupotrebu djece te ga konzistentno razvrstati u zakonske kategorije. Kloess i saradnici pokazuju da čak i iskusni policijski analitičari imaju značajne poteškoće pri procjeni dvije ključne dimenzije, da li je prikazana osoba dijete i da li je sadržaj "nedozvoljen" odnosno "indecentan" u smislu zakona (Kloess, Woodhams, Whittle, Grant, & Hamilton-Giachritsis, 2017). Posebno problematične su tzv. "granične slike"odnosno adolescenti u ranijim stadijima puberteta, djelimična golotinja, ili situacije u kojima kontekst može imati i "nevinu" interpretaciju. Inter-rater analize pokazuju da se kod takvih snimaka javlja veći stepen neslaganja između kodera, što direktno utiče na dosljednost krivičnog gonjenja i procjenu težine djela. Radi smanjenja subjektivnosti uvedene su skale tipa COPINE i kasnije jednostavniji sistemi kategorizacije (A, B, C), koje razdvajaju penetrativne radnje, nepenetrativne seksualne aktivnosti i "erotsko poziranje" (Taylor, Holland, & Quayle, 2001). Međutim, upravo kategorija C ("erotsko poziranje") pokazuje koliko je normativna granica fluidna. Analitičari priznaju da se u praksi često "drže sigurnog terena" i fokusiraju na očigledno teške materijale, dok dio nižeg nivoa ostaje u zoni neodlučnosti. To ima neposrednu posljedicu na identifikaciju žrtava, odnosno djeca čije se slike formalno ne prepoznaju kao CSAM ostaju izvan spektra proaktivnih istraga i međunarodnih baza.

Poseban izazov predstavlja procjena starosti. Istraživanja pokazuju da čak ni medicinski stručnjaci nisu značajno bolji od laika u razlikovanju kasnih adolescenata od punoljetnih osoba na osnovu fotografija, upravo zbog velike varijabilnosti u tempu pubertetskog razvoja (Cattaneo, i dr., 2009). U digitalnom kontekstu dodatno otežavaju etničke razlike u tjelesnoj građi, promjene u indeksu tjelesne mase i globalna priroda CSAM-a. U operativnom smislu to znači da procjena starosti mora biti kombinirana sa drugim indikatorima – kontekstom scene, metapodacima, nazivom fajla, jezikom i kulturnim obilježjima okruženja – umjesto da se oslanja na vizuelni utisak.

3.4.2. Hash baze, P2P monitoring i web-crawleri kao temelji identifikacije

Na tehničkoj razini, većina savremenih sistema borbe protiv CSAM-a počiva na hash bazama poznatog materijala. PhotoDNA i slične tehnologije generišu "otiske" slika, omogućavajući prepoznavanje već ranije identifikovanih snimaka čak i kada su djelimično izmijenjeni (Edwards, Christensen, Rayment-McHugh, & Jones, 2021). Time se postižu dva cilja, a to su broj digitalnih artefakata koje analitičar mora ručno pregledati drastično se smanjuje, a istovremeno se omogućava da se ista žrtva prati kroz različite kolekcije počinitelja i preko više platformi, što je presudno za njen fizički pronalazak. Nadzor P2P mreža i specijalizirani alati poput iCOP-a idu korak dalje, kombinirajući hash pretragu sa analizom naziva fajlova i saobraćaja kroz mrežu (Peersman, Schulze, Rashid, Brennan, & Fischer, 2016). Studije pokazuju da mali broj "čvorišta" generiše nesrazmjerno veliki dio prometa CSAM-a, te da bi uklanjanje samo vrha distribucijske piramide moglo smanjiti dostupnost materijala na pojedinim mrežama za 30–40% (Wolak, Liberatore, & Levine, 2014). Sa stanovišta identifikacije počinitelja, praćenje IP-adresa, obrazaca dijeljenja i listi "sjemenskih" fajlova omogućava profiliranje najaktivnijih distributera, koji su ujedno i najvjerovatniji producenti ili administratori zatvorenih zajednica, dakle akteri sa najvećim "operativnim značajem".

Web-crawleri primijenjeni na "clear web" i, u ograničenoj mjeri, na darknet, automatski prate linkove s već poznatih CSAM domena i mapiraju mrežu povezanih stranica (Westlake, Bouchard, & Frank, 2012). Primjer projekata poput Project Arachnid[2] pokazuje da je moguće procesuirati stotine miliona stranica i identificirati desetine hiljada unikatnih CSAM slika u kratkom vremenu, što policiji otvara mogućnost da gađa sajtove sa najvećom "centralnošću" i tako razbija infrastrukturu distribucije. Istovremeno, svaki put kad se poznata slika pojavi na novoj lokaciji, generiše se trag koji može voditi ka novim počiniteljima i eventualno novim informacijama o identitetu žrtve.

3.4.3. Metapodaci, nazivi fajlova i analiza darkneta

Noviji radovi sve više ističu vrijednost metapodataka i tekstualnih tragova kao izvora za identifikaciju kako CSAM sadržaja, tako i aktera koji njime upravljaju. Studija Pereire i saradnika (2024) pokazuje da su klasifikacijski modeli zasnovani isključivo na nazivima fajlova i putanjama (file paths) u stanju da postignu visok stepen tačnosti, upravo zato što počinitelji razvijaju specifičan, prepoznatljiv vokabular i kodirani jezik u imenovanju sadržaja. P2P pretrage se ionako u velikoj mjeri zasnivaju na tekstualnom pretraživanju naziva fajlova, pa je prelazak na automatiziranu analizu tih obrazaca logičan korak.

[2] Projekt Arachnid je nastau u Australiji i predstavlja specifičan skup alata usmjeren na žrtve online seksualne eksploatacije i namijenjen je borbi protiv širenja materijala o seksualnom zlostavljanju djece (CSAM) na internetu. Pokrenut je 2017. godine i objedinjuje automatizirane metode otkrivanja CSAM-a.

Ngo i saradnici razvijaju sistem za detekciju CSAM-a na dark web forumima baziran na mašinskom učenju, koji na korpusu od preko 353.000 objava uspijeva da identifikuje oko 63.000 CSAM-relevantnih objava i preko 10.500 "kreatora" CSAM sadržaja (Ngo et al., 2024). Analiza metapodataka tih postova daje nekoliko važnih uvida: dominantne teme i preferencije pojedinih autora, tipične starosne skupine i nacionalnosti žrtava koje se spominju, te platforme koje se najčešće koriste za pribavljanje i razmjenu materijala (Omegle, YouTube, Skype, Instagram, Telegram). Za potrebe identifikacije počinitelja, ovakvi obrasci služe kao osnova za ciljanje najaktivnijih i najopasnijih aktera, kao i za prepoznavanje novih žarišnih tačaka na "surface" platformama gdje se žrtve regrutiraju ili gdje se CSAM inicijalno proizvodi (npr. live streaming preko VoIP aplikacija, web-kamera i društvenih mreža).

Metapodaci u širem smislu kao EXIF podaci fotografije, vremenske oznake, geolokacija, verzija softvera, jezik sistema dopunjuju ovu sliku. Iako su počinitelji sve svjesniji potrebe da "čiste" metapodatke, analiza milijuna fajlova i mrežnih interakcija ipak omogućava statističko profiliranje tipičnih konfiguracija, vremenskih obrazaca i tehnoloških sredstava koja koriste određene grupe. To ne daje automatski "ime i prezime", ali sužava operativni prostor i usmjerava klasične istražne radnje.

3.4.4. Automatizirano otkrivanje, AI i forenzički workflow

Pregled literature o automatiziranom otkrivanju CSAM-a ukazuje na jasnu konvergenciju, najefikasniji sistemi kombinuju više modaliteta – hash vrijednosti, vizuelne karakteristike slike, tekstualne signale u nazivima fajlova i metapodacima umjesto da se oslanjaju na jedan indikator (Edwards et al., 2021). Duboke neuronske mreže postižu najbolje rezultate pri detekciji do tada neviđenog CSAM-a, posebno kada se višestruki deskriptori slike i videa spajaju u jedinstveni klasifikator (Lee, Ermakova, Ververis, & Fabian, 2020). Vitorino i drugi (2018) pokazuju da CNN modeli istrenirani na velikim policijskim datasetima mogu vrlo efikasno razlikovati CSAM od adult pornografije, dok radovi o kombiniranju detekcije pornografije i procjene dobi dodatno sužavaju fokus na potencijalne žrtve (Vitorino et al., 2018; Lee et al., 2020).

Međutim, Pereira i saradnici (2024) naglašavaju da se modeli moraju testirati u realističnim scenarijima, uključujući potpuno benigne "out-of-sample" setove i situacije u kojima počinitelji namjerno mijenjaju tekstualne obrasce (adversarial examples tipa "Lo7ita", "b4", slično). Visoka stopa lažno pozitivnih nalaza može praktično blokirati implementaciju sistema u platformama sa milijardama korisnika, a sa stanovišta policije stvara dodatni operativni teret. Istraživanje Sanchez i saradnika (2019), zasnovano na anketi istražitelja, pokazuje da su praktičari veoma osjetljivi na pitanje lažno pozitivnih nalaza; većina ih smatra veću stopu FP ozbiljnijim problemom od propuštenih slučajeva, upravo zato što FP direktno opterećuju ograničene resurse. Istovremeno, Sancher i saradnic

(2019) ukazuju da mnogi praktičari nisu dovoljno upoznati sa osnovama data science i AI, iako već rade sa alatima koji te tehnike koriste. To stvara raskorak između mogućnosti tehnologije i načina na koji se zaista koristi u praksi.

S tehničke strane, razvijeni su brojni alati za trijažu i filtriranje od jednostavnih sistema za detekciju golotinje na nivou piksela, preko specijaliziranih "field triage" alata, do kompleksnih sistema koji automatski rangiraju uređaje i medije prema vjerovatnoći da sadrže relevantne dokaze (Marturana & Tacconi, 2013). Sa stanovišta identifikacije žrtava i počinitelja, njihova vrijednost leži u tome što kratkoročno oslobađaju istražitelje od pregledavanja ogromnih količina benignog materijala, čime se brže dolazi do "čistog" CSAM-a u kojem je moguće prepoznati konkretna lica, prostore i obrasce ponašanja.

3.4.5. Identifikacija žrtava i počinitelja

Iako većina navedenih tehnologija primarno služi detekciji i klasifikaciji sadržaja, one su istovremeno temelj za identifikaciju žrtava i počinitelja u užem smislu. U praksi se to odvija kroz nekoliko komplementarnih koraka. Prvo, hash baze i automatizirana vizuelna detekcija omogućavaju izdvajanje materijala koji sadrži do tada neidentifikovane žrtve, što postaje prioritet za specijalizirane timove za "victim identification" (Edwards et al., 2021; Johansson, 2019). Drugo, procjena dobi, spoljašnjih obilježja, jezika u pozadini i kulturnih artefakata (odjeća, arhitektura, tehnika) pomaže u geografskoj i demografskoj atribuciji žrtve, iako Kloess i drugi (2017) jasno pokazuju da procjena starosti ostaje izvor ozbiljne nesigurnosti, posebno kod adolescenata. Treće, u sve većoj mjeri koriste se tehnike poput prepoznavanja lica, poređenja prostorija, namještaja i "mikro-okruženja" između različitih slučajeva i prijava, što omogućava da se ista žrtva ili isti počinitelj povežu kroz više istraga i jurisdikcija (Edwards et al., 2021). U širem, kriminološkom smislu, studije o "crime commission processes" ukazuju da producenti CSAM-a često spajaju online i offline dimenziju pri čemu kombiniraju kontaktno zlostavljanje sa snimanjem i digitalnom distribucijom. Tu se ključne odluke donose na temelju procjene rizika detekcije, dostupnosti djece i tehničkih mogućnosti (Cale et al., 2021). Upravo razumijevanje tih procesa pomaže policiji da prioritizira profil počinitelja koji je vjerovatnije istovremeno i online distributer i offline zlostavljač.

Identifikacija počinitelja zavisi i od "klasičnih" digitalnih tragova: IP adresa, logova, naloga na društvenim mrežama, komunikacije u P2P i darknet okruženju, kao i od načina na koji se te informacije integriraju sa rezultatima OSINT, HUMINT, SIGINT i tradicionalnih istražnih radnji. U istraživanju OKG i njihovih članova koriste se otvoreni izvori kao što su društvene mreže na kojima akteri mogu ostaviti značajan broj podataka i informacija, kao što su fotografije, video snimke, objave i tako dalje (Muhić, 2024). Johansson pokazuje da je, na primjer, u Švedskoj jedan od ključnih problema nedostatak obaveze ISP-ova da čuvaju IP logove, što direktno otežava identifikaciju počinitelja čak i kada je

CSAM sadržaj otkriven (Johansson, 2019). Slično tome, Leclerc i saradnici (2022) ističu da policijski istražitelji kao ključne vještine navode kombinaciju "social engineering" komunikacijskih sposobnosti, dobrog poznavanja IT tehnologija i razumijevanja profila seksualnih prestupnika. Drugim riječima, ni najnapredniji algoritmi ne mogu zamijeniti vještinu istražitelja da iskoristi digitalne tragove za razvijanje operativnih hipoteza i njihovo testiranje kroz ispitivanja, nadzor i druge mjere.

3.4.6. Ljudski faktor: kapaciteti, opterećenje i zaštita istražitelja

Većina navedenih tehnika podrazumijeva intenzivan rad specijaliziranih policijskih timova i digitalnih forenzičara. Više studija potvrđuje da je riječ o profesionalnoj populaciji izložene visokom riziku sekundarne traumatizacije, hroničnog stresa i "burnouta", upravo zbog kontinuiranog kontakta sa ekstremno uznemirujućim sadržajem (Burns, Morley, Bradshaw, & Domene, 2008; Seigfried-Spellar, 2017; Sanchez, Grajeda, Baggili, & Hall, 2019). Istražitvači u Leclercovoj studiji navode kao ključne probleme enorman obim podataka, nedostatak osoblja i tehničkih resursa, te ograničeno razumijevanje fenomena CSAM-a u menadžmentu vlastitih institucija (Leclerc et al., 2022). Johansson dolazi do sličnih nalaza za Švedsku gdje različite policijske regije rade po različitim procedurama, digitalno forenzičko osoblje je "usko grlo", a CSAM se u praksi često tretira kao "niskoprioritetni" kriminalitet (Johansson, 2019). Sanchez i saradnici (2019) pokazuju da istražitelji prepoznaju veliku vrijednost filtriranja i trijažnih tehnologija. To se radi prvenstveno da bi smanjili vlastitu izloženost i ubrzali rad ali da istovremeno relativno malo koriste alate zasnovane na naprednim AI tehnikama, dijelom i zato što ih nedovoljno razumiju (Sanchez, Grajeda, Baggili, & Hall, 2019). Efektivno korištenje tehnika identifikacije žrtava i počinitelja stoga zahtijeva ne samo nabavku tehnoloških rješenja, nego i ulaganje u sistematsku obuku, superviziju, psihološku podršku i jasne protokole rada, kako bi se omogućilo da ljudi koji rade najteže zadatke ostanu funkcionalni i profesionalno održivi.

4. Institucionalni, operativni i pravni odgovori na online seksualnu eksploataciju djece

4.1. Nacionalni i međunarodni pravni okvir

Savremeni međunarodni pravni okvir koji regulira online seksualnu eksploataciju djece razvijao se u vremenu koje nije poznavalo današnji obim, dinamiku i tehnološke mogućnosti digitalne proizvodnje i distribucije materijala seksualnog zlostavljanja djece. Uprkos velikoj normativnoj gustoći i širokom prihvatanju najvažnijih međunarodnih instrumenata, uočljiva je strukturalna napetost između formalnih obaveza država i njihovih stvarnih kapaciteta da adekvatno odgovore na fenomen koji se transformira brže nego što zakonodavstvo može reagirati. Prema Global Status Report on Preventing Violence Against Children (WHO,

2020), većina država ima relativno razvijen normativni okvir zaštite djece, ali manje od polovine posjeduje funkcionalne mehanizme provedbe. U digitalnom okruženju, gdje se CSAM distribuira kroz anonimne mreže, peer-to-peer sisteme, šifrirane komunikacijske kanale i platforme zasnovane na generativnoj umjetnoj inteligenciji, ta disproporcija između normativnog i operativnog postaje još izraženija. Razumijevanje međunarodnog i evropskog pravnog okvira time postaje ključno za identifikaciju uzroka neuspjeha istraga, sporosti u identifikaciji žrtava i ograničenog dometa kaznenih mehanizama. Konvencija o pravima djeteta iz 1990. godine predstavlja temeljni međunarodni instrument zaštite djece, ali je nastala u historijskom kontekstu u kojem internet tek počinje ulaziti u širu društvenu upotrebu. Zbog toga CRC nije sadržavala specifične odredbe koje bi prepoznale digitalno okruženje kao primarni prostor viktimizacije, niti je predviđala fenomene kao što su virtualni CSAM, deepfake tehnologije, vizualne manipulacije ili anonimna globalna tržišta distribuirana putem darkneta. Njena najveća snaga leži u uspostavljanju principa najboljeg interesa djeteta, obaveze preventivnog djelovanja i unapređenja dječijeg razvoja, ali upravo ti principi ostaju nedovoljno operacionalizirani u digitalnom kontekstu. Dodatni Protokol o prodaji djece, dječjoj prostituciji i dječjoj pornografiji (OPSC) predstavlja pokušaj dopune tih praznina, ali analiza Maxwella (2022) jasno pokazuje da OPSC ostaje primarno fokusiran na kriminalizaciju, dok su preventivne mjere formulirane široko, sugestivno i bez jasnih minimalnih standarda koje bi države morale ispuniti. Takav pristup dovodi do situacije u kojoj države uglavnom ispunjavaju formalne obaveze kriminalizacije, dok sistemske preventivne politike ostaju rudimentarne ili se uopće ne razvijaju.

Budimpeštanska konvencija Vijeća Evrope iz 2001. godine predstavlja prvi sveobuhvatni međunarodni instrument koji adresira računalno posredovane oblike kriminaliteta, uključujući i proizvodnju, distribuciju i posjedovanje „child pornography“ u smislu člana 9. Ona je postavila arhitekturu međunarodne policijske i pravosudne saradnje, ali je ubrzo postalo jasno da njezina efikasnost trpi zbog nekoliko ključnih faktora. Transnacionalni karakter CSAM kriminaliteta otežava primjenu teritorijalnih pravila nadležnosti, pa istrage koje uključuju servere, počinioce i žrtve u različitim državama završavaju u dugotrajnim procedurama međusobnog pravnog pomaganja. Uz to, države različito definiraju šta se smatra nezakonitim sadržajem, osobito u pogledu virtualnih, realističnih i AI-generisanih prikaza djece, što otežava koordinirano djelovanje i razmjenu dokaza (Sorbán, 2024). Razlike u propisima o obaveznom čuvanju IP logova dodatno usložnjavaju situaciju, budući da se u nekim jurisdikcijama podaci čuvaju nekoliko mjeseci, dok se u drugim čuvaju godinama, što u praksi određuje granice uspješne digitalne istrage (Kasper & Laurits, 2016).

Lanzarote konvencija iz 2007. godine unijela je kvalitativni iskorak kriminalizacijom grooming ponašanja putem informacionih tehnologija i uspostavljanjem obaveze država da poduzmu sve odgovarajuće mjere radi zaštite

djece od seksualne eksploatacije na internetu. Ipak, kao i svi instrumenti Vijeća Evrope, Lanzarote konvencija pati od odsustva mehanizama sankcioniranja država koje ne implementiraju svoje obaveze. Njena fleksibilna normativna struktura dopušta različita tumačenja, posebno u vezi s virtualnim i AI-manipulisanim prikazima, što stvara dodatne pravne praznine u kontekstu generativne umjetne inteligencije i naprednih alata za vizualnu manipulaciju dječijih slika (Parti & Szabó, 2024). Uprkos tome što uvodi ključne konceptualne inovacije, Lansarote konvencija nije predvidjela mogućnost stvaranja potpuno fiktivnih, hiperealističnih prikaza djece, pa njena primjena u slučajevima AI-generisanog materijala ostaje nedovoljno razrađena.

Na regionalnom nivou, najvažniji instrument predstavlja Direktiva 2011/93/EU o borbi protiv seksualnog zlostavljanja djece, koja obavezuje države članice da kriminaliziraju sve oblike online seksualne eksploatacije, uključujući grooming, posjedovanje, distribuciju, stvaranje i podsticanje stvaranja CSAM-a. Direktiva predviđa i proaktivne istrage koje ne zavise od prijave žrtve, proširenu ekstrateritorijalnu nadležnost, mjere podrške žrtvama od najranije faze postupka te specijalizirane operativne mehanizme. Ipak, kao instrument minimalne harmonizacije, ona dopušta državama da njene odredbe transponuju na različite načine, što je u praksi proizvelo duboke razlike u definicijama, procedurama i sankcijama. Ta fragmentacija otežava koordinaciju istraga, razmjenu dokaza, saradnju sa Europolom i sprovođenje zajedničkih operacija, posebno u slučajevima koji uključuju peer-to-peer sisteme, razmjene putem enkriptiranih aplikacija ili AI-generisane sadržaje (Huemer, 2024). Dodatni problem leži u tome što Direktiva ne sadrži detaljne smjernice u vezi s izazovima koje donosi generativna umjetna inteligencija, ne dotiče se realističnih avatar-prikaza djece u metaverzumskim okruženjima i ne nudi rješenja za situacije u kojima E2EE komunikacija onemogućava pristup dokazima. Najnoviji pokušaj uspostavljanja snažnijeg evropskog pravnog okvira predstavlja Prijedlog regulacije *COM (2022) 209 final*, koji predviđa obavezu internetskih platformi da detektuju, uklanjaju i prijavljuju CSAM, kao i identifikaciju grooming komunikacija kroz automatizirane sisteme. Regulacija, međutim, otvara ozbiljna pitanja balansa između zaštite djece i zaštite privatnosti, budući da njezina implementacija u praksi zahtijeva nadzor nad korisničkim komunikacijama koji je u suprotnosti sa standardima enkriptirane privatne komunikacije i načelima GDPR-a (Rezende, 2024). Evropske organizacije za zaštitu privatnosti upozoravaju da bi široko nadgledanje moglo stvoriti presedan za masovno nadziranje građana, dok evropske policijske i tužilačke institucije tvrde da je bez takvih mehanizama nemoguće pratiti eksponencijalni rast digitalne eksploatacije djece.

Sve ove razine pravne regulacije ukazuju na duboko ukorijenjen problem: postojeći pravni instrumenti nastali su u vremenu analognog kriminaliteta i ne uspijevaju u potpunosti odgovoriti na digitalne fenomene koji uključuju globalnu distribuciju, brisanje tragova, E2EE komunikacije, upotrebu kriptovaluta i

generativnu umjetnu inteligenciju. Razlike u definicijama, kapacitetima i primjeni prava između država stavljaju djecu u neravnopravan položaj, dok operativne prepreke poput varijabilnog čuvanja IP logova, spore međunarodne pravne pomoći i ograničenog pristupa digitalnim dokazima, često rezultiraju neuspjelim istragama ili nemogućnošću identifikacije žrtava. Time postaje jasno da je, uprkos široko ratificiranim instrumentima i formalno visokim standardima zaštite, pravni okvir i dalje nedovoljno usklađen sa stvarnim zahtjevima digitalnog okruženja i da zahtijeva duboku, strukturnu reformu kako bi mogao odgovoriti na rastući fenomen online seksualne eksploatacije djece.

4.2. Organizacijski modeli i kapaciteti policije i tužilaštava

Iako međunarodni i evropski pravni okvir postavlja minimalne standarde kriminalizacije i međudržavne saradnje, stvarni domet zaštite djece u digitalnom prostoru zavisi prvenstveno od organizacijskih modela, kapaciteta, resursa i operativnih procedura nacionalnih policijskih i tužilačkih institucija. Online seksualna eksploatacija djece se ne može adekvatno procesuirati u sistemima čije institucionalne arhitekture pripadaju periodu prije masovne digitalizacije, niti u organizacijama koje i dalje tretiraju digitalni kriminalitet kao periferan oblik delinkvencije. Empirijski podaci, kao i komparativne studije (Sanchez et al., 2019; Johansson, 2019), pokazuju da se većina nacionalnih sistema suočava s hroničnim nedostatkom specijaliziranih jedinica, fragmentiranim procedurama, nedovoljno obučenim kadrom i visokim emocionalnim troškovima koji dugotrajni rad s CSAM materijalom ostavlja na istražitelje. Ove slabosti imaju direktne posljedice: veliki broj slučajeva ostaje neistražen, prepoznate žrtve ostaju neidentifikovane, a predmeti u tužilaštvima kasne mjesecima ili godinama.

U većini država, organizacijski odgovor zasniva se na specijaliziranim jedinicama za cyber kriminal, digitalnu forenziku i seksualne delikte, no stvarni obim njihovih ovlasti i kapaciteta značajno varira. Strukturalno, policijske agencije najčešće primjenjuju model u kojem se digitalne istrage odvijaju u tri komponente - analitičkoj, operativnoj i forenzičkoj. Analitičke jedinice prikupljaju i obrađuju prijave, analiziraju OSINT i SOCMINT tragove, mapiraju P2P mreže i prate trendove distribucije. Operativne jedinice sprovode undercover aktivnosti u online okruženju, iniciraju prikrivene komunikacije sa osumnjičenim osobama i sakupljaju materijalne tragove u realnom vremenu. Forenzičke jedinice preuzimaju zaplijenjene uređaje, analiziraju metapodatke, koriste hash-baze i specijalizirane algoritme za identifikaciju sadržaja, te izlučuju dokaze koji će biti korišteni u krivičnim postupcima. Međutim, u praksi su ove tri funkcije često dislocirane, nedovoljno koordinirane i zavisne od individualnog entuzijazma i ekspertize malog broja službenika, što predstavlja ozbiljno ograničenje u slučajevima u kojima brzina, tehnološko znanje i međusektorska komunikacija određuju ishod istrage.

Poseban izazov predstavlja preopterećenost policijskih i tužilačkih kapaciteta. Studija Sanchez i saradnika (2019) pokazuje da istražitelji u CSAM predmetima rade pod značajnim psihološkim pritiskom, izloženi su sekundarnoj viktimizaciji i čestim simptomima burnouta, što dovodi do visoke fluktuacije, smanjenog učinka i gubitka institucionalne memorije. U mnogim državama, broj prijava višestruko nadmašuje broj raspoloživog osoblja. NCMEC je samo u 2023. godini primio 35,9 miliona prijava (National Centre for Missing & Exploited Children, 2023), dok Europol i Interpol bilježe stalni porast materijala koji se distribuiraju u fragmentima preko enkriptiranih chat aplikacija, cloud servisa i dark web foruma. Policijske i tužilačke institucije ne mogu pratiti taj obim, što rezultira selektivnim prioritiziranjem, često na štetu slučajeva koji uključuju online grooming ili materijal bez neposrednog fizičkog zlostavljanja, ali sa dugoročnim psihološkim posljedicama po djecu. U takvom modelu, CSAM se u mnogim državama tretira kao krivično djelo „nižeg prioriteta“, što direktno utječe na brzinu i kvalitet istraga.

Tehnička infrastruktura predstavlja dodatnu dimenziju institucionalnih ograničenja. Analiza terabajta materijala sa zaplijenjenih uređaja zahtijeva napredne alate, ogromne kapacitete skladištenja i specijalizirane SQL ili AI-pokretane sisteme koji omogućavaju klasifikaciju sadržaja, prepoznavanje žrtava i povezivanje slučajeva iz različitih jurisdikcija. U mnogim državama ti sistemi nisu standardizirani; koristi se heterogena kombinacija zastarjelih softvera, komercijalnih alata i open-source rješenja koja nisu interoperabilna (Johansson, 2019). Nedostatak standardizacije otežava forenzičku analizu, usporava istrage i umanjuje kvalitet dokaza koji se prezentiraju tužilaštvima. Uz to, policijske agencije u državama sa ograničenim resursima često nemaju ni osnovne kapacitete za dešifriranje uređaja, analizu enkriptovanih komunikacija ili rad sa P2P monitoring alatima, što stvara vidljivi jaz između tehnoloških mogućnosti počinilaca i kapaciteta institucija da im se suprotstave.

Uloga međunarodnih institucija, kao što su NCMEC, Europol i Interpol, postaje ključna u prevazilaženju ovih jazova, ali istovremeno otkriva slabosti nacionalnih sistema. Europolov EC3, Interpolova ICSE baza i NCMEC-ova CyberTipline pružaju neophodne alate za identifikaciju žrtava i usklađivanje globalnih evidencija, ali njihova efikasnost zavisi od brzine i kvaliteta nacionalnih odgovora. Države koje nemaju razvijene kapacitete za proaktivno skeniranje, prepoznavanje hash podudarnosti ili analizu metapodataka ostaju izvan globalnih tokova podataka, što znači da žrtve iz tih jurisdikcija ostaju neidentifikovane, a počinioci neprocesuirani. U tom smislu, međunarodna infrastruktura može samo djelimično kompenzirati nacionalne slabosti; ona ne može nadomjestiti nedostatak specijaliziranih kadrova, jasnih procedura, adekvatnog finansiranja ili političke volje za prioritetno tretiranje online seksualne eksploatacije djece.

4.3. Operativne strategije i modeli saradnje u suprotstavljanju online seksualnoj eksploataciji djece

Operativni odgovor na online seksualnu eksploataciju djece razvija se u složenom prostoru u kojem se isprepliću tehnološke inovacije, transnacionalni kriminalni ekosistemi i institucionalne razlike između država. Dok pravni okvir definiše obaveze, a organizacijski kapaciteti određuju šta je praktično izvodivo, operativne strategije predstavljaju konačan, najdinamičniji sloj institucionalnog djelovanja, onaj u kojem se norme i kapaciteti moraju pretvoriti u konkretne istrage, identifikaciju žrtava i razbijanje mreža počinilaca. Online seksualna eksploatacija djece karakterizira se izrazitom fluidnošću: počinioci koriste raznolike platforme, brzo migriraju između servisa, kombiniraju legitimne i anonimne kanale komunikacije, a sve češće koriste i generativne AI alate. U takvom okruženju, tradicionalni reaktivni modeli policijskog rada pokazuju se nedovoljnim, pa se države sve više oslanjaju na proaktivne, inteligentne i međunarodno koordinirane strategije.

Operativne strategije zasnivaju se na tri ključna pristupa a to su proaktivno otkrivanje, tehničko-forenzička analitika i međunarodna saradnja. Proaktivne strategije uključuju sistematsko praćenje online prostora, korištenje undercover identiteta u komunikaciji sa osumnjičenim osobama, identifikaciju obrazaca grooming ponašanja i analizu otvorenih i polu-zatvorenih mrežnih prostora. OSINT i SOCMINT metode u tom kontekstu postaju nezamjenjive. Policijske jedinice prikupljaju informacije iz javnih profila, digitalnih tragova, društvenih mreža, otvorenih P2P hubova i kriptoforuma, te koriste algoritamske alate za prepoznavanje rizičnih interakcija. Edwards i saradnici (2021) naglašavaju da P2P monitoring nije samo tehnički proces otkrivanja distribucije CSAM-a, nego i taktička strategija infiltracije zatvorenih mreža u kojima počinioci dijele materijale i informacije o novim modusima izbjegavanja nadzora. Uspjeh ovakvih operacija zavisi od iskustva istražitelja, njihove sposobnosti da prepoznaju obrasce ponašanja u fragmentiranom digitalnom okruženju i kapaciteta da simultano prate više kanala komunikacije. Drugi sloj operativnih strategija čini tehničko-forenzička analitika. Materijali prikupljeni kroz proaktivne operacije, zapljene uređaja ili prijave korisnika prolaze kroz složene faze digitalne obrade kao što su hash-matching, analizu metapodataka, geolokacijsku procjenu, vizuelnu klasifikaciju i identifikaciju potencijalnih žrtava. Automatizirani sistemi i algoritamska rješenja igraju ključnu ulogu u brzini obrade materijala, ali njihova efikasnost zavisi od kvaliteta nacionalnih baza podataka i mogućnosti pristupa međunarodnim platformama. Projekti poput kanadskog Project Arachnid, koji automatski skenira internet i detektira CSAM sadržaj u realnom vremenu, pokazali su se kao primjer dobre prakse, ali njihova primjena zavisi od regulatorne i tehničke infrastrukture u pojedinim državama. Australski modeli ACIC-a, koji povezuju obavještajne podatke s operativnim timovima i automatiziranim sistemima za praćenje mreža, dodatno ilustriraju kako centralizirani i tehnološki

sofisticirani pristupi mogu nadomjestiti nacionalne nedostatke u kadrovskim kapacitetima. Treći strateški sloj predstavlja međunarodna saradnja, bez koje je ozbiljna borba protiv online seksualne eksploatacije nemoguća. Većina CSAM sadržaja distribuira se preko servera koji se nalaze u drugim državama, a počinioci vrlo često koriste VPN-ove, proxy-je i enkriptirane komunikacije kako bi prikrili lokaciju, što istrage automatski uvodi u transnacionalnu domenu. Europolova Evropska cybercrime jedinica (EC3) koordinira operacije između članica EU, dok Europolove analitičke platforme omogućavaju identifikaciju obrazaca i povezivanje razbacanih fragmenata materijala. Interpolova ICSE baza podataka, koja sadrži identifikovane i neidentifikovane žrtve, ključni je alat koji omogućava da se pojedinačni slučajevi povežu u širi operativni mozaik. NCMEC-ova CyberTipline predstavlja međunarodni mehanizam koji može inicirati istrage u desetinama država za nekoliko sati, ali njegova efikasnost uveliko zavisi od toga koliko brzo i pouzdano nacionalne policijske institucije mogu reagirati na proslijeđene informacije.

Ipak, međunarodna saradnja suočava se s brojnim izazovima. Različiti standardi dokazivanja među državama, spor odziv internet provajdera na zahtjeve za dostavu podataka, pravne razlike u definiranju CSAM-a i enkripcija sadržaja koja onemogućava pristup podacima predstavljaju ozbiljna ograničenja. U mnogim slučajevima, čak i kada je identifikacija počinitelja moguća, pravni standardi dokazivanja u jednoj državi sprečavaju korištenje dokaza prikupljenih u drugoj, što dovodi do nesrazmjerno velikog broja neprocesuiranih predmeta. U slučajevima gdje se koriste kriptovalute za naplatu pristupa livestream zlostavljanju, istrage postaju dodatno složene, jer zahtijevaju kombinaciju digitalne forenzike, finansijskog praćenja i međunarodnog pravnog pomaganja, što mnoge države ne mogu brzo ili efikasno provesti.

5. Zaključak

Online seksualna eksploatacija djece danas se razvija u prostoru u kojem su ubrzane tehnološke promjene, globalna dostupnost digitalnih platformi i sofisticirane metode prikrivanja stvorile kriminalni ekosistem koji nadilazi kapacitete tradicionalnog pravnog i institucionalnog odgovora. Fenomen CSAM-a prestao je biti ograničen na lokalne granice ili pojedinačne aktere; on se oblikuje kao transnacionalna, dinamična i tehnološki potpomognuta prijetnja koja neprestano erodira postojeće modele zaštite djece. U takvom okruženju postaje jasno da normativni instrumenti, ma koliko dobro koncipirani, ne mogu ispuniti svoju svrhu ukoliko nisu praćeni odgovarajućim operativnim sposobnostima, tehničkim kapacitetima i stvarnom političkom voljom da se ovaj oblik nasilja prepozna kao prioritet sigurnosne agende.

Srž problema nije samo u nedosljednostima zakona, već u činjenici da se digitalni rizici razvijaju brže nego što pravni sistemi mogu reagovati. Generativna umjetna inteligencija, realistične vizualne manipulacije dječjih slika, enkripcija komunikacija i anonimne mreže potkopavaju tradicionalne metode kriminalističkog rada i zahtijevaju pristupe koji integrišu forenzičku analitiku, proaktivno nadziranje, međunarodnu koordinaciju i interdisciplinarno znanje. Bez takve integracije, istrage ostaju reaktivne, fragmentirane i spore, dok počinioci koriste prednosti digitalnog okruženja da bi izbjegli identifikaciju i pravne posljedice. Institucionalni odgovor, posebno u policiji i tužilaštvima, suočava se s teretom za koji mnogi sistemi nisu dizajnirani. Preopterećenost istražitelja, nedostatak specijalizirane obuke, psihološki pritisci dugotrajnog izlaganja CSAM materijalu i ograničena tehnička infrastruktura čine da se značajan broj predmeta nikada ne procesuira, a veliki broj žrtava ostaje neidentifikovan.

Ova strukturalna ograničenja stvaraju začarani krug jer što je sistem slabiji, to su počinioci hrabriji, a djeca izloženija, dok digitalno okruženje proizvodi nove oblike rizika brže nego što institucije uspijevaju izgraditi otpornost. Iz tih razloga, borba protiv online seksualne eksploatacije djece ne može se oslanjati isključivo na krivičnopravni odgovor, koliko god on bio neophodan. Potrebna je transformacija paradigme od reaktivnih modela koji intervenišu nakon nastanka štete, prema preventivnim, proaktivnim i tehnološki potpomognutim mehanizmima koji smanjuju dostupnost materijala, otežavaju pristup potencijalnim žrtvama, prepoznaju rizična ponašanja prije nego što eskaliraju i stvaraju digitalna okruženja u kojima su djeca manje ranjiva. U tom smislu, prevencija ne predstavlja dopunski segment sistema, nego njegov osnovni zaštitni okvir.

Kao zaključak pregleda navedene teorije, uviđa se da zaštita djece u digitalnom okruženju zahtijeva stabilan spoj tri elementa, a to su normativne jasnoće, operativne sposobnosti i međunarodne solidarnosti. Nijedan od ta tri elementa ne može djelovati samostalno. Međunarodni instrumenti moraju biti usklađeni s tehnološkom realnošću, institucije moraju biti finansijski i kadrovski ojačane, a saradnja između država mora biti brža, sadržajnija i oslobođena birokratskih barijera koje trenutno omogućavaju počiniocima da koriste geografske razlike kao zaštitni štit. Samo u sistemu koji prepoznaje da je sigurnost djece neraskidivo vezana za tehničke, političke i pravne kapacitete savremenih društava moguće je govoriti o stvarnoj, a ne deklarativnoj zaštiti njihovih prava.

LITERATURA

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 110–126.

Basave, A. E., Fernandez, M., & Alani, H. (2014). Detecting Child Grooming Behaviour Patterns on Social Media. *Lecture Notes in Computer Science*.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect*, 185–199.

Bouhours, B., & Broadhurst, R. (2011). *On-line Child Sex Offenders: Report on a Sample of Peer to Peer Offenders Arrested between July 2010-June 2011.* Canberra: Australian National University.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology*, 20–31.

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends and Issues in Crime and Criminal Justice*.

Cattaneo, C., Ritz-Timme, S., Gabriel, P., Gibelli, D., Giudici, E., Pasquale Poppa, D. N., . . . Grandi, M. (2009). The difficult issue of age assessment on pedo-pornographic material. *Forensic Science International*, 21-24.

Council of Europe. (2007). *Council of Europe Convention on the Protection of Children against Sexual.* Lanzarote: Council of Europe.

Dumitriu, C.-G., Dudu, A., & Nanău, I.-A. (2024). SYSTEMATIC REVIEW: GROOMING BEHAVIOR IN CASES OF CHILD SEXUAL ABUSE: STAGES OF THE PROCESS, RELATION DYNAMICS AND PREVENTION. *Anthropological Researches and Studies*, 268-292.

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & issuesin crime and criminal justice*.

Europol. (2025). *Internet Organised Crime Threat Assessment.* Europol.

Finkelhor, D., Turner, H., & Colburn, D. (2020). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Netw Open*. doi:doi:10.1001/jamanetworkopen.2022.34471

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect*, 238–248.

Grant, T., & Chiang, E. (2017). Online grooming: moves and strategies. *Language and Law*, 103-141.

Huemer, M.-A. (2024). *Revision of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.* European Parliamentary Research Service.

Interpol & ECPAT. (2018). *owards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.* ECPAT.

Johansson, C. (2019). *Combating online child sexual abuse material. An explorative study of Swedish police investigations.* Malmo: Faculty of Health and Society.

Kasper, A., & Laurits, E. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. *The Future of Law and eTechnologies*, 195–233.

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse*, 73-96.

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2017). The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse*, 173-196.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (2022). Child Sexual Abuse Material Online: The Perspective of Online Investigators on Training and Support Get access Arrow. *Policing: A Journal of Policy and Practice*.

Lee, H.-E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*.

Marturana, F., & Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, 193-204.

Maxwell, F. (2022). Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age. *The International Journal of Children's Rights*.

McManus, M. A., Long, M. L., Alison, L., & Almond, L. (2015). Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression*, 368–384.

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report.* NCMEC.

Ngo, V. M., Gajula, R., Thorpe, C., & Mckeever, S. (2024). Discovering child sexual abuse material creators' behaviors and preferences on the dark web. *Child Abuse & Neglect*.

O'Connell, R. (2003). *A Typology of Child Cybersexploitation and Online Grooming Practices.* Cyberspace Research Unit, University of Central Lancashire.

Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws* .

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, 50–64.

Pereira, M., Dodhia, R., Anderson, H., & Brown, R. (2024). Metadata-Based Detection of Child Sexual Abuse Material. *IEEE Transactions on Dependable and Secure Computing*, 3153-3164.

Ray, A., & Henry, N. (2024). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, 138-155.

Rezende, I. N. (2024). The proposed regulation to fight online child sexual abuse: An appraisal of privacy, data protection and criminal justice issues. *International Review of Law Computers & Technology*, 369–390.

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). *Digital Investigation*, 124-142.

Seigfried-Spellar, K. C. (2017). Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. *Journal of Police and Criminal Psychology*, 215–226.

Sorbán, K. (2024). Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations . *Belügyi Szemle*, 133-151.

Taylor, M., Holland, G., & Quayle, E. (2001). Typology of paedophile picture collections. *The Police Journal*, 97-107.

UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.* New York: UN.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, 303-313.

Westlake, B., Bouchard, M., & Frank, R. (2012). Comparing methods for detecting child exploitation content online. *European Intelligence and Security Informatics Conference*, (str. 153-163). Odense.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In Their Own Words: Young Peoples' Vulnerabilities to Being Groomed and Sexually Abused Online. *Psychology, 5*(10). doi:http://dx.doi.org/10.1016/j.avb.2012.09.003

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Colling, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 62-70.

WHO. (2020). *Global status report on preventing violence against children.* Geneva: WHO.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72–79.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72-79.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, 347–356.

ONLINE SEXUAL EXPLOITATION OF CHILDREN: OFFENDER METHODS AND SECURITY AGENCY RESPONSES

DOI: *10.70329/2744-2403.2025.5.10.8*

Review article

Aldina Bjelić, MA[3]

Abstract

Online sexual exploitation of children is one of the fastest-growing forms of cybercrime, driven by the rapid development of digital technologies, global connectivity and the wide availability of communication platforms. Offenders use different methods to target vulnerable children, including grooming, sextortion, social engineering, creating fake identities and distributing child sexual abuse material through encrypted channels, peer-to-peer networks and darknet services. Technological factors such as end-to-end encryption, cryptocurrencies, anonymisation networks and generative artificial intelligence further complicate detection and give offenders a high level of operational security. Security agencies respond by developing specialised teams, strengthening digital forensic capacities, improving international cooperation and relying on OSINT and SOCMINT methods to identify offenders and track criminal networks. However, challenges such as lack of staff, technical barriers, fragmented jurisdictions and the speed of technological change continue to limit the effectiveness of the institutional response. Legal and political measures, including the Budapest Convention and the Lanzarote Convention, provide a framework for action, but in practice there is still a significant gap between normative requirements and operational capabilities. The paper emphasises that combating online sexual exploitation of children requires a combination of preventive measures, technological innovation, multisectoral cooperation and stronger capacities of security institutions. Protecting children in the digital environment is not only a legal and social priority but also an important factor of overall security stability.

Keywords: *cybercrime, grooming, sextortion, darknet, OSINT*

[3] aldinabjelic@hotmail.com

1. Introduction

Online sexual exploitation of children is one of the most complex and fastest-growing challenges of the modern digital environment. The development of information and communication technologies, the wide availability of the internet and the mass use of smartphones have created new spaces of interaction where children spend an increasing part of their everyday lives. In this setting, traditional patterns of victimisation take on new digital dimensions, and offenders use specific techniques adapted to the online environment to identify, manipulate and exploit children. This phenomenon is becoming more serious because the internet enables a wide range of anonymous and hard-to-detect activities that cross geographical borders and escape traditional forms of oversight and control. At the same time, the global rise in cases of online sexual exploitation of children shows a growing gap between rapid technological progress and the ability of institutions to adequately protect the most vulnerable population. Security and other agencies face challenges such as encrypted communication channels, decentralised networks, cryptocurrencies and generative artificial intelligence, which further complicate the identification of offenders and the prosecution of criminal acts. Although international standards, legal frameworks and specialised units dealing with this form of crime already exist, their effectiveness often depends on technical equipment, digital forensic capacity and the level of international cooperation. Considering these circumstances, the aim of this review paper is to systematise current knowledge about the methods most commonly used by online offenders, analyse institutional and security responses, and highlight the key challenges that shape the possibilities for effective prevention and repression. The intention is to offer a clear and comprehensive overview of literature and practices that can help professionals, researchers and decision-makers improve child-protection policies in the digital environment.

2. Defining Cyber Exploitation of Children

Cyber exploitation of children refers to a set of criminal acts that involve the use of information and communication technologies for the sexual exploitation of minors, the distribution or production of child sexual abuse material, manipulation, extortion or other forms of unlawful behaviour against children. According to the Lanzarote Convention of the Council of Europe (2007), sexual exploitation of children includes all actions in which a child is used for the sexual satisfaction of another person, regardless of whether the act takes place in a physical or digital space. The digital environment allows these actions to occur without physical contact, while offenders use anonymity, technical protection and

the global availability of the internet to avoid monitoring and responsibility. Internet technology enables connecting distant users and spreading news and information, but it also carries the possibility of influencing the mind and ways of thinking of every human being (Muhić, 2025). In contemporary literature and practice, the term most commonly used is online sexual exploitation of children, or Online Child Sexual Exploitation, which according to Europol reports (2025) includes grooming, sextortion, recruitment of children for sexual activities via the internet and the distribution of child sexual abuse material. In this regard, special emphasis is placed on CSAM (Child Sexual Abuse Material), which visually depicts the sexual abuse of a child. Interpol and ECPAT (2018) increasingly propose the use of the term CSEM (Child Sexual Exploitation Material), emphasising that the focus is not only on the visual representation of abuse but also on the exploitation behind the creation of such content. One of the most important elements of cyber exploitation is grooming, the manipulative process of building trust between the offender and the child. Whittle et al. (2014) define grooming as a targeted, step-by-step and psychologically driven strategy in which the offender creates an emotional bond with the victim, preparing them for sexualised communication or contact. Grooming today mostly takes place on social networks, online games and chat applications, where the offender can communicate freely, without direct supervision by adults. Sextortion represents another key modality of exploitation, and Wolak et al. (2018) describe it as a form of extortion in which the offender demands additional sexual content, money or other benefits, threatening to publish real or manipulated material showing the child in a sexualised context. This form of crime is becoming more common due to the possibility of editing images and videos, including deepfake technology, which UNODC (2015) identifies as a growing challenge for victim identification and evidence procedures. Understanding cyber exploitation of children requires awareness of the technological factors that allow offenders to act with minimal risk. Reports by Europol and Interpol show that encrypted applications, anonymous networks such as Tor, cryptocurrencies and peer-to-peer systems provide a high level of digital security for offenders, while at the same time making investigations by security agencies more difficult. UNODC also warns about the rise of synthetic visual materials generated by artificial intelligence, which are used for manipulation, blackmail or distribution, further blurring the line between real and created content. Therefore, cyber exploitation of children can be clearly defined only when observed through three interconnected aspects- the criminal behaviours manifested in the digital environment, the technological tools that enable anonymity and the spread of material, and the psychological–manipulative strategies used by offenders in communication with victims. Only the combination of these elements allows proper recognition of risks, accurate categorisation of forms of exploitation and the development of institutional mechanisms for preventing and combating this type of crime.

3. Methods Used by Offenders in Online Sexual Exploitation of Children

The methods used by offenders in online sexual exploitation of children continually develop in parallel with the evolution of communication technologies, digital platforms and new possibilities for hiding identity. Unlike traditional forms of abuse, which require physical presence and direct contact, the online environment allows offenders to act transnationally, anonymously and with minimal risk of detection. Europol's IOCTA reports (2022–2025) emphasise that the greatest threat lies in the dynamic nature of these methods, which quickly adapt to changes in security protocols and monitoring mechanisms.

3.1 Grooming as a Central Behavioural Pattern

Grooming is one of the most complex and dangerous forms of online manipulation of children, and understanding it requires an analysis of the dynamic and interconnected stages through which offenders seek to achieve psychological control over the child. The typology developed by O'Connell (2003) is one of the most influential and detailed early models and serves as the basis for modern explanations of how communication patterns, manipulative strategies and technological factors fit into the process of exploitation. However, later studies show that grooming does not always follow a linear order and that offenders often speed up certain phases. For this reason, grooming today must be viewed as a fluid, adaptable and multidimensional process shaped by the offender's motivation, the child's characteristics and the specifics of the digital environment. O'Connell (2003) outlined several grooming stages that are important to consider for better understanding and investigating this type of crime.

Friendship-forming stage

According to O'Connell (2003), the process usually begins with the establishment of friendship, where the offender initiates the first contact with the child, either by pretending to be a peer or openly presenting themselves as an adult. The goal is to assess the child's willingness to communicate and to create a basic sense of familiarity. In this stage, the offender asks introductory questions about age, interests, school obligations or hobbies and may request photos of the child to confirm identity or check physical appearance. Dumitriu, Dudu and Nanău (2024) note that already in this stage it is possible to detect victim selection, since offenders target children who show signs of vulnerability or a need for approval.

Bond-forming stage

This stage represents the deepening of initial contact and the creation of emotional closeness. The offender presents themselves as support, a trustworthy listener or a "best friend", and the conversation expands to topics such as family relations,

school problems, successes, insecurities and everyday challenges (O'Connell, 2003). The goal is to create an illusion of emotional safety. According to Whittle et al. (2013), offenders actively monitor the child's emotional states in this phase to identify moments of vulnerability that can be used to strengthen the connection. Cano, Fernandez and Alani (2014) point out that this stage corresponds to the first part of Olson's theory of luring communication, known as Deceptive Trust Development, in which the offender intentionally creates an atmosphere of trust and shared identity.

Risk assessment stage

After establishing the basic relationship, offenders move to assessing the risk of being discovered. O'Connell (2003) explains that offenders ask questions such as "Who uses the computer?", "Are your parents at home right now?" or "Do you have a phone that only you use?" to determine the level of supervision and the safety of continued communication. This stage is essential because it influences the intensity and direction of the next actions. Chiang and Grant (2017) note that modern groomers often assess risk much earlier, sometimes within the first minutes of conversation, allowing quick evaluation of manipulation potential and avoidance of oversight.

Exclusivity stage

In this phase, the offender introduces narratives about a special relationship, shared secrets and emotional connection. Typical expressions include claims that the child can trust only them, that adults don't understand them, or that the two of them are "special" and "connected in a way others cannot understand". The goal is to isolate the child from other sources of support and create dependency. According to Dumitriu et al. (2024), this stage reflects mechanisms of isolation and psychological control similar to those found in offline abuse. This stage also prepares the child for the normalisation of sexualised communication by strengthening feelings of loyalty and emotional obligation.

Sexual stage

Once a certain level of trust and isolation is achieved, the offender gradually or suddenly introduces sexual content. Questions can range from subtle ("do you have a crush?") to direct ("do you touch yourself?"). Offenders may also request explicit images, suggest using a camera or describe sexual behaviour. Chiang and Grant (2017) show that modern groomers often introduce sexual content much earlier than O'Connell's model suggests, sometimes within minutes, which presents a major challenge for traditional detection tools. Kloess, Hamilton-Giachritsis and Beech (2017) distinguish between groomers who use an indirect approach, gradually increasing sexualisation, and those who use a direct approach without emotional preparation.

Fantasy enactment stage

O'Connell (2003) identifies a final stage in which the offender tries to involve the child in sexually explicit actions, either online or offline. This includes guiding the child through simulated sexual scenarios, performing explicit acts on camera or suggesting a physical meeting. Chiang and Grant (2017) confirm that this stage may appear very early in modern cases due to the fast pace of communication and the fact that many offenders operate within pedophile communities on the darknet, where knowledge and "tips" on effective exploitation strategies are shared.

Dynamic, overlapping and accelerated phases

Although O'Connell's model was pioneering and remains the most detailed staged approach, modern empirical studies (Chiang & Grant, 2017; Kloess et al., 2017) show that grooming in the contemporary online environment occurs much faster and that the stages are far from linear. Research shows that:
• all stages can occur within the first hour of communication
• sexualisation can appear in the first messages
• stages often overlap
• groomers may skip entire stages if the child appears vulnerable
• digital platforms enable fast escalation, especially when using encrypted apps

Dumitriu et al. (2024) confirm that grooming should be viewed as an adaptive process influenced by the offender's motivation, the victim's vulnerability and the communication context, and not as a fixed sequence of steps.

3.2 Online Sexual Extortion

Online sexual extortion is one of the most aggressive and harmful forms of technology-mediated sexual exploitation of children, and in the last decade it has become a priority threat in Europol reports and international organisations. Although public discourse often equated it with grooming or broader categories of online sexual violence, current research shows that it is a separate and highly destructive behavioural pattern. In simple terms, sextortion occurs when an offender threatens to publish, distribute or send sexually explicit images or videos of a child if the child does not meet certain demands, whether sexual, emotional or material. This basic structure of coercion forms the core of a phenomenon that, according to findings by Finkelhor et al. (2020), affects around 3.5% of youth before adulthood, while the real prevalence is likely much higher due to very low reporting rates.

Unlike grooming, which relies mostly on creating emotional closeness and gradually weakening boundaries, online sexual extortion is based on a sudden and

radical shift in power once the offender gains possession of sexual material involving the child. Açar (2016) defines this form of exploitation through three key elements, first, the digital environment as the setting of the act, second, possession of compromising material and the third, use of that material as a tool of blackmail. Only when all three elements are present can we speak of sextortion as a specific form of online sexual violence. This formulation is particularly useful because it distinguishes sexual extortion from grooming, sexting, cyberbullying and other digital risks. Research shows that the initial material is most often created through voluntarily sent images in the context of a romantic relationship, friendship or expected intimacy. Wolak et al. (2018) find that 75% of minor victims knowingly sent the first material but under pressure or emotional manipulation, and more than 60% of offenders came from the victim's circle of acquaintances, peers or former partners. These findings challenge the stereotype of the "stranger predator" and show that many incidents occur within existing adolescent power dynamics. At the same time, modern extortion increasingly involves unknown offenders, including criminal groups that use fake profiles to initiate the exchange of intimate images, escalate communication quickly and later demand money, more explicit material or other forms of obedience (Ray & Henry, 2024).

The methods of obtaining material vary, but three dominant patterns appear in the literature (Açar, 2016). The first concerns extortion within existing relationships, usually among adolescents, where intimate photos become a tool of control after conflict or a breakup. The second involves predatory behaviour in which grooming techniques are used only as an initial step to obtain visual material, followed by a quick escalation of threats. The third includes technically sophisticated methods, such as hacking accounts or cameras, although these are much less common in practice because they require knowledge that most offenders do not have (Açar, 2016). However, IoT devices and live-streaming functions introduce new risks, especially in the context of recording without consent. The dynamics of extortion are particularly dangerous because threats serve not only as a means of control but also as a factor of psychological destabilisation. Typically, the offender threatens to publish the material, send it to parents, friends or teachers, create fake profiles or distribute it within school communities. Studies show that many offenders repeat threats for months and that, in cases involving minors, they sometimes encourage self-harm or suicide to strengthen their control (Wolak et al., 2018). These escalations demonstrate that sextortion is not only a digital phenomenon but a form of psychological and emotional violence with severe consequences for the victim's mental health. The psychological consequences of sexual extortion are severe, and the literature reports long-term effects such as depression, strong anxiety, guilt, shame, withdrawal from social contact and serious self-destructive thoughts (Ray & Henry, 2024). There are documented cases in which children changed schools,

stopped education or attempted suicide to escape threats they did not know how to stop. Crucially, most victims do not seek help because half of minors in Wolak et al.'s (2018) study never reported the incident, fearing judgement, disbelief, parental reactions or damage to reputation. This creates a vicious cycle in which extortion continues precisely because it remains invisible.

3.3 Production and Distribution of CSAM: Technological Infrastructure, Criminal Dynamics and Challenges for Investigation

The modern production and distribution of child sexual abuse material (CSAM) takes place in a digital environment characterised by speed, anonymity and global reach. Technological development over the past twenty years has fundamentally changed criminal processes, making the creation and spread of CSAM easier and operationally safer for offenders. Lee et al. (2020) emphasise that today's online environment combines three key dimensions important for understanding this phenomenon, the legal framework, distribution channels and technical detection mechanisms. These dimensions shape the entire infrastructure in which offenders operate and, at the same time, set clear limitations for investigative bodies. The criminal process begins with the production phase, which now occurs in a wide range of contexts from direct contact abuse within intrafamilial settings to fully online exploitation through webcams and digital devices. The systematic review by Cale et al. (2021) shows that a significant portion of CSAM is produced in environments where the offender has direct access to the child. In more than half of cases, the offender is a family member or close acquaintance of the victim. This is confirmed by findings from Gewirtz-Meydan et al. (2018), which show that family members, partners of parents and individuals in the child's immediate environment are the most common producers of such content. At the same time, there is a growing number of cases in which CSAM is produced exclusively online, without physical contact, through direct persuasion of children to perform sexualised acts in front of a camera (McManus, Long, Alison, & Almond, 2015). This form represents a relatively new category of digital crime, encouraged by the expansion of video-communication apps and offenders' low perception of risk.

The distribution of CSAM is central within the modern ecosystem of child sexual exploitation and takes place through three dominant channels. Firsth is the open web, then P2P networks and finaly, the dark web. On the open web, CSAM appears in two contexts, in direct offender-child interactions through social networks, and in the form of unstructured, temporarily available material that escapes moderation. Cale et al. (2021) note that the open web is where most initial contacts between children and offenders occur, especially on platforms such as Facebook, Instagram, Snapchat and various video-sharing applications. Grooming, sexualised persuasion and the collection of initial photos dominate this segment, and this content often becomes the starting point for broader distribution

within criminal networks. This shows a constant connection between production and distribution because material created during grooming frequently becomes part of wider circulation. P2P networks form the second layer of distribution and enable global sharing of large files without a central intermediary. Bissias et al. (2016) estimate that at a certain point more than 800,000 users worldwide participated in sharing CSAM on P2P networks, while Bouhours and Broadhurst (2011) highlight that much of the exchange occurs locally within language and cultural groups of connected users. These networks are characterised by huge data volumes, frequent sharing of long-term archived material and fragmentation of files, all of which make the identification of original content more difficult. Police agencies in many countries report that P2P networks generate workloads that exceed their technical and staffing capacities, a finding also confirmed by Johansson (2019) in the Swedish policing context.

The most organised and dangerous layer of distribution is found on the dark web. Ngo, Gajula, Thorpe and McKeever (2024) analysed more than 353,000 posts on eight dark web forums and identified over 10,000 active CSAM contributors who use these platforms for material exchange, communication, advice on avoiding detection and the creation of closed communities. The authors note specific criminal patterns, exchange of exclusive content, coded jargon, advanced operational security practices and structured hierarchies in which status is built through volume of contribution. These structures represent the digital equivalent of organised criminal networks and significantly hinder infiltration and evidence collection. Research also shows that platforms such as Tor and I2P are the main access channels, supported by encryption, cryptocurrencies and decentralised hosting services that further complicate investigative work.

All these dynamics generate serious operational challenges for investigations. Leclerc et al. (2022) report that investigators around the world highlight the lack of specialised training, technical resources and analytical support as the biggest obstacles to effective case processing. Problems range from outdated equipment and a shortage of digital forensic experts to weak cooperation with global social networks and legal barriers that slow access to data. Johansson (2019) further notes that many police organisations still treat CSAM as a lower-priority offence, resulting in overloaded investigators, lengthy procedural delays and an institutional response that remains weak compared to the scale of harm.

3.4. Techniques for Identifying Victims and Offenders

Identifying victims and offenders in cases of online child sexual abuse represents the key link between the “digital trace” and the traditional criminal justice process. Three layers interact in this process: forensic analysis of visual content,

automated detection and classification techniques for CSAM, and operational-investigative methods aimed at tracing the real individuals behind the screen. Modern literature shows that none of these components is sufficient on its own. The greatest effect is achieved by combining several approaches, supported by a clearly defined institutional division of roles and responsibilities.

3.4.1. Forensic Analysis and Classification of Visual Material

A basic precondition for identifying victims and offenders is the ability to recognise that certain material involves child sexual abuse and to consistently classify it according to legal categories. Kloess et al. show that even experienced police analysts have significant difficulty evaluating two key dimensions whether the person shown is a child, and whether the content is "illegal" or "indecent" in a legal sense (Kloess, Woodhams, Whittle, Grant, & Hamilton-Giachritsis, 2017). Particularly challenging are so-called "borderline images", such as early pubescent adolescents, partial nudity or situations where context may be interpreted as "innocent". Inter-rater analyses show higher disagreement among coders on such material, which directly affects the consistency of prosecution and assessment of offence severity. To reduce subjectivity, classification tools such as the COPINE scale and later simplified categories (A, B, C) were introduced, separating penetrative acts, non-penetrative sexual activities and "erotic posing" (Taylor, Holland, & Quayle, 2001). However, category C ("erotic posing") illustrates how fluid the normative boundary is. Analysts often admit they prefer to focus on clearly severe material, while lower-level cases remain in a zone of uncertainty. This has a direct impact on victim identification, as children whose images are not formally recognised as CSAM remain outside proactive investigations and international databases.

Age estimation presents a particular challenge. Research shows that even medical experts are not significantly better than laypersons at distinguishing older adolescents from adults on the basis of photographs, due to high variability in pubertal development (Cattaneo et al., 2009). In the digital context this challenge is heightened by ethnic differences in body structure, changes in body mass index and the global nature of CSAM. In practical terms this means that age assessment must be combined with other indicators such as scene context, metadata, file names, language and cultural elements of the environment, rather than relying solely on visual impression.

3.4.2. Hash Databases, P2P Monitoring and Web Crawlers as Foundations of Identification

On the technical level, most modern CSAM-detection systems rely on hash databases of known material. PhotoDNA and similar technologies generate "fingerprints" of images, allowing recognition of previously identified files even when they have been partially altered (Edwards, Christensen, Rayment-McHugh, & Jones, 2021). This achieves two goals. First, the number of digital artefacts

requiring manual review is drastically reduced, and investigators can track the same victim across different offender collections and platforms, which is crucial for physical rescue. Monitoring of P2P networks and specialised tools such as iCOP go further by combining hash searches with analysis of file names and network traffic (Peersman, Schulze, Rashid, Brennan, & Fischer, 2016). Studies show that a small number of "nodes" produce a disproportionately large share of CSAM traffic, and that removing only the top of the distribution pyramid could reduce material availability on certain networks by 30–40% (Wolak, Liberatore, & Levine, 2014). From the perspective of offender identification, tracking IP addresses, sharing patterns and "seed file" lists allows profiling of the most active distributors, who are often the main producers or administrators of closed communities, meaning actors with the highest "operational significance".

Web crawlers applied to the clear web and, to a limited extent, to the darknet automatically track links from known CSAM domains and map networks of connected pages (Westlake, Bouchard, & Frank, 2012). Initiatives such as Project Arachnid demonstrate that it is possible to process hundreds of millions of pages and identify tens of thousands of unique CSAM images in a short period of time, giving police the capability to target sites with the highest "centrality" and disrupt distribution infrastructure. At the same time, every instance in which a known image appears at a new location generates a trace that may lead to new offenders and potentially new information about the identity of the victim.

3.4.3. Metadata, File Names and Darknet Analysis

Newer studies increasingly highlight the value of metadata and textual traces as sources for identifying both CSAM content and the actors involved in its distribution. Research by Pereira et al. shows that classification models based solely on file names and file paths can achieve a high level of accuracy because offenders tend to develop specific, recognisable vocabulary and coded language when naming their files (Pereira, Dodhia, Anderson, & Brown, 2024). P2P searches already rely heavily on textual searches of file names, so moving towards automated analysis of these patterns is a logical next step.

Ngo et al. developed a machine-learning system for detecting CSAM on dark web forums, which, on a corpus of over 350,000 posts, successfully identified around 63,000 CSAM-relevant entries and more than 10,500 "creators" of CSAM content (Ngo et al., 2024). Analysis of metadata from these posts offers several key insights: dominant themes and preferences of certain authors, typical age groups and nationalities of victims mentioned, and platforms most commonly used for obtaining and exchanging material (Omegle, YouTube, Skype, Instagram, Telegram). For the purpose of offender identification, such patterns serve as a basis for targeting the most active and dangerous individuals, as well as for identifying new hotspots on "surface" platforms where victims are recruited or

where CSAM is initially produced (e.g., live streaming via VoIP applications, webcams and social networks).

Metadata in a broader sense – such as EXIF data, timestamps, geolocation, software version and system language – further enrich the analytical picture. Although offenders are increasingly aware of the need to "clean" metadata, the analysis of millions of files and network interactions still allows statistical profiling of typical configurations, time patterns and technological tools used by certain groups. This does not automatically provide a specific identity, but it narrows the operational field and guides traditional investigative work.

3.4.4. Automated Detection, AI and Forensic Workflow

The review of literature on automated CSAM detection shows a clear convergence. The most effective systems combine multiple modalities – hash values, visual characteristics of images, textual signals in file names and metadata – instead of relying on a single indicator (Edwards et al., 2021). Deep neural networks achieve the best results when detecting previously unseen CSAM, especially when multiple image and video descriptors are merged into a unified classifier (Lee, Ermakova, Ververis, & Fabian, 2020). Vitorino et al. (2018) show that CNN models trained on large police datasets can effectively distinguish CSAM from adult pornography, while studies combining pornography detection and age estimation further narrow the focus on potential child victims (Vitorino et al., 2018; Lee et al., 2020). However, Pereira et al. emphasise that models must be tested in realistic scenarios, including fully benign "out-of-sample" sets and situations in which offenders intentionally modify textual patterns (adversarial examples such as "Lo7ita", "b4", and similar) (Pereira et al., 2024). A high rate of false positives can practically block the implementation of such systems on platforms with billions of users, and for police work it creates additional operational burden. The practitioner survey by Sanchez et al. shows that investigators are highly sensitive to false positives; most consider a high FP rate a more serious problem than missed cases precisely because FP findings directly overwhelm limited resources (Sanchez, Grajeda, Baggili, & Hall, 2019). At the same time, Sanchez et al. (2019) note that many practitioners are not sufficiently familiar with data science and AI basics, even though they already work with tools that rely on these techniques. This creates a gap between technological potential and actual practical use.From a technical standpoint, many tools for triage and filtering have been developed – from simple pixel-level nudity detectors, through specialised field-triage tools, to complex systems that automatically rank devices and storage media by the likelihood of containing relevant evidence (Marturana & Tacconi, 2013). In terms of identifying victims and offenders, their value lies in reducing the time investigators spend reviewing large amounts of benign material, allowing them to reach "clean" CSAM faster, where concrete faces, environments and behavioural patterns can be recognised.

3.4.5. Identification of Victims and Offenders

Although most of the technologies mentioned above primarily serve to detect and classify content, they also form the foundation for identifying victims and offenders in a narrower sense. In practice, this process unfolds through several complementary steps. First, hash databases and automated visual detection help isolate material that contains previously unidentified victims, which then becomes a priority for specialised "victim identification" teams (Edwards et al., 2021; Johansson, 2019). Second, estimating age, external characteristics, background language and cultural artefacts (such as clothing, architecture or household items) helps to geographically and demographically attribute the victim, although Kloess et al. (2017) clearly show that age estimation remains a major source of uncertainty, especially with adolescents. Third, investigative teams increasingly use techniques such as facial recognition, comparison of rooms, furniture and "micro-environments" across different cases and reports, which makes it possible to link the same victim or offender across multiple investigations and jurisdictions (Edwards et al., 2021). In a broader criminological sense, studies on crime commission processes show that CSAM producers often merge online and offline dimensions, combining contact abuse with recording and digital distribution. Key decisions in these cases depend on the offender's assessment of detection risk, access to children and technical capacity (Cale et al., 2021). Understanding these processes helps police prioritise offenders who are likely to be both online distributors and offline abusers.

Offender identification also depends on traditional digital traces such as IP addresses, logs, social media accounts, communication within P2P and darknet environments and the way these elements are integrated with OSINT, HUMINT, SIGINT and classic investigative methods. In the investigation of organised criminal groups and their members, open sources such as social networks provide a large amount of relevant information, including photographs, videos, posts and similar content (Muhić, 2024). Johansson shows that in Sweden, for example, one major challenge is the lack of an obligation for ISPs to store IP logs, which directly complicates offender identification even when CSAM content has been detected (Johansson, 2019). Similarly, Leclerc et al. (2022) report that police investigators highlight a mix of "social engineering" communication skills, strong IT literacy and understanding of sexual offender profiles as key competencies. In other words, even the most advanced algorithms cannot replace the investigator's ability to turn digital traces into operational hypotheses and test them through interviews, surveillance and other measures.

3.4.6. The Human Factor: Capacities, Workload and Investigator Protection

Most of the techniques described above require intensive work by specialised police teams and digital forensic analysts. Multiple studies confirm that this professional group faces a high risk of secondary trauma, chronic stress and burnout due to ongoing exposure to extremely disturbing content (Burns, Morley,

Bradshaw, & Domene, 2008; Seigfried-Spellar, 2017; Sanchez, Grajeda, Baggili, & Hall, 2019). Investigators in Leclerc's study identify several key problems such as enormous data volumes, lack of personnel and technical resources and limited understanding of the CSAM phenomenon among the management of their own institutions (Leclerc et al., 2022). Johansson reports similar findings in Sweden: different police regions follow different procedures, digital forensic staff represent a major "bottleneck" and CSAM is often treated as a "low-priority" crime in practice (Johansson, 2019). Sanchez et al. (2019) show that investigators recognise the high value of filtering and triage technologies, mainly because they reduce exposure to harmful material and speed up the workflow. At the same time, investigators report relatively limited use of advanced AI-based tools, partly because they do not fully understand how such tools work (Sanchez, Grajeda, Baggili, & Hall, 2019). Effective implementation of techniques for identifying victims and offenders therefore requires more than simply procuring technological solutions. It also demands investment in systematic training, supervision, psychological support and clear operational protocols to ensure that the personnel who perform the most difficult tasks remain functional and professionally sustainable.

4. Institutional, Operational and Legal Responses to Online Sexual Exploitation of Children

4.1. National and International Legal Framework

The modern international legal framework regulating online sexual exploitation of children was developed in a period that did not anticipate today's scale, speed and technological capabilities of digital production and distribution of child sexual abuse material. Despite strong normative density and wide adoption of key international instruments, there is a visible structural tension between the formal obligations of states and their actual capacities to respond adequately to a phenomenon that evolves faster than legislation can adapt. According to the *Global Status Report on Preventing Violence Against Children* (WHO, 2020), most states have relatively developed normative frameworks for child protection, but fewer than half possess effective implementation mechanisms. In the digital environment, where CSAM is distributed through anonymous networks, peer-to-peer systems, encrypted communication channels and platforms based on generative artificial intelligence, this gap between normative commitments and operational capacity becomes even more pronounced. Understanding the international and European legal framework is therefore essential for identifying the root causes of investigative failures, delays in victim identification and the limited reach of criminal justice mechanisms. The *Convention on the Rights of the Child* (CRC) of 1990 is the foundational international instrument for child protection, yet it was created in a historical context in which the internet was only

beginning to enter wider use. For that reason, the CRC does not contain specific provisions recognising the digital environment as a primary space of victimisation, nor does it address phenomena such as virtual CSAM, deepfake technologies, visual manipulation or anonymous global markets operating through the darknet. Its greatest strength lies in establishing principles such as the best interests of the child, the obligation to take preventive action and the promotion of child development. However, these principles remain insufficiently operationalised in the digital context. The *Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography* (OPSC) represents an attempt to fill these gaps, but Maxwell's analysis (2022) shows that the OPSC remains primarily focused on criminalisation, while preventive measures are formulated broadly, suggestively and without clear minimum standards that states must meet. This approach leads to a situation in which states mostly fulfil their formal criminalisation obligations, while systemic preventive policies remain underdeveloped or entirely absent.

The Budapest Convention of the Council of Europe (2001) is the first comprehensive international instrument addressing computer-mediated crime, including the production, distribution and possession of "child pornography" under Article 9. It established the architecture for international police and judicial cooperation, but its effectiveness has been limited by several structural factors. The transnational nature of CSAM-related crime complicates the application of territorial jurisdiction, meaning that cases involving servers, offenders and victims in different countries often end up in lengthy mutual legal assistance procedures. In addition, states define illegal content differently, especially in relation to virtual, realistic or AI-generated depictions of children, which complicates coordinated action and evidence exchange (Sorbán, 2024). Differences in regulations on mandatory retention of IP logs further burden investigations, since some jurisdictions store logs for only a few months while others keep them for years, which in practice determines the outer limits of successful digital investigations (Kasper & Laurits, 2016).

The Lanzarote Convention (2007) introduced a qualitative shift by criminalising grooming behaviour via information technologies and establishing the obligation of states to take all appropriate measures to protect children from online sexual exploitation. However, as with all Council of Europe instruments, the Lanzarote Convention lacks mechanisms to sanction states that fail to implement their obligations. Its flexible normative structure allows different interpretations, especially regarding virtual and AI-manipulated depictions, which creates additional legal gaps in the context of generative AI and advanced image-manipulation tools (Parti & Szabó, 2024). Although it introduced important conceptual innovations, the Lanzarote Convention did not anticipate the creation of fully fictional, hyper-realistic depictions of children. As a result, its application to AI-generated content remains under-developed.

At the regional level, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children is the most important instrument. It obliges EU Member States to criminalise all forms of online sexual exploitation, including grooming, possession, distribution, creation and facilitation of CSAM. The Directive also provides for proactive investigations that do not depend on a victim's report, extended extraterritorial jurisdiction, victim-support measures from the earliest stages of proceedings and specialised operational mechanisms. However, as a minimum-harmonisation instrument, it allows Member States to transpose its provisions differently, which has resulted in deep differences in definitions, procedures and sanctions. This fragmentation hinders investigative coordination, evidence exchange, cooperation with Europol and the implementation of joint operations, particularly in cases involving peer-to-peer systems, encrypted applications or AI-generated content (Huemer, 2024). An additional problem is that the Directive does not provide detailed guidance on the challenges posed by generative AI, does not address realistic child-like avatars in metaverse environments and does not offer solutions for situations in which end-to-end encryption prevents access to evidence. The most recent attempt to create a stronger European legal framework is the draft Regulation COM (2022) 209 final, which would require internet platforms to detect, remove and report CSAM, as well as identify grooming communication through automated systems. The Regulation, however, raises serious questions about the balance between child protection and privacy, since its practical implementation would require monitoring user communications in ways that conflict with standards of encrypted private communication and the principles of the GDPR (Rezende, 2024). European privacy-protection organisations warn that such large-scale monitoring could set a precedent for mass surveillance, while police and prosecution bodies argue that without these mechanisms it is impossible to address the exponential growth of online child exploitation.

All these layers of legal regulation point to a deeply rooted problem which is the existing legal instruments were created in an era of analogue crime and are not fully capable of responding to digital phenomena that involve global distribution, trace deletion, E2EE communication, the use of cryptocurrencies and generative artificial intelligence. Differences in definitions, capacities and legal implementation across states place children in an unequal position, while operational barriers such as inconsistent IP-log retention, slow international legal assistance and limited access to digital evidence often result in failed investigations or an inability to identify victims. This makes it clear that, despite widely ratified instruments and formally high protection standards, the legal framework remains insufficiently aligned with the real demands of the digital environment. A deep, structural reform is required if the system is to respond effectively to the growing phenomenon of online sexual exploitation of children.

4.2. Organisational Models and Capacities of Police and Prosecution Services
Although the international and European legal framework sets minimum standards for criminalisation and interstate cooperation, the actual level of child protection in the digital environment depends primarily on the organisational models, capacities, resources and operational procedures of national police and prosecutorial institutions. Online sexual exploitation of children cannot be effectively addressed within systems whose institutional architecture belongs to the period before mass digitalisation, nor within organisations that still treat digital crime as a peripheral form of offending. Empirical data and comparative studies (Sanchez et al., 2019; Johansson, 2019) show that most national systems face chronic shortages of specialised units, fragmented procedures, insufficiently trained staff and the high emotional burden that prolonged exposure to CSAM material places on investigators. These weaknesses have direct consequences. Many cases remain uninvestigated, identified victims remain unidentified in practice and prosecutorial files are delayed for months or even years.

In most countries, the organisational response relies on specialised cybercrime, digital forensics and sexual offences units, yet the real scope of their mandates and capacities varies significantly. Structurally, police agencies usually apply a model in which digital investigations unfold across three components- analytical, operational and forensic. Analytical units collect and process reports, analyse OSINT and SOCMINT traces, map P2P networks and track distribution trends. Operational units conduct undercover activities in online environments, initiate covert communication with suspects and collect real-time material traces. Forensic units handle seized devices, analyse metadata, use hash databases and specialised algorithms to identify content and extract evidence for criminal proceedings. However, in practice these three functions are often separated, poorly coordinated and dependent on the individual motivation and expertise of a small number of officers. This represents a major limitation in cases where speed, technological knowledge and inter-sectoral communication determine the outcome of the investigation.

The overburdening of police and prosecutorial capacities represents a particularly acute challenge. The study by Sanchez et al. (2019) shows that investigators working on CSAM cases operate under significant psychological pressure, are exposed to secondary victimisation and frequently experience symptoms of burnout. This leads to high staff turnover, reduced efficiency and a loss of institutional memory. In many countries, the number of reports far exceeds available personnel. In 2023 alone, NCMEC received 35.9 million reports (National Center for Missing & Exploited Children, 2023), while Europol and Interpol continue to record a constant rise in material distributed in fragments across encrypted chat applications, cloud services and dark web forums. Police and prosecutorial bodies cannot keep up with this volume, resulting in selective prioritisation, often at the expense of cases involving online grooming or material

without immediate physical abuse, but with significant long-term psychological consequences for children. In such systems, CSAM is treated in many states as a "lower-priority" offence, which directly affects the speed and quality of investigations.

Technical infrastructure adds another dimension to institutional limitations. Processing terabytes of data from seized devices requires advanced tools, large storage capacities and specialised SQL or AI-driven systems capable of classifying content, identifying victims and linking cases across jurisdictions. In many countries, these systems are not standardised; instead, a heterogeneous mix of outdated software, commercial tools and open-source solutions is used, often without interoperability (Johansson, 2019). The lack of standardisation complicates forensic analysis, slows down investigations and undermines the quality of evidence presented to prosecutors. In addition, police agencies in resource-limited states often lack even basic capacities for device decryption, analysis of encrypted communications or work with P2P monitoring tools, creating a visible gap between the technological capabilities of offenders and the institutional capacity to counter them.

The role of international institutions such as NCMEC, Europol and Interpol is therefore crucial in bridging some of these gaps, but their work also exposes weaknesses within national systems. Europol's EC3, Interpol's ICSE database and NCMEC's CyberTipline provide essential tools for victim identification and coordination of global records, yet their effectiveness depends on the speed and quality of national responses. States without developed capacities for proactive scanning, hash-matching or metadata analysis remain outside global information flows, leaving victims in those jurisdictions unidentified and offenders unprosecuted. In this sense, international infrastructure can only partially compensate for national weaknesses; it cannot replace the absence of specialised staff, clear procedures, adequate funding or the political will to treat online sexual exploitation of children as a priority issue.

4.3. Operational Strategies and Models of Cooperation in Countering Online Sexual Exploitation of Children

Operational responses to online sexual exploitation of children develop within a complex environment where technological innovation, transnational criminal ecosystems and institutional differences between states intersect. While legal frameworks define obligations and organisational capacities determine what is practically feasible, operational strategies represent the final and most dynamic layer of institutional action, the point where norms and capacities must be translated into real investigations, victim identification and the dismantling of offender networks. Online child exploitation is marked by extreme fluidity. Offenders use diverse platforms, move rapidly between services, combine

legitimate and anonymous communication channels and increasingly rely on generative AI tools. In such an environment, traditional reactive policing models have proven insufficient, pushing states toward proactive, intelligence-led and internationally coordinated strategies.

Operational strategies rest on three core approaches such as proactive detection, technical-forensic analytics and international cooperation. Proactive strategies involve systematic monitoring of online spaces, the use of undercover identities when communicating with suspects, the identification of grooming patterns and the analysis of open and semi-closed online environments. OSINT and SOCMINT methods become indispensable in this context. Police units gather information from public profiles, digital traces, social networks, open P2P hubs and crypto forums, and use algorithmic tools to detect risky interactions. Edwards et al. (2021) emphasise that P2P monitoring is not only a technical mechanism for detecting CSAM distribution but also a tactical strategy for infiltrating closed networks where offenders share material and information on new methods of evading detection. The success of such operations depends on investigator experience, their ability to recognise behavioural patterns in fragmented digital environments and their capacity to monitor multiple communication channels at once. The second layer of operational strategies is technical-forensic analytics. Material obtained through proactive operations, device seizures or user reports passes through complex stages of digital processing, hash matching, metadata analysis, geolocation assessment, visual classification and the identification of potential victims. Automated systems and algorithmic tools are crucial for processing speed, but their effectiveness depends on the quality of national databases and access to international platforms. Projects such as Canada's Project Arachnid, which automatically scans the internet and detects CSAM content in real time, have proven valuable models, although their implementation depends on national regulatory and technical infrastructures. Australia's ACIC models, which integrate intelligence data with operational teams and automated network-monitoring systems, further demonstrate how centralised and technologically advanced approaches can compensate for shortages in national staffing capacities. The third strategic layer is international cooperation, without which a serious fight against online sexual exploitation is impossible. Most CSAM is hosted or distributed via servers located in other countries, and offenders frequently use VPNs, proxies and encrypted communications to obscure their location, automatically turning investigations into transnational cases. Europol's European Cybercrime Centre (EC3) coordinates operations among EU member states, and Europol's analytical platforms help identify patterns and connect scattered fragments of material. Interpol's ICSE database, containing identified and unidentified victims, is a crucial tool enabling individual cases to be linked into a broader operational picture. NCMEC's CyberTipline can trigger investigations in

dozens of countries within hours, but its effectiveness depends heavily on the speed and reliability of national police responses.

However, international cooperation faces numerous obstacles. Differences in evidentiary standards between states, slow responses from internet service providers to data requests, legal differences in CSAM definitions and content encryption all pose significant limitations. In many cases, even when an offender can be identified, evidentiary standards in one jurisdiction prevent the use of material collected in another, resulting in a disproportionate number of unprosecuted cases. In situations where cryptocurrencies are used to pay for access to livestreamed abuse, investigations become even more complex, requiring a combination of digital forensics, financial tracking and mutual legal assistance, processes that many states cannot carry out quickly or effectively.

5. CONCLUSION

Online sexual exploitation of children is developing in an environment where rapid technological change, global access to digital platforms and sophisticated methods of concealment have created a criminal ecosystem that exceeds the capacities of traditional legal and institutional responses. The CSAM phenomenon is no longer limited to local boundaries or isolated offenders; it has evolved into a transnational, dynamic and technologically enabled threat that continually erodes existing models of child protection. In such a context, it becomes evident that normative instruments, no matter how well designed, cannot achieve their purpose unless accompanied by adequate operational abilities, technical capabilities and real political will to recognise this form of violence as a priority security concern.

The core problem does not lie only in inconsistencies within the law, but in the fact that digital risks evolve faster than legal systems can respond. Generative artificial intelligence, realistic visual manipulation of child images, encrypted communication and anonymous networks undermine traditional investigative methods and require approaches that integrate forensic analytics, proactive monitoring, international coordination and interdisciplinary knowledge. Without such integration, investigations remain reactive, fragmented and slow, while offenders exploit the advantages of the digital environment to avoid identification and legal consequences.

The institutional response, particularly within police and prosecution services, faces a burden for which many systems were never designed. Overworked investigators, a lack of specialised training, the psychological pressures of long-

term exposure to CSAM material and limited technical infrastructure result in a large number of cases never being processed and many victims remaining unidentified. These structural limitations create a vicious cycle, the weaker the system, the bolder the offenders and the more exposed the children, while the digital environment produces new forms of risk faster than institutions can build resilience.

For these reasons, the fight against online sexual exploitation of children cannot rely solely on the criminal justice response, although it remains indispensable. What is needed is a shift in paradigm from reactive models that intervene only after harm occurs, toward preventive, proactive and technologically supported mechanisms that reduce material availability, restrict access to potential victims, recognise risky behaviours before they escalate and create digital environments in which children are less vulnerable. In this sense, prevention is not a supplementary component of the system but its primary protective framework.

P As a conclusion of the reviewed theory, it becomes clear that protecting children in the digital environment requires a stable combination of three elements: normative clarity, operational capability and international solidarity. None of these elements can function on its own. International instruments must be aligned with technological realities, institutions must be strengthened in terms of funding and staffing, and cooperation between states must be faster, more substantial and free of bureaucratic barriers that currently allow offenders to use geographical differences as a protective shield. Only in a system that recognises that child safety is closely linked to the technical, political and legal capacities of modern societies can we speak of real, and not merely declarative, protection of children's rights.

LITERATURE

Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 110–126.

Basave, A. E., Fernandez, M., & Alani, H. (2014). Detecting Child Grooming Behaviour Patterns on Social Media. *Lecture Notes in Computer Science*.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect*, 185–199.

Bouhours, B., & Broadhurst, R. (2011). *On-line Child Sex Offenders: Report on a Sample of Peer to Peer Offenders Arrested between July 2010-June 2011.* Canberra: Australian National University.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology*, 20–31.

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends and Issues in Crime and Criminal Justice*.

Cattaneo, C., Ritz-Timme, S., Gabriel, P., Gibelli, D., Giudici, E., Pasquale Poppa, D. N., . . . Grandi, M. (2009). The difficult issue of age assessment on pedo-pornographic material. *Forensic Science International*, 21-24.

Council of Europe. (2007). *Council of Europe Convention on the Protection of Children against Sexual.* Lanzarote: Council of Europe.

Dumitriu, C.-G., Dudu, A., & Nanău, I.-A. (2024). SYSTEMATIC REVIEW: GROOMING BEHAVIOR IN CASES OF CHILD SEXUAL ABUSE: STAGES OF THE PROCESS, RELATION DYNAMICS AND PREVENTION. *Anthropological Researches and Studies*, 268-292.

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & issuesin crime and criminal justice*.

Europol. (2025). *Internet Organised Crime Threat Assessment.* Europol.

Finkelhor, D., Turner, H., & Colburn, D. (2020). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Netw Open*. doi:doi:10.1001/jamanetworkopen.2022.34471

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect*, 238–248.

Grant, T., & Chiang, E. (2017). Online grooming: moves and strategies. *Language and Law*, 103-141.

Huemer, M.-A. (2024). *Revision of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.* European Parliamentary Research Service.

Interpol & ECPAT. (2018). *owards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.* ECPAT.

Johansson, C. (2019). *Combating online child sexual abuse material. An explorative study of Swedish police investigations.* Malmo: Faculty of Health and Society.

Kasper, A., & Laurits, E. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. *The Future of Law and eTechnologies*, 195–233.

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse*, 73-96.

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2017). The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse*, 173-196.

Leclerc, B., Cale, J., Holt, T., & Drew, J. (2022). Child Sexual Abuse Material Online: The Perspective of Online Investigators on Training and Support Get access Arrow. *Policing: A Journal of Policy and Practice*.

Lee, H.-E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*.

Marturana, F., & Tacconi, S. (2013). A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, 193-204.

Maxwell, F. (2022). Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age. *The International Journal of Children's Rights*.

McManus, M. A., Long, M. L., Alison, L., & Almond, L. (2015). Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression*, 368–384.

Muhić, E. (2024). Operativna upotreba OSINT-a u istraživanju organiziranih kriminalnih grupa. *Zaštita i sigurnost, 4*(2), 314-338.

Muhić, E. (2025). Psihološke operacije na društvenim mrežama - primjeri, tehnike, taktike i procedure. *Zaštita i sigurnost, 5*(1). doi:https://doi.org/10.70329/2744-2403.2025.5.9.7

National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report.* NCMEC.

Ngo, V. M., Gajula, R., Thorpe, C., & Mckeever, S. (2024). Discovering child sexual abuse material creators' behaviors and preferences on the dark web. *Child Abuse & Neglect*.

O'Connell, R. (2003). *A Typology of Child Cybersexploitation and Online Grooming Practices.* Cyberspace Research Unit, University of Central Lancashire.

Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws* .

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, 50–64.

Pereira, M., Dodhia, R., Anderson, H., & Brown, R. (2024). Metadata-Based Detection of Child Sexual Abuse Material. *IEEE Transactions on Dependable and Secure Computing*, 3153-3164.

Ray, A., & Henry, N. (2024). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, 138-155.

Rezende, I. N. (2024). The proposed regulation to fight online child sexual abuse: An appraisal of privacy, data protection and criminal justice issues. *International Review of Law Computers & Technology*, 369–390.

Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). *Digital Investigation*, 124-142.

Seigfried-Spellar, K. C. (2017). Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. *Journal of Police and Criminal Psychology*, 215–226.

Sorbán, K. (2024). Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations . *Belügyi Szemle*, 133-151.

Taylor, M., Holland, G., & Quayle, E. (2001). Typology of paedophile picture collections. *The Police Journal*, 97-107.

UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.* New York: UN.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, 303-313.

Westlake, B., Bouchard, M., & Frank, R. (2012). Comparing methods for detecting child exploitation content online. *European Intelligence and Security Informatics Conference*, (str. 153-163). Odense.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In Their Own Words: Young Peoples' Vulnerabilities to Being Groomed and Sexually Abused Online. *Psychology, 5*(10). doi:http://dx.doi.org/10.1016/j.avb.2012.09.003

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Colling, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 62-70.

WHO. (2020). *Global status report on preventing violence against children.* Geneva: WHO.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72–79.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 72-79.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, 347–356.