OS

Trgovina ljudima posredstvom interneta i tehnologije

Detaljan izvještaj

GRETA
Grupa eksperata
za borbu protiv
trgovine ljudima

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Trgovina ljudima posredstvom interneta i tehnologije

Detaljan izvještaj

Izvještaj pripremio
dr. Paolo Campana
vanredni profesor, Univerzitet u Cambridgeu
Ujedinjeno Kraljevstvo

april 2022.

Vijeće Evrope

Izdanje na francuskom jeziku:
La traite des êtres humains en ligne et facilitée par les technologies

Sva ostala prepiska koja se odnosi na ovaj dokument treba biti upućena Sekretarijatu Konvencije Vijeća Evrope o akciji protiv trgovine ljudima trafficking@coe.int

Sve fotografije: Shutterstock

Urednička jedinica SPDP nije lektorisala ovu publikaciju radi ispravljanja tipografskih i gramatičkih grešaka.

Štampano u Vijeću Evrope

Sadržaj

Skraćenice korištene u tekstu

AI:	Vještačka inteligencija
ASW:	Web-lokacija za usluge za odrasle
VE:	Vijeće Evrope
CID:	Odjeljenje za krivične istrage
CSE:	Seksualna eksploatacija djece
CV:	Radna biografija
EAW:	Evropski nalog za hapšenje
EIO:	Evropski nalog za istragu
EJN:	Evropska pravosudna mreža
EU:	Evropska unija
BDP:	Bruto domaći proizvod
GDPR:	Opća uredba o zaštiti ličnih podataka
GRETA:	Grupa eksperata Vijeća Evrope za borbu protiv trgovine ljudima
HDD:	Čvrsti disk
ZIT:	Zajednički istražni tim
IKT:	Informacijsko-komunikacijske tehnologije
ISP:	Pružalac internet usluga
UPP:	Uzajamna pravna pomoć
NVO:	Nevladina organizacija
OSINT:	Obavještajni podaci iz otvorenih izvora
THB:	Trgovina ljudima
TOR:	Onion Ruter
VOIP:	Protokol za prijenos glasa putem interneta

Uvod

Internet, i općenito informacijsko-komunikacijske tehnologije (IKT), igraju važnu ulogu u oblikovanju naših života. Pandemija COVID-19 jasno je pokazala u kojoj mjeri su internet i IKT postali neizostavan dio različitih aktivnosti i društvenih interakcija – i ubrzala je njihov značaj. Svijet kriminala nije izuzetak u tome – a to uključuje i trgovinu ljudima.

Nema sumnje da tehnologija donosi izazove – kao i mogućnosti – i za organe za provođenje zakona i za nevladine organizacije (NVO). Istovremeno, baza dokaza o trgovini ljudima posredstvom interneta i tehnologije i dalje je ograničena i nepovezana. U ovom trenutku, najbolji dostupni dokazi potječu iz relativno malog broja studija, koje se obično zasnivaju na malom broju ispitanika među policijskim službenicima i predstavnicima nevladinih organizacija – najčešće provedenim u veoma ograničenom broju država – kao i na malobrojnim izvještajima međunarodnih organizacija. Ova studija prevazilazi granice anegdotalnih dokaza time što nudi analizu trgovine ljudima posredstvom interneta i tehnologije na osnovu dokaza koji su sistematski prikupljani od država ugovornica – potpisnica Konvencije Vijeća Evrope (VE) o borbi protiv trgovine ljudima. Takvi dokazi su dopunjeni informacijama prikupljenim od nevladinih organizacija koje pružaju pomoć žrtvama trgovine ljudima, kao i od tehnoloških kompanija.

Oblast primjene ove studije je relativno široka. Ona nudi procjenu razmjere u kojoj tehnologija utječe na trgovinu ljudima, kao i istraživanje modusa operandija trgovaca ljudima u kontekstu trgovine ljudima posredstvom interneta i tehnologije. U osnovi ove studije leži istraživanje operativnih i pravnih izazova s kojima se suočavaju države ugovornice – i u određenoj mjeri NVO – prilikom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom interneta i IKT-a, kao i prilikom identifikacije žrtava i podizanja nivoa svijesti među ugroženim grupama. Ključno je to da studija također istražuje strategije, alate i „dobre prakse" koje su usvojile države ugovornice i NVO u cilju prevazilaženja takvih izazova i unapređenja odgovora na trgovinu ljudima posredstvom interneta i tehnologije. Ovaj dokument otkriva sličnosti između država, kao i iskustva specifična za određene države. Poseban akcent je stavljen na obuke – kao ulaganja u ljudski kapital, one su jednako važne kao ulaganja u tehničke alate.

Ova studija je provedena kao dio višegodišnjeg interesovanja Vijeća Evrope za pitanje tehnologije i trgovine ljudima. Pored toga što nudi sistematsku procjenu trenutno dostupne baze dokaza, ova studija također ima za cilj pružiti Grupi eksperata Vijeća Evrope za borbu protiv trgovine ljudima (GRETA) i drugim subjektima alat za provođenje budućih procjena i praćenje promjena u oblasti tehnologije i ponašanja.

Metodologija

Dokazi izneseni u ovoj studiji prikupljeni su pomoću novog upitnika koji je sadržavao pitanja otvorenog i zatvorenog tipa. Upitnik je pripremljen u tri verzije (priložene u Prilozima): duža verzija za države ugovornice (40 pitanja) i dvije kraće verzije za NVO (14 pitanja) i tehnološke kompanije (11 pitanja). Dizajn upitnika zasniva se na analizi okruženja koja je provedena između oktobra i decembra 2020. godine i obuhvata različite izvore: međunarodne organizacije, akademsku zajednicu, NVO, kao i privatni sektor (vidjeti Aneks A za više detalja). Upitnik je pripremljen u saradnji s članicama GRETA-e i Sekretarijatom Vijeća Evrope u periodu od januara do marta 2021. godine. Prikupljeni su odgovori od 40 država ugovornica,[1] 12 NVO[2] i 2 tehnološke kompanije[3] tokom juna i jula 2021. godine (jedan zakašnjeli odgovor stigao je do Sekretarijata Vijeća Evrope u septembru 2021. godine). Analize su rađene u periodu između juna i septembra 2021. godine. To je relativno kratak rok za studiju koja je obuhvatala prilično širok spektar problema, država i subjekata. Iako ova studija pruža detaljnu procjenu velike količine dokaza, ona ni u kom slučaju nije sveobuhvatna niti bez ograničenja. O tome će biti više riječi u nastavku teksta, kada to bude relevantno.

Ova studija primjenjuje definiciju Latonera (2012: 9–10) da tehnologija predstavlja „informacijske i komunikacijske tehnologije, naročito one koje čine digitalna i umrežena okruženja. Tehnologije koje omogućavaju korisnicima da razmjenjuju digitalne informacije putem mreža uključuju internet, online društvene mreže i mobilne telefone."

Tehnologija će opstati – a s njom i strukturne promjene u načinu rada počinilaca krivičnih djela, otvaranje mogućnosti i pogoršanje postojećih ranjivosti. Stoga postoji potreba da države ugovornice usvoje i opreme svoje agencije za provođenje zakona i sisteme krivičnog pravosuđa mogućnostima za praćenje ovog okruženja koje se (neprekidno) mijenja. Ova studija u tom smislu pruža preporuke zasnovane na dokazima.

[1] Albanija; Armenija; Austrija; Azerbejdžan; Bosna i Hercegovina; Bjelorusija; Belgija; Bugarska; Hrvatska; Kipar; Danska; Estonija; Finska; Francuska; Njemačka; Grčka; Mađarska; Island; Irska; Latvija; Litvanija; Luksemburg; Malta; Republika Moldavija; Monako; Crna Gora; Holandija; Sjeverna Makedonija; Norveška; Poljska; Portugal; Rumunija; San Marino; Slovačka; Slovenija; Španija; Švedska; Švicarska; Ukrajina i Ujedinjeno Kraljevstvo.

[2] Astra (Srbija); Different and Equal (Albanija); FIZ (Švicarska); Hope Now (Danska); Jesuit Refugee Service (Sjeverna Makedonija); KOK (Njemačka); La Strada (Republika Moldavija); La Strada International (širom Evrope); Migrant Rights Centre (Irska); Praksis (Grčka); Schweizer Plattform gegen Menschenhandel (Švicarska); Sustainable Rescue Foundation (Holandija).

[3] Facebook i IBM.

Rezime izvještaja

Utjecaj tehnologije na trgovinu ljudima

Utjecaj tehnologije na trgovinu ljudima naročito je važan u dvije faze procesa trgovine: tokom **regrutiranja** i **eksploatacije**. Dokazi koje su dostavile države ugovornice ukazuju na sve „veći" značaj tehnologije u kontekstu trgovine ljudima, pri čemu većina država ugovornica sada smatra da je utjecaj tehnologije na trgovinu ljudima „veoma važan" ili „važan".

Države ugovornice ukazuju na sve veći značaj online materijala, reklama/oglasa i stranica/aplikacija za traženje posla, kao i na sve veći značaj online socijalizacije i ličnih interakcija. S druge strane, oba ova segmenta stvaraju prilike za počinioce u oblasti trgovine ljudima i pogoršavaju postojeće ranjivosti. Tehnologija je promijenila način interakcije među ljudima što se odražava i na svijet kriminala, uključujući i trgovinu ljudima. Ovo je strukturna promjena kojoj se organi za provođenje zakona i sistemi krivičnog pravosuđa moraju prilagoditi.

Tehnologija može igrati ulogu u fazi **regrutiranja** time što olakšava identifikaciju, lociranje i uspostavljanje kontakta s potencijalnim žrtvama. U zavisnosti od tipa eksploatacije, koriste se različiti mehanizmi.

U kontekstu regrutiranja u svrhu **seksualne eksploatacije**, nekoliko država ugovornica je otkrilo slučajeve oglasa za posao koji su bili povezani s trgovinom ljudima i dokaze regrutiranja

preko platformi društvenih medija, kao i aplikacija za upoznavanje. Uobičajena strategija je takozvana **tehnika „ljubavnika"**: vrsta regrutiranja putem interneta gdje trgovac ljudima identificira i stupa u kontakt s potencijalnom žrtvom preko online platforme, upoznaje njene hobije i interesovanja, kao i ličnu i porodičnu situaciju. Trgovac ljudima potom pruža empatiju i podršku potencijalnoj žrtvi u kontekstu romantičnog odnosa – želi uspostaviti povjerenje, a time i kontrolu nad žrtvom.

Dostupno je obilje dokaza iz više zemalja o slučajevima **ucjene** žrtava. Ovo se najčešće postiže time što se prvo prikupe „kompromitirajuće" informacije o žrtvama – naprimjer, time što se traže fotografije ili videosnimci nagog tijela – i potom te informacije koriste da se osoba prisili na prostituciju.

Tokom **faze eksploatacije**, tehnologija može omogućiti **prodaju** seksualnih usluga koje pružaju žrtve trgovine ljudima. Dostupno je obilje dokaza iz više zemalja o web-stranicama koje se koriste za reklamiranje seksualnih usluga. Među takvim reklamama nalaze se i usluge koje pružaju žrtve trgovine ljudima. Štaviše, iako se emitiranje uživo najčešće povezuje sa seksualnim zlostavljanjem djece, više država je ukazalo na činjenicu da emitiranje uživo može također uključivati i odrasle žrtve trgovine ljudima.

Osim toga, tehnologija se može koristiti za **koordinaciju aktivnosti**. Ključno je to da tehnologija omogućava **razdvajanje** između mjesta gdje se seksualna aktivnost izvodi i mjesta gdje se vrši koordinacija. Ovo ima važne implikacije u pogledu provođenja zakona.

Države su pružile dokaze o tehnološkim alatima koje trgovci ljudima koriste za **praćenje i kontrolu** žrtava tokom faze eksploatacije. Ucjene i kompromitirajuće informacije se također koriste protiv žrtava kao sredstvo kontrole tokom ove faze.

Brojne države prijavljuju pojavu trendova u kontekstu seksualne eksploatacije koji uključuju sve češću upotrebu „web-kamera za prijenos uživo" i aplikacija za videopozive „plati koliko koristiš", kao i sve veću upotrebu aplikacija za kontrolu žrtava. Takve web-kamere i aplikacije za videopozive mogu se koristiti za emitiranje seksualnih radnji koje izvode žrtve trgovine ljudima uživo. Nekoliko država je navelo da je pandemija COVID-19 povećala mogućnosti za trgovce ljudima za uspostavljanje kontakta putem interneta s ranjivim pojedincima.

U kontekstu trgovine ljudima u svrhu **radne eksploatacije**, dokazi koje su pružile države ugovornice ukazuju da se IKT prvenstveno koriste za **regrutiranje** žrtava, naročito posredstvom **oglasa za posao na internetu**. Takvi oglasi se ne objavljuju samo na stranicama rezerviranim za traženje posla, već i na društvenim medijima u specijaliziranim grupama za traženje posla i u grupama za uzajamnu pomoć. Nekoliko država je naglasilo značaj web-stranica koje imaju za cilj omogućavanje razmjene informacija među radnicima migrantima koje trgovci ljudima koriste kao prostor za regrutiranje.

Trend u nastajanju u kontekstu radne eksploatacije, koji su prijavile neke države, uključuje povećanje broja slučajeva regrutiranja putem interneta i društvenih mreža. Vjeruje se da je ovom trendu doprinijela pandemija COVID-19. Iako se čini da tehnologija ne igra značajnu ulogu u fazi eksploatacije, države su prijavile povećanje mogućnosti za eksploataciju žrtava trgovine ljudima koje donosi ekonomija honorarnih poslova („gig ekonomija"), naročito platforme za isporuku.

Nema dokaza relevantne uloge koju **mračna mreža** igra u kontekstu trgovine odraslim ljudima (cirkulacija materijala za seksualnu eksploataciju djece nije obuhvaćena oblašću

primjene ove studije). Slično tome, čini se da korištenje **kriptovaluta** nije rasprostranjeno u kontekstu trgovine ljudima (s druge strane, kriptovalute se koriste za kupovinu pristupa prijenosu seksualnog zlostavljanja djece uživo).

Dokazi koje su pružile **NVO** prikazuju sličnu situaciju. Nevladine organizacije su primijetile korištenje interneta i društvenih medija tokom svih faza trgovine ljudima, naročito u vezi s (a) regrutiranjem; (b) eksploatacijom; i (c) vršenjem kontrole i pritiska nad žrtvama. Pored toga, trgovci ljudima koriste IKT, uključujući društvene medije i šifrirane aplikacije, kako bi nastavili da održavaju kontakt sa žrtvama trgovine ljudima nakon što napuste situaciju u kojoj se vrši eksploatacija, često kako bi ih spriječili da podnesu prijave i zatraže pravdu.

Novi trendovi primijećeni u dokazima koje su pružile NVO ukazuju na povećanje eksploatacije djece putem **web-kamera i društvenih medija**. Navodi se i to da su počinioci počeli koristiti **online igrice** kako bi stupili u kontakt s potencijalnim žrtvama.

Konačno, dostupni dokazi ukazuju na to da upotreba tehnologije dopunjava, a ne zamjenjuje lične interakcije van mreže. Tehnologiju i interakcije licem u lice najbolje je posmatrati kao integrirane.

Izazovi tokom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom tehnologije

Izazovi tokom otkrivanja

Otkrivanje slučajeva trgovine ljudima posredstvom interneta i tehnologije i identifikacija žrtava i dalje predstavljaju velike izazove. Države ugovornice ukazuju na brojne izazove:

- Neprekidno rastući broj online aktivnosti/interakcija. Nadziranje interneta zahtijeva ogromne resurse i podliježe pravnim ograničenjima (uključujući primjenu zakona o privatnosti i ograničenja korištenja sistema za skeniranje mreže radi prikupljanja podataka u nekim državama);
- Broj online oglasa (otvorenih i malih oglasa) za seksualne i neseksualne usluge često je prevelik za ručno pretraživanje;
- Poteškoće prilikom identifikacije počinilaca i žrtava, jer mogu koristiti nadimke i pseudonime tokom svojih online aktivnosti i mogu koristiti softver za anonimizaciju (npr. VPN);
- Korištenje šifrirane komunikacije između trgovaca i žrtava. Konverzacija između trgovaca ljudima i žrtava odvija se u zatvorenim grupama;
- Ponašanje korisnika interneta koje se brzo mijenja;
- Izazovi prilikom sortiranja online oglasa kako bi se identificirali oni koji se odnose na trgovinu ljudima u kontekstu seksualnih i neseksualnih usluga. Znaci upozorenja na oglase povezane sa seksualnom i radnom eksploatacijom i dalje su nedovoljno razvijeni i nedovoljno se koriste;
- Nepostojanje specijaliziranih jedinica pri policiji i/ili odsustvo specijaliziranih istražitelja za slučajeve trgovine ljudima s naprednim vještinama korištenja računara. Nedostatak službenika koji su obučeni za izvođenje tajnih operacija na internetu. Cyber operacije mogu dugo trajati i oduzimati puno vremena;
- Proces slanja zahtjeva kompanijama koje upravljaju društvenim medijima koji oduzima mnogo vremena i odsustvo reakcije nekih od takvih kompanija;
- Kratki periodi čuvanja IP adresa i poteškoće oko pristupanja takvim podacima.

Izazovi tokom istraga

Šifriranje podataka predstavlja najozbiljniji izazov s kojim se suočavaju države ugovornice (nivo ozbiljnosti 80 od 100). Nakon toga slijede velika količina podataka (71), brzina tehnoloških promjena (66), nedovoljna tehnička oprema (63), neodgovarajući zakonodavni alati (61), odsustvo tehničkih znanja među organima za provođenje zakona (53) i odsustvo pomoći privatnog sektora (46).

Protokoli za šifriranje podataka koji se nalaze u popularnim aplikacijama i online servisima smatraju se problematičnim. Šifriranje također ograničava mogućnost praćenja komunikacije. Nekoliko država je nagovijestilo postojanje alata za dešifriranje nekih vrsta uređaja. Međutim, ovo je okruženje koje se neprekidno razvija i zahtijeva (velika) ulaganja u obuke i softver. Koraci preduzeti za prevazilaženje ovog problema uključuju uspostavljanje jedinica/centara za borbu protiv cyber kriminala čiji je zadatak rad s tehnologijom za dešifriranje. Osim toga, veoma je značajno udruživanje resursa na nadnacionalnom nivou za potrebe razvoja tehnoloških proizvoda, kao što su softveri za dešifriranje i skeniranje mreže radi prikupljanja podataka.

Elektronske komunikacije i IKT uređaji generiraju **velike količine podataka koje neprekidno rastu**, a koje predstavljaju ogroman napor za istražitelje. Ovaj napor utječe na sposobnost istražitelja da izdvoje i pažljivo analiziraju podatke, što samo po sebi zahtijeva specijalizirani softver, kao i posebne obuke o sistematizaciji i pretraživanju tako velikih količina dokaza.

Postoji opća saglasnost da je razvoj kapaciteta za rukovanje velikim količinama **elektronskih dokaza** od ključnog značaja. Međutim, takvi kapaciteti se moraju neprekidno modernizirati. Države su navele da izazovi s kojima se suočavaju ne leže samo u sve većoj količini podataka koje generiraju online platforme i društveni mediji, već i u promjenjivim **obrascima ponašanja** njihovih korisnika.

Nedostatak tehničke opreme prepoznat je kao izazov u nekoliko država. Specijalizirani softver i hardver često je veoma skup i zahtijeva konstantna ažuriranja i skupe ugovore o licenciranju kako bi se pratio korak s brzinom tehnoloških promjena. **Potreba da se prati korak s tehnološkim promjenama** može imati značajan utjecaj na budžet policije. Ovaj problem je prijavilo nekoliko država, bez obzira na njihov nivo BDP-a (bruto domaćeg proizvoda).

Ulaganja u ljudski kapital su jednako važna kao i ulaganja u softver i hardver, ako ne i važnija, posebno kada se odnose na **odsustvo razvoja i potrebu za razvojem tehničkih znanja među organima za provođenje zakona**. Dokazi ukazuju na potrebu za razvojem znanja o (a) pojavi novih trendova i promjenama u upotrebi tehnologije; (b) pojavi novih aplikacija i usluga na tehnološkom tržištu koje karakteriziraju brze promjene, i (c) razvoju novih sigurnosnih protokola i metoda šifriranja. Najvažnije je to da znanje treba mudro rasporediti unutar organizacije. Naprimjer, nedostatak specijaliziranih službenika na lokalnom nivou može stvoriti **uska grla u istragama**, ako je potrebno više puta tražiti pomoć od (preopterećene) centralizirane jedinice.

Nekoliko zemalja je istaklo potrebu za **organiziranjem dodatne tehničke obuke za sve policijske službenike**, uključujući za sticanje znanja o tehnologiji i načinima kako ona funkcionira. Slično tome, odgovarajuća obuka o pribavljanju i rukovanju **elektronskim**

dokazima treba se osigurati za najveći broj relevantnih službenika i treba biti redovna tema u nastavnim planovima i programima obuka za policijske službenike. U složenijim slučajevima može biti potrebno formirati timove s multidisciplinarnim vještinama (npr. okupiti istražitelje, finansijske stručnjake i stručnjake za cyber kriminal).

Dalji izazovi uključuju pitanja koja proizlaze iz neodgovarajućih **obaveza čuvanja podataka** nametnutih pružaocima internet usluga (ISP) i iz primjene zakona o privatnosti, naprimjer u vezi sa sistemima za skeniranje mreže radi prikupljanja podataka.

Izazovi tokom krivičnog gonjenja

Sve u svemu, izazovi s kojima se sreće tužilaštvo imaju nižu ocjenu od izazova tokom istraga, pri čemu je samo za „pribavljanje dokaza iz drugih zemalja" ocjena nešto viša od 50 (od 100). Ovo je praćeno nedostatkom obuke među tužiocima (40); neodgovarajućim zakonodavnim alatima (38) i nedostatkom pomoći privatnog sektora (33). Čini se da ekstradicija osumnjičenih (28) i određivanje nadležnosti (16) igraju marginalnu ulogu.

Adekvatna **obuka tužilaca** smatra se ključnom za obezbjeđivanje da predmeti koji se razvijaju uz pomoć IKT-a budu robusni, da se elektronski dokazi pravilno prikupljaju i koriste, i da se predmeti na odgovarajući način iznose pred sudijom/porotom. Neke države ugovornice primijetile su slučajeve u kojima tužioci nisu bili upoznati s procedurama za traženje elektronskih podataka od privatnih kompanija ili s procedurama za pribavljanje dokaza i saradnje iz drugih zemalja (npr. putem zajedničkog istražnog tima – ZIT ili evropskog naloga za istragu – EIO).

Neke države ugovornice pokrenule su pitanje postupanja s elektronskim materijalom, naročito u kontekstu **obaveza po osnovu GDPR-a** (Opće uredbe EU o zaštiti ličnih podataka). Također je izražena zabrinutost oko međunarodnih propisa o zaštiti podataka koji mogu ometati prikupljanje, čuvanje i obradu informacija dobijenih primjenom tehnoloških istražnih tehnika (kao što je skeniranje mreže radi prikupljanja podataka (engl. *web crawling*)).

Primijećeni su izazovi koji se tiču IP adresa i elektronskih dokaza. IP adrese trebaju biti povezane s korisničkim imenima i korisnicima kad god je to moguće. Međutim, korisnička imena se mogu promijeniti u bilo kojem trenutku i osumnjičeni ih često koriste naizmjenično.

Još jedan izazov odnosi se na **iznošenje dokaza** pred porotom (i sudijom), jer tehnički dokazi u slučajevima koji se razvijaju uz pomoć IKT-a mogu biti složeni i često je potreban stručnjak da ih izvede. Razvijanje interne stručnosti među službenicima o tome kako efikasno i tačno izvesti elektronske dokaze sve više dobija na značaju.

Izazovi međunarodne saradnje

Velika većina država ugovornica naznačila je dugo vrijeme potrebno za obradu **zahtjeva za uzajamnu pravnu pomoć** (UPP) kao jednu od glavnih prepreka međunarodnoj saradnji. Procedure uzajamne pravne pomoći smatraju se sporim, ponekad nepredvidivim, a potrebni su im i međunarodno dogovoreni šabloni. Ovo pitanje je naročito otežano kada se saradnja odvija izvan pravnog okvira EU.

Saradnja van pravnog okvira EU posmatra se kao proces koji oduzima puno vremena i koji karakterizira veća zamršenost zbog nedostatka usaglašenosti između različitih pravnih sistema, uz elemente nepredvidivosti i nedosljednosti. Jasnije operativne procedure, poboljšana redovna razmjena između kontaktnih tačaka, jasno utvrđivanje zahtjeva za međunarodnu pravnu pomoć i diskusija na samom početku doprinijeli bi usaglašavanju procesa.

Tehnologija omogućava kriminalnim mrežama da organiziraju i kontroliraju aktivnosti eksploatacije na daljinu – naprimjer, iz druge zemlje – često uz svijest da zahtjevi za pravosudnu saradnju neće biti pravovremeno realizirani, ako uopće budu. Ovo stvara potrebu za unapređenjem ili u nekim slučajevima uspostavljanjem sporazuma s državama porijekla žrtava ako se nalaze izvan EU.

Izazovi u obradi zahtjeva za UPP također mogu biti rezultat **nedostatka adekvatno obučenog osoblja** za formuliranje i upravljanje zahtjevima, kao i korištenja zastarjele tehnologije.

Elektronski dokazi mogu otežati identifikaciju tačne lokacije podataka i države u čijoj nadležnosti se ti podaci nalaze, što otežava formuliranje zahtjeva za uzajamnu pravnu pomoć.

Upućeni su pozivi za uspostavljanje zajedničkog pravnog okvira za **brzu razmjenu digitalnih dokaza**. Nekoliko država je izrazilo zabrinutost zbog nepostojanja homogene regulative o **čuvanju podataka**, što ometa razmjenu elektronskih dokaza. Sve u svemu, države ugovornice su izrazile potrebu za sveobuhvatnijim okvirom koji uređuje čuvanje i prijenos elektronskih dokaza i za zajedničkim pravnim okvirom koji bi zamijenio trenutne *ad hoc* bilateralne radne sporazume između država i privatnih kompanija koje drže podatke (vidjeti u nastavku). Države ugovornice su također istakle potrebu da se unaprijedi razmjena podataka tokom istraga.

Izazovi tokom saradnje s privatnim kompanijama

Nekoliko država je navelo da su ISP (pružaoci internet usluga), pružaoci sadržaja i kompanije koje nude društvene medije generalno sarađivali u pogledu pitanja vezanih za trgovinu ljudima i seksualnu eksploataciju djece. Ipak, identificirani su brojni izazovi. Oni uključuju:

- **Dobijanje pravovremenog odgovora** od nekih pružalaca internet usluga i pružalaca sadržaja. Obraćanje hostovima putem zamolnica poslatih preko relevantnih institucija može dovesti do dugog čekanja uz rizik da sadržaj bude izbrisan do trenutka kada se postupi po zahtjevu;
- **Pojašnjavanje pravnih zahtjeva** u skladu s kojima IKT kompanije i pružaoci internet usluga funkcioniraju. Neke države su izrazile zabrinutost da neki ISP nameću formalističke i „pravno neopravdane" zahtjeve agencijama za provođenje zakona i ne obrazlažu i ne objašnjavaju odbijanja na odgovarajući način;
- **Nedostatak određene kontakt-tačke** u privatnim kompanijama. Velike kompanije koje posluju u više država često nemaju osoblje koje posjeduje jezičke i pravne vještine relevantne za svaku državu u kojoj posluju;
- **Nedostatak znanja** među pružaocima sadržaja i kompanijama koje pružaju društvene medije o tome koja je nacionalna agencija odgovorna za koje odluke, npr. uklanjanje nezakonitog sadržaja. Bilo je prijedloga da se uvede uloga „pouzdanog čuvara sadržaja",

odnosno da se odrede određene agencije koje bi imale zadatak da se povežu s međunarodnim pružaocima usluga radi uklanjanja sadržaja. Pouzdani čuvar sadržaja bi imao otvoren kanal komunikacije s kompanijama i izgradio bi uzajamno povjerenje.

Dokazi prikupljeni od nevladinih organizacija

Općenito govoreći, dokazi prikupljeni od nevladinih organizacija ukazuju na slične probleme koji se razmatraju iznad. Konkretnije, NVO su istakle sljedeće probleme:

- **Nedostatak kapaciteta** organa za provođenje zakona, što uključuje nedostatak obuke, hardvera i softvera i ograničenu upotrebu posebnih istražnih tehnika. Također postoji nedostatak specijalizacije među nekim policijskim snagama i pravosuđem u vezi s trgovinom ljudima posredstvom tehnologije;
- **Tehnološko okruženje koje se brzo mijenja i *modus operandi* počinilaca**. Profesionalcima je teško pratiti korak s trgovinom ljudima posredstvom tehnologije, što ometa njihovu sposobnost da brzo identificiraju slučajeve. Znanje o tehničkom okruženju i praksama (*modus operandi*) često se ne razmjenjuje;
- Korištenje privatnih foruma, chat soba ili šifriranih aplikacija za kontakte između počinilaca i žrtava. Ovo otežava (a) otkrivanje takvih kontakata i (b) njihovo pribavljanje kao dokaza koji će se koristiti na sudu. NVO su predložile navođenje informacija/upozorenja o sigurnom korištenju privatnih kanala komunikacije u chat sobama i aplikacijama;
- **Pravila o zaštiti podataka i privatnosti** mogu ometati identifikaciju žrtava, kao i trgovaca ljudima. Pravila propisana GDPR-om ograničavaju upotrebu tehnologije za otkrivanje digitalnih tragova koje ostavljaju i žrtve i počinioci;
- **Nedostatak interdisciplinarne tehnološke saradnje** između privatnih kompanija, javnih agencija i nevladinih organizacija kako bi se u potpunosti iskoristila sve veća količina podataka o trgovini ljudima;
- **Nedostatak tehnološke strategije** u nacionalnim akcionim planovima za borbu protiv trgovine ljudima;
- **Nedostatak kapaciteta, resursa i tehničkih alata** nevladinih organizacija za redovno otkrivanje online eksploatacije posredstvom tehnologije;
- **Suprotstavljeni ciljevi** ili različiti pristupi nevladinih organizacija i organa za provođenje zakona.

Dokazi prikupljeni od tehnoloških kompanija

Kao što je navedeno iznad, samo dvije kompanije su dostavile odgovore na upitnik. Kompanija Facebook je primijetila da korisnici „rijetko prijavljuju" sadržaje koji se odnose na trgovinu ljudima. Kompanija IBM je primijetila nekoliko prepreka za saradnju s organima za provođenje zakona, uključujući zabrinutost u vezi sa zakonitošću takve saradnje, posebno u vezi s privatnošću podataka i pravnom složenošću situacije koja uključuje nadležnost više država. IBM je također zatražio pojašnjenja o međunarodnim pravnim dozvolama za prikupljanje i dijeljenje podataka s organima za provođenje zakona.

Strategije i dobre prakse

Otkrivanje slučajeva trgovine ljudima posredstvom IKT-a

Države su navele da primjenjuju različite strategije za otkrivanje slučajeva trgovine ljudima posredstvom interneta i IKT-a. Često se navodi strategija **nadgledanja interneta**, uključujući foruma i, u nekim slučajevima, TOR mreže (mračne mreže). Ovo je u kombinaciji s upotrebom **obavještajnih podataka iz otvorenih izvora (OSINT)**, što znači prikupljanje podataka s društvenih medija i iz drugih javno dostupnih online izvora o mreži kontakata određene osobe, njenim životnim uvjetima i finansijskoj situaciji.

Neke države su formirale **„cyber patrole" sa specijaliziranim službenicima** zaduženim za provođenje OSINT istraga na internetu. Neke države dozvoljavaju tajne istrage na internetu (cyber infiltracija).

Neke agencije za provođenje zakona koriste **alate za „struganje" interneta** posebno razvijene za izdvajanje informacija s web-lokacija, naročito za identifikaciju rizika i ranjivosti na web-lokacijama za usluge za odrasle (ASW).

Vezano za OSINT istrage, koriste se **tehnike analize društvenih mreža** kako bi se razumjele i rekonstruirale mreže kontakata počinioca i/ili žrtve. **Relacione informacije** su ključne: informacije prikupljene iz različitih izvora mogu se sistematizirati i koristiti **za rekonstrukciju kriminalnih mreža**, odnosno odnosa između mjesta, počinilaca i žrtava.

Međutim, nisu sve države ugovornice navele da koriste „proaktivne" strategije. Nekoliko država ugovornica je navelo da njihove istrage o trgovini ljudima posredstvom IKT-a ostaju „reaktivne".

Nekoliko država je implementiralo **sisteme pomoću kojih korisnici interneta mogu prijaviti sadržaje i web-lokacije** za koje sumnjaju da su povezane s nezakonitim aktivnostima, uključujući seksualnu i radnu eksploataciju.

U nekim državama, naprimjer, u Francuskoj, pružaoci internet usluga i web-lokacija dužni su pomoći organima za provođenje zakona u borbi protiv širenja materijala koji se odnose na određena krivična djela, uključujući trgovinu ljudima. Od njih se zahtijeva da uspostave lako dostupan i vidljiv sistem koji omogućava svakom pojedincu da označi sumnjivi materijal.

Neke države su prijavile organiziranje **kampanja za podizanje svijesti** za povećanje otkrivanja slučajeva trgovine ljudima posredstvom IKT-a. To uključuje kampanje za podizanje svijesti usmjerene ka klijentima koji koriste web-lokacije na kojima se nalaze oglasi za seksualne usluge kako bi ih informirali o riziku od slučajeva trgovine ljudima (Belgija i Ujedinjeno Kraljevstvo) i kampanje koje pružaju informacije o tome kako pronaći sigurne prilike za zapošljavanje (Poljska i Bugarska). Nadležni organi nekih država koristili su društvene medije za širenje ciljanih informacija, ponekad uz kreiranje ciljanih Facebook reklama povezanih s linijom za dojavu.

Istraga slučajeva trgovine ljudima posredstvom IKT-a

U nekim državama, agencije za provođenje zakona provode **cyber infiltraciju** u kriminalne mreže koristeći prikrivene tehnike, kao i tajne istrage. Nekoliko država je izrazilo potrebu za povećanjem broja takvih **tajnih istraga**, zbog čega ulažu u obuku specijaliziranih službenika. Postoji opća saglasnost o značaju nabavke i pristupanju **specijaliziranom softveru**, kao i o značaju velikih količina podataka i poboljšanja mogućnosti u pogledu velikih količina podataka. Također je ključan razvoj alata za preuzimanje informacija s mobilnih telefona bez otkrivanja šifre i za dešifriranje razgovora preko aplikacija za komunikaciju.

Smatra se da je **ulaganje u ljudski kapital** jednako ključno kao i ulaganje u tehnološku opremu. Ulaganje u ljudski kapital može podrazumijevati da se službenicima za provođenje zakona osiguraju kontinuirane obuke i aktivnosti razvoja zasnovane na najboljim lokalnim i globalnim praksama. Isto tako, nekoliko država je ukazalo na značaj uključivanja specijaliziranih istražnih službenika s „digitalnim znanjem" u istrage slučajeva trgovine ljudima. Jedan model bi podrazumijevao prisustvo osoblja posebno obučenog za provođenje istraga na internetu i društvenim mrežama koje je integrirano u svaku jedinicu specijaliziranu za borbu protiv trgovine ljudima. Time bi se formirale **grupe za tehničku podršku** istražiteljima. U takvim grupama mogu biti policijski službenici s policijskim ovlaštenjima ili ostali policijski službenici. Ova ideja se **udaljava od tradicionalnog policijskog modela** zasnovanog na policajcima pod zakletvom i usvaja principe – koje već primjenjuju neke policijske uprave – da službenici koji nisu pod zakletvom imaju više tehničku ulogu (npr. analitičari).

Osim toga, države ugovornice su istakle značaj **međuagencijskog istražnog rada** uz učešće i saradnju širokog spektra specijaliziranih agencija – kao i značaj razmjene znanja među institucijama. Slično tome, države su ukazale na značaj **unapređenja prekogranične saradnje** kroz, naprimjer, međusobnu razmjenu službenika s državama porijekla žrtava. Na operativnom nivou, države su napomenule da bi istraga mogla biti olakšana **lakšim čuvanjem dokaza na međunarodnom nivou i pristupom takvim dokazima**.

Prilikom provođenja istraga, sugerirano je da se države ne bi trebale previše oslanjati na **preskriptivnu listu indikatora**, npr. da identificiraju visokorizične reklame/oglase na internetu, već da se također oslanjaju na slojevitost informacija različite prirode, uključujući obavještajne podatke, informacije iz otvorenih izvora i policijskih evidencija. Naglašen je

značaj analize mreže i relacionih podataka.

Iako oduzima puno vremena, **strateška analiza** koja generira znanje o novim trendovima i ažurirane informacije o modusu operandiju počinilaca (uključujući tehnologiju i web-lokacije koje koriste počinioci) smatra se veoma značajnom.

Tehnologija se također može koristiti za **olakšavanje prikupljanja dokaza od žrtava** i tokom istrage i krivičnog gonjenja predmeta trgovine ljudima, kao i za smanjenje opterećenja za žrtve.

Podsticanje međunarodne saradnje

Države ugovornice su prepoznale sljedeće dobre principe za podsticanje međunarodne saradnje:

- Korištenje resursa dostupnih u agencijama kao što su Europol i Eurojust, i uspostavljanje zajedničkih istražnih timova (ZIT) za one države koje su dio pravosudnog okvira EU;
- Uspostavljanje kontakata s drugim zainteresiranim stranama u ranoj fazi istrage;
- Razvijanje veoma dobrog razumijevanja pravnog konteksta i mogućnosti saradnje s drugim državama;
- Organiziranje koordinacionih sastanaka radi razmjene informacija i dokaza što je brže moguće i kako bi se utvrdila zajednička strategija od samog početka;
- Razvijanje zajedničkog razumijevanja standardiziranih pristupa i osiguravanje transnacionalne interoperabilnosti agencija za provođenje zakona kroz transnacionalne obuke.

Saradnja među nepolicijskim organima, koja se često zanemaruje, može biti jednako relevantna kao i saradnja s policijskim organima, naročito u kontekstu trgovine ljudima u svrhu radne eksploatacije (npr. između inspektorata rada).

Identifikacija žrtava i pomoć

Čini se da se **prepoznavanje lica** često koristi u slučajevima seksualne eksploatacije djece (CSE). Međutim, čini se i da je upotreba ove tehnike ograničenija izvan konteksta seksualne eksploatacije djece. Nekoliko država je ukazalo na upotrebu tehnoloških alata za identifikaciju žrtava trgovine ljudima koji koriste velike količine podataka (uglavnom sistema za skeniranje mreže radi prikupljanja podataka, ali i alata za prepoznavanje lica pod strožim uvjetima).

Nekoliko država se oslanja na indikatore za identifikaciju slučajeva trgovine ljudima („**znake upozorenja**"); međutim, ovo su „opći" indikatori trgovine ljudima i nisu specifični za trgovinu ljudima posredstvom IKT-a. Iako postoji jasna potreba da se razviju indikatori specifični za trgovinu ljudima posredstvom IKT-a, nadležni organi su također upozorili da se ne treba previše oslanjati na „znake upozorenja". Čak i u slučajevima u kojima su indikatori konkretno razvijeni za identifikaciju žrtava na web-lokacijama za usluge za odrasle (ASW), kao što je slučaj u Ujedinjenom Kraljevstvu, indikatori pokazuju neka jasna ograničenja i najbolje ih je koristiti u kombinaciji s **analizom društvenih mreža i ljudskom procjenom** dokaza.

Tehnološki alati mogu biti veoma dragocjeni u vršenju redukcije podataka i rukovanju velikim količinama informacija; međutim, potrebno je da ih koriste dobro obučeni operateri koji su

upoznati sa specifičnom temom/problemom (npr. trgovina ljudima). Korištenje vještačke inteligencije i tehnoloških alata za identifikaciju žrtava nije bez problema, uključujući etička pitanja i mogućnost diskriminacije (npr. profiliranje zasnovano na diskriminatornim kriterijima; vidjeti u nastavku).

Što se tiče inicijativa zasnovanih na tehnologiji za pomoć žrtvama i širenje informacija ugroženim zajednicama, države su identificirale primjere (1) online mehanizama za samoprijavljivanje i telefonskih linija za pomoć, uključujući digitalnu pomoć putem chat funkcije; (2) online kampanja za podizanje svijesti koje su često usmjerene na određene rizične grupe (npr. osobe koje traže posao); (3) namjenski razvijenih aplikacija i online alata; i (4) zvaničnih materijala koji su dostupni online i prevedeni na nekoliko jezika. Dobra praksa je rad s privatnim kompanijama na izradi **društvenog oglašavanja** (naprimjer, zajednički razvoj s društvenim medijima i sponzoriranje od strane društvenih medija). Međutim, online kampanje ne bi trebale zamijeniti direktne, lične kontakte s ranjivim pojedincima.

Dokazi prikupljeni od nevladinih organizacija

Nevladine organizacije su naglasile značaj postojanja **odgovarajućih i ažuriranih informacija** kojima žrtve trgovine ljudima i oni koji su podložni eksploataciji i zlostavljanju mogu lako pristupiti putem interneta. Takve online platforme također trebaju **omogućiti samoidentifikaciju** žrtava. Ovo bi se trebalo kombinirati s **kampanjama za podizanje svijesti**.

Nevladine organizacije su dalje istakle značaj razvoja znanja o rizicima vezanim za IKT i općenito o trgovini ljudima posredstvom tehnologije, također među organizacijama koje pomažu žrtvama, uključujući one koje pružaju savjetodavne usluge. Pošto je **očuvanje elektronskih dokaza** ključno za razvoj jakih istraga, od izuzetnog je značaja da savjetnici i NVO na prvoj liniji borbe budu upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem chat historija).

Dokazi prikupljeni od nevladinih organizacija potvrđuju da „**znaci upozorenja**" u slučajevima trgovine ljudima posredstvom tehnologije nisu u širokoj upotrebi. Nevladine organizacije prijavljuju korištenje standardnih indikatora, ali pozivaju na **reviziju takvih indikatora** kako bi se razmotrile specifičnosti IKT-a posredstvom tehnologije.

Nevladine organizacije su identificirale primjere **inicijativa zasnovanih na tehnologiji** koje su razvile da (a) podstiču samoprijavljivanje putem interneta; (b) uspostave kontakt s rizičnom populacijom, naprimjer, da razbiju izolaciju i osnaže žrtve; (c) podižu svijest među ranjivim i rizičnim grupama i omoguće traženje pomoći putem namjenskih aplikacija i web-lokacija; i (d) provode kampanje za podizanje svijesti putem interneta.

Općenito govoreći, NVO sve više koriste tehnologiju, ali njihov opći nivo i dalje ostaje „ograničen". Postoji opća saglasnost da se više može učiniti kako bi se bolje iskoristila tehnologija, naročito u pogledu načina na koji se tehnologija koristi za širenje informacija; za pristupanje potencijalnim žrtvama i komunikaciju s njima; i za primanje dojava i prijava.

Nevladine organizacije su također otvorile neka **kritična pitanja** u vezi s inicijativama i tehnološkim alatima, uključujući potrebu za periodima testiranja novih alata i – što je najvažnije – dokazima o njihovoj efikasnosti (koji su još uvijek veoma ograničeni). One

pozivaju na **više evaluacije i procjene utjecaja** razvijenih tehnoloških alata. Pored toga, često ne postoji dugoročna finansijska strategija za promoviranje i korištenje razvijenih alata, uključujući resurse za njihovo ažuriranje. Nevladine organizacije su također naglasile da, općenito posmatrano, još uvijek postoji ograničena dostupnost tehnoloških **alata koje praktičari mogu koristiti** (da bi odgovarali potrebama nevladinih organizacija, alati moraju biti „jeftini" i „jednostavni za upotrebu").

Dodatni dokazi prikupljeni na osnovu analize okruženja

Ostala pitanja otvorena u dostupnoj bazi dokaza uključuju sljedeća:

- Potrebu da se djeluje na osnovu informacija koje se koriste kroz tehnologiju (u slučaju o kojem su raspravljali Rende Taylor i Shih (2019), pokazalo se da se rijetko reagira na izvještaje radnika podnesene putem aplikacije za prijavu povratnih informacija o eksploataciji u lancima snabdijevanja);
- Tehnologiju ne treba posmatrati kao zamjenu za praktično znanje na terenu;
- Grupno djelovanje za potrebe otkrivanja žrtava može otvoriti pitanja privatnosti, kao i potencijalnog rizika od osvete. Iako se savjeti korisnika smatraju veoma dragocjenim, inicijative za grupno djelovanje moraju biti pažljivo ispitane i uravnotežene u odnosu na rizik stvaranja virtuelnih (i nevirtuelnih) grupa osvetnika;
- Potreba da se unaprijede prikupljanje i analiza digitalnih dokaza u cilju smanjenja opterećenja za žrtve (npr. kada se od njih traži da pruže dokaze protiv trgovaca ljudima ili u njihovu odbranu).

Obuka: šta je osigurano, šta je potrebno

Ogromna većina država je prijavila da organizira obuke o trgovini ljudima. Međutim, nivoi i formati obuka koje se organiziraju za **organe za provođenje zakona** razlikuju se od države do države. Neke države zahtijevaju od svih policajaca koji bi mogli doći u kontakt s potencijalnom žrtvom da prođu obuku, dok druge ograničavaju obuku na specijalizirane jedinice.

Postoji opća saglasnost o činjenici da službenici trebaju proći obuku o (a) načinu otkrivanja slučajeva trgovine ljudima i žrtava; (b) načinu prikupljanja, čuvanja i obrade elektronskih dokaza, uključujući metode izdvajanja informacija iz računara i drugih digitalnih medija; i (c) načinu korištenja relevantnog softvera, uključujući „**analizu velikih količina podataka**" i sistema za skeniranje mreže radi prikupljanja podataka (gdje to dozvoljava nacionalno zakonodavstvo). Nekoliko država smatra da je neophodna **obuka o OSINT-u**. Istražne tehnike koje uključuju **tajne istrage na internetu** također se smatraju sve važnijim.

Iako je većina država prijavila osiguravanje elemenata gore pomenutih obuka, one su također naglasile probleme, uključujući (a) potrebu da se obuka održi aktuelnom i, u nekim slučajevima, da se značajno unaprijede postojeći elementi; i (b) da se poveća procenat osoblja koje prolazi obuku. Neke države su izrazile zabrinutost zbog ograničenih obuka koje se često pružaju kada je riječ o pitanjima povezanim s IKT-om i, još više, trgovinom ljudima posredstvom IKT-a.

Gledajući u budućnost, **rizik od uskih grla u sistemu** je posebno akutan. S obzirom da će se zločini posredstvom IKT-a, uključujući trgovinu ljudima, vjerovatno neprekidno povećavati, postoji potreba da se ne oslanjamo previše na centralizirane centre za borbu protiv

visokotehnološkog (cyber) kriminala. Ključno je uključiti opće/osnovno **znanje o visokotehnološkom kriminalu** u rutinske obuke koje se organiziraju za istražitelje, a ne da se na to gleda kao na skup „specijaliziranih" vještina kako bi se izbegla takva uska grla.

Šest širokih oblasti se smatra ključnim za izgradnju kapaciteta: prikupljanje i analiza informacija iz otvorenih izvora (OSINT); prikupljanje podataka s profila društvenih mreža i aplikacija za komunikaciju, kao i s mračne/TOR mreže; ispitivanje informacija koje se nalaze na uređajima za komunikaciju i čuvanje informacija, uključujući informacije koje su korisnici izbrisali, kao i znanje o šifriranju; sposobnost da se podaci dobijeni iz IKT izvora potkrijepe dodatnim dokazima prikupljenim tokom krivične istrage; identifikacija žrtava/potencijalnih žrtava u online okruženju; obuka o ekonomskom i finansijskom kriminalu s elementom posvećenim online transakcijama i potencijalno kriptovalutama.

Organiziranje **obuka za tužioce i sudije** u vezi s trgovinom ljudima posredstvom IKT-a prilično je neujednačeno u različitim državama ugovornicama. Nekoliko država je navelo da trenutno ne organizira nikakve obuke za pravosuđe o ovoj pojavi. Druge države organiziraju opće obuke o trgovini ljudima bez elemenata posebno fokusiranih na pitanja vezana za IKT.

NVO su izrazile potrebu da im domaći organi za provođenje zakona i međunarodne organizacije organiziraju obuke o najnovijim dostignućima u tehnološkom okruženju i u oblasti trgovine ljudima, uključujući promjene u strategijama regrutiranja. Također su istakli potrebu za obukama o najboljim međunarodnim praksama i razmjeni iskustava među državama.

Pravni instrumenti

Nedostaci postojećeg međunarodnog okvira

Općenito posmatrano, države ugovornice su izrazile pozitivan stav o dostupnim pravnim instrumentima koji omogućavaju saradnju među državama u borbi protiv trgovine ljudima. Konvencije Vijeća Evrope o uzajamnoj pravnoj pomoći i o visokotehnološkom kriminalu smatraju se „najčešće" korištenim instrumentima i, generalno, ocijenjene su kao „adekvatne". Ipak, države ugovornice su identificirale neke potencijalne nedostatke i oblasti u kojima bi se postojeće zakonodavstvo moglo poboljšati. Najvažniji nedostaci koji su primijećeni odnose se na:

- Odsustvo zajednički dogovorenog (standardiziranog) pravnog okruženja koje podržava razmjenu između pružalaca internet usluga i nadležnih organa kada se bave specifičnim istragama;
- Odredbe koje omogućavaju pravovremeni odgovor privatnih kompanija na zahtjeve za dostavljanje podataka;
- Odredbe kojima se primoravaju privatne kompanije da otkriju informacije na direktan zahtjev/nalog druge države ugovornice;
- Odredbe kojima se provode zajednička pravila o čuvanju podataka;
- Odredbe za olakšavanje prikupljanja svjedočenja žrtava i korištenje svjedočenja u drugoj državi;
- Pitanja u vezi s transnacionalnim mjerama protiv web-lokacija na kojima se nalaze materijali koji se mogu povezati s olakšavanjem eksploatacije žrtava;
- Odredbe koje uvode „obavezu stalnog praćenja" za kompanije u čitavom lancu snabdijevanja;
- Upotrebu terminologije koja ne dozvoljava uvijek da se zakonodavstvo razvija paralelno s promjenama u modusu operandiju trgovaca ljudima;
- Razlike u prenošenju krivičnog djela trgovine ljudima (prema Protokolu UN-a iz Palerma) u nacionalno zakonodavstvo.

Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija) i borba protiv trgovine ljudima posredstvom IKT-a

Konvencija Vijeća Evrope o cyber kriminalu (Budimpeštanska konvencija) najrelevantniji je instrument usmjeren ka kriminalu posredstvom IKT-a koji navode države ugovornice.

Države ugovornice smatraju odredbe koje se odnose na **procesno pravo** najznačajnijim u kontekstu trgovine ljudima posredstvom IKT-a (Poglavlje II, odjeljak 2. Konvencije). Štaviše, one su naglasile **značaj neograničavanja procesnih mjera na ona krivična djela koja su izričito navedena** (npr. ona u Poglavlju II, odjeljak 1). Konvencija jasno ostvaruje svoj puni potencijal samo kada nije ograničena na krivična djela koja su izričito navedena u Poglavlju II, odjeljak 1. Ovo je naročito tačno u kontekstu trgovine ljudima posredstvom IKT-a.

Nekoliko država je ukazalo na korisnost odredbi navedenih u Poglavlju III Konvencije o međunarodnoj saradnji kao pravnom osnovu za **prikupljanje i razmjenu elektronskih dokaza** među državama. Konvencijom se uspostavlja mreža kontaktnih tačaka. Iako je ovo važan alat, gledajući u budućnost, vjerovatno je da će – sa sve centralnijom ulogom koju igraju IKT i elektronski dokazi – takve kontaktne tačke biti pod sve većim pritiskom – i brzo preopterećene ako ne budu imale adekvatno osoblje. Ovo nas dovodi do problema **uskih grla** unutar sistema, pri čemu je ključno odrediti gdje se nalazi kontaktna tačka unutar sistema krivičnog pravosuđa, što može biti veoma značajno.

Gledajući u budućnost, sljedeći koraci mogu omogućiti da se **Konvencija o visokotehnološkom kriminalu dalje koristi** u borbi protiv trgovine ljudima:

- Provođenje Drugog dodatnog protokola uz Konvenciju, koji je usvojen u novembru 2021. godine i bit će otvoren za potpisivanje 12. maja 2022. godine;
- Završetak usaglašavanja nacionalnog zakonodavstva s Konvencijom o visokotehnološkom kriminalu kako bi se iskoristio njen puni potencijal;
- Šira i poboljšana obuka o mogućnostima koje nudi Konvencija o visokotehnološkom kriminalu pošto neke države ugovornice trenutno ne koriste raspoložive alate u punom potencijalu;
- Veća svijest o obimu proceduralnih odredbi sadržanih u Konvenciji, pošto dokazi ukazuju na određeni stepen neslaganja među ispitanim državama o mjeri u kojoj se sadašnje odredbe mogu primijeniti na slučajeve trgovine ljudima;
- Provođenje procedure za ubrzavanje pružanja uzajamne pravne pomoći omogućavanjem slanja zahtjeva direktno subjektu koji se nalazi u stranoj državi, pod uvjetom da je o tome obaviješten pravosudni organ te države;
- Razvoj sinergije između GRETA-e i Komiteta za Konvenciju o visokotehnološkom kriminalu (TC-Y) radi kontinuiranog procjenjivanja primjene Konvencije o visokotehnološkom kriminalu u kontekstu trgovine ljudima.

Izazovi koje su identificirale NVO

NVO su ukazale na „jasna ograničenja" u pogledu **zaštite podataka (GDPR) i pravila privatnosti**. Osim toga, one pozivaju na donošenje zakona koji dozvoljavaju korištenje **digitalne forenzike** kao prihvatljivog dokaza u svim državama. Dalji izazovi se odnose na

ažuriranje propisa tako da uzimaju u obzir visokotehnološki (cyber) kriminal i internet, kao i osmišljavanje zakonodavstva i operativnih pravila za digitalne istrage.

Nacionalni pravni okviri koji se odnose na uklanjanje sadržaja u vezi s trgovinom ljudima

Velika većina država ima zakonske mjere koje uređuju identifikaciju, filtriranje i uklanjanje internet sadržaja u vezi s trgovinom ljudima. Mjere se često ne odnose konkretno na trgovinu ljudima, već općenito na „nezakonit sadržaj" (izuzetak su materijali o seksualnoj eksploataciji djece). U nekim državama procedure za uklanjanje sadržaja u vezi s trgovinom ljudima zahtijevaju sudski nalog. Neke od ovih država smatraju ove procedure „suviše rigidnim" ili neefikasnim i zalažu se za efikasnija sredstva. Na kraju, neke države su naglasile da pružaoci usluga koji se nalaze u inostranstvu mogu lako zaobići nacionalno zakonodavstvo o pravnoj odgovornosti pružalaca usluga.

Ljudska prava, etika i zaštita podataka

Dokazi prikupljeni od država ugovornica

Sve države ugovornice su navele usvajanje domaćeg zakonodavstva koje uređuje **obradu podataka** i **zaštitu podataka**. Što se tiče **lične zaštite žrtava**, jedan broj država je ukazao na uvođenje mjera za sprečavanje počinilaca da stupe u kontakt sa žrtvama; ispitivanje svjedoka putem videokonferencije kako bi se spriječio kontakt s optuženima; a u nekim slučajevima i mogućnost da žrtve pruže dokaze na sudu anonimno radi zaštite identiteta.

Države ugovornice su navele da imaju uspostavljene **starosno osjetljive protokole** u obliku različitih skupova procedura i zaštitnih mjera koje se obično primjenjuju u zavisnosti od toga da li je žrtva dijete (mlađe od 18 godina). Što se tiče **rodno osjetljivih protokola**, sve države kojima su ove informacije dostupne navele su da nemaju takve protokole, a jedini izuzetak je Austrija, koja je ukazala na poseban sistem podrške zasnovan na spolu žrtve.

Dokazi prikupljeni od nevladinih organizacija

U okviru standardne procedure, NVO traže pristanak žrtve prije nego što podijele informacije s organima za provođenje zakona. Problemi nastaju kada žrtve oklijevaju podnijeti pritužbu policiji iz različitih razloga, uključujući rizik od odmazde, socijalnog isključenja ili mogućnost da žrtva bude deportovana. NVO procjenjuju da je to slučaj s „mnogim žrtvama trgovine ljudima". Pitanja zaštite podataka i razmjene podataka mogu stvoriti **moralne dileme**. Iako dijeljenje podataka s organima za provođenje zakona i podnošenje pritužbi podržava istrage, koje potom kasnije mogu potencijalno spasiti i zaštititi više žrtava, to ima svoju cijenu za pojedinačnu žrtvu, koja bi mogla biti izložena rizicima i prijetnjama.

NVO su pozvale da se posveti više pažnje **potencijalnim rizicima i šteti koje stvaraju prikupljanje podataka velikih razmjera i tehnološki alati**. Također su pozvali na dalje razmatranje i dodatne mjere kontrole korištenja podataka i njihovog sigurnog čuvanja – i da se osigura poštovanje pravila zaštite podataka.

Na kraju, postoji veoma ograničen broj dokaza o **rodno osjetljivim protokolima** koje su razvile NVO. **Starosno osjetljivi protokoli** se obično primjenjuju na osnovu toga da li je žrtva maloljetna ili odrasla osoba.

Dodatni dokazi prikupljeni na osnovu analize okruženja

IKT mogu imati značajan utjecaj na **ljudska prava** pojedinaca, uključujući pravo na privatnost, slobodu izražavanja i zaštitu od diskriminacije. Politike za borbu protiv trgovine ljudima koje se u velikoj mjeri oslanjaju na tehnologiju moraju biti osmišljene tako da uzimaju u obzir ljudska prava.

Identificirana su ključna pitanja koja se odnose na **privatnost podataka, etiku, transparentnost, odgovornost i informirani pristanak**. OSCE (2020) je identificirao niz etičkih pitanja u vezi s razvojem tehnologije za borbu protiv trgovine ljudima, uključujući: (a) zaštitu privatnosti podataka; (b) protokole o saglasnosti koje potpisuju žrtve; (c) obuku za osobe koje rukuju osjetljivim podacima, posebno podacima o žrtvama; (d) sigurno čuvanje podataka; (e) sprečavanje upotrebe tehnologije za prikupljanje osjetljivih podataka o ranjivim osobama (naprimjer, opće prikupljanje podataka o ranjivim ili marginaliziranim populacijama, čime se stvara rizik od diskriminatornih praksi); i (f) korištenje tehnologije na način koji ne krši ljudska prava žrtava, kao ni prava opće populacije. ICAT (2019) i drugi izvori ukazali su na osjetljivost u vezi s dijeljenjem podataka. Kada se podaci dijele između država i/ili relevantnih agencija, to se treba uraditi u skladu s načelima privatnosti i povjerljivosti.

Gerry i drugi (2016) upozorili su na rizik koji donose široko rasprostranjeni **alati za praćenje** u borbi protiv trgovine ljudima. Iako takva tehnologija može ponuditi nove mogućnosti za intervenciju u situacijama trgovine ljudima, ona se također sastoji od **oblika nadzora koji potencijalno veoma zadire** u privatnost pojedinca.

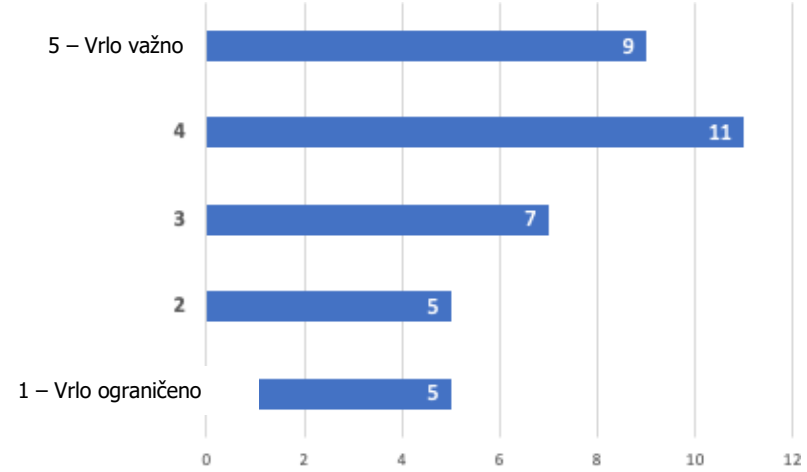
Na kraju, nekoliko izvora, uključujući Milivojević i drugi (2020) i Gerry i drugi (2016), ističe značaj **da se žrtvama ne uskraćuje mogućnost korištenja tehnologije**, jer pristup tehnologiji može biti njihov jedini način da komuniciraju s vanjskim svijetom i može poslužiti kao važan mehanizam suočavanja. Uklanjanje pristupa tehnologiji može obespraviti žrtve; promoviranju sigurnog pristupa tehnologiji treba umjesto toga dati prednost. Općenito govoreći, najbolji interes žrtve treba se staviti u centar svake akcije.

1. Utjecaj tehnologije na trgovinu ljudima

1.1. Dokazi prikupljeni od država ugovornica

Dokazi koje su dostavile države ugovornice potvrđuju sve veći značaj tehnologije u kontekstu trgovine ljudima, a naročito u vezi s regrutiranjem i eksploatacijom. Tehnologija i online aktivnosti postaju sve relevantnije u životima ljudi – i to se ogleda u kontekstu trgovine ljudima. Većina država ugovornica smatra da je utjecaj tehnologije na trgovinu ljudima „veoma važan" ili „važan" (slika 1).[4]

Slika 1. Utjecaj tehnologije na trgovinu ljudima: Države ugovornice



Napomena: N = 37

Među državama koje su prijavile ograničen utjecaj, neke su također prijavile veoma ograničene slučajeve ili nepostojanje slučajeva trgovine ljudima (tj. nizak tehnološki utjecaj, općenito nizak nivo trgovine ljudima). U drugim državama, upotreba tehnologije je (još uvijek) prilično ograničena (tj. niska upotreba tehnologije, nizak tehnološki utjecaj). U ovom posljednjem slučaju, slika bi se mogla promijeniti kako upotreba tehnologije postaje rasprostranjenija. Zaista, neke države ugovornice su istakle sve veći značaj online materijala, reklama/oglasa i stranica/aplikacija za traženje posla, kao i **sve veći značaj** online socijalizacije i ličnih interakcija. S druge strane, oba ova segmenta **stvaraju prilike** za počinioce u oblasti trgovine ljudima i **pogoršavaju postojeće ranjivosti.**

1.1.1. Trgovina ljudima u svrhu seksualne eksploatacije

U kontekstu **regrutiranja u svrhu seksualne eksploatacije**, nekoliko država ugovornica identificiralo je slučajeve oglasa za posao koji nude sumnjivo visoke plaće, često u sektorima usluga, što se pokazalo kao sredstvo za regrutiranje pojedinaca za eksploataciju. Nekoliko država je ukazalo na prisustvo veoma obmanjujućih ili potpuno lažnih oglasa za posao, koji se često objavljuju na web-lokacijama kojima se često pristupa i koji su navedeni među

[4] Tri države nisu dale odgovor na ovo pitanje.

legitimnim oglasima. Pored toga, postoje dokazi o regrutiranju preko platformi društvenih medija od strane pojedinaca koji nude poslove, naprimjer, u ugostiteljstvu (npr. konobarisanje) i poljoprivredi.

Počinioci obično obećavaju (nepostojeći) dobro plaćen posao u inostranstvu, a zatim prisiljavaju osobu da pruža seksualne usluge u zemlji odredišta.

Prema Nacionalnom izvještaju o situaciji u vezi s trgovinom ljudima za 2019. godinu koji su pripremili njemački nadležni organi, 11% identificiranih žrtava kontaktirano je ili regrutirano putem interneta (N = 47). Od tih 47 žrtava, 31 je kontaktirana preko često korištene platforme društvenih medija, a 13 preko portala za oglašavanje (tri žrtve su regrutirane korištenjem „druge" metode zasnovane na internetu). Bugarska nacionalna komisija za borbu protiv trgovine ljudima istakla je da su potencijalne žrtve koje se kontaktiraju putem društvenih medija „uglavnom mlade djevojke i žene". Holandske vlasti su prijavile da se, na osnovu informacija dostupnih u policijskom sistemu, platforme društvenih medija koriste za regrutiranje maloljetnih žrtava. Prema dokazima iz Austrije, regrutiranje se obično odvija u državama porijekla žrtava.

Kada se obraćaju potencijalnim žrtvama na internetu, počinioci mogu primjenjivati prilično sofisticiran modus operandi, često zasnovan na lažnim profilima koji pokazuju visok životni standard i značajno bogatstvo. Kako su naveli bugarski nadležni organi, „određeni broj istraga je otkrio da prije nego što priđu svojim potencijalnim žrtvama i započnu regrutiranje, počinioci pažljivo pregledaju fotografije svojih meta [kako bi] istražili njihove životne uvjete, društveni status i okruženje, porodične odnose i status veze, kao što su brak, razvod ili vjeridba. […] Tek nakon tako pažljivog ispitivanja počinioci stupaju u kontakt sa svojim žrtvama, koristeći izuzetne psihološke vještine ubjeđivanja i motiviranja žrtava da se upuste u određena ponašanja". Dokazi o takvom modusu operandiju opsežni su i dolaze iz nekoliko zemalja, uključujući Austriju, Bosnu i Hercegovinu, Bugarsku, Belgiju, Hrvatsku, Mađarsku, Republiku Moldaviju, Holandiju, Poljsku, Portugal, Slovačku, Švedsku i Ukrajinu. Takav modus operandi je često dio takozvane tehnike „ljubavnika", tj. pretvaranja da se počinilac upušta u romantičnu vezu kako bi se žrtva primorala na prostituciju. Kako su ocijenili nadležni organi u Rumuniji, između ostalih, „tehnika ljubavnika je i dalje najčešće korišteno sredstvo". Sastoji se u kontaktiranju osobe preko online platforme, upoznavanju njenih hobija i interesovanja, porodične situacije i ličnih okolnosti (kao i ranjivosti). Nakon toga, „trgovac ljudima prilazi žrtvi s empatijom, s velikom željom da joj pomogne i da je razumije, kao i da je finansijski podrži. Često se žrtvom manipulira obećanjima ozbiljne veze, ponekad i zahtjevima za brak, u pokušaju da se zadobije njeno povjerenje, a zatim i kako bi se uspostavila psihološka kontrola nad žrtvom" (dokazi iz Rumunije). Prema dokazima iz Belgije, žrtve regrutirane preko platformi društvenih medija imaju tendenciju da pokazuju obrasce porodične nestabilnosti, napuštanja škole, niskog samopoštovanja i, općenito, psihosocijalne ranjivosti.

Dokazi iz Francuske ukazuju da mreže trgovine ljudima različitih nacionalnosti, uključujući južnoameričkim, istočnoevropskim i francuskim državljanima uključenim u takozvanu trgovinu ljudima „de cité" („podvođenje u uskraćenom kraju"), koriste društvene mreže za regrutiranje žrtava. Čini se da su mreže za trgovinu ljudima koje uključuju pojedince iz afričkih zemalja izuzetak od ovog pravila. Brojne države su dostavile dokaze o regrutiranju preko aplikacija za upoznavanje (uključujući Ujedinjeno Kraljevstvo, Norvešku, Finsku, Austriju, Ukrajinu i Bjelorusiju).

Dostupno je obilje dokaza iz više zemalja o slučajevima **ucjene**. Ovo se najčešće postiže time

što se prvo prikupe „kompromitirajuće" informacije o žrtvama – naprimjer, time što se traže fotografije ili videosnimci nagog tijela – i potom koriste te informacije da se osoba prisili na prostituciju. Počinioci prvo uspostavljaju odnos sa žrtvom, zadobijaju njeno povjerenje, a zatim traže „kompromitirajuće" informacije. Nekoliko država ugovornica prijavilo je dokaze takvog ponašanja, uključujući Bosnu i Hercegovinu, Bugarsku, Hrvatsku, Holandiju, Finsku, Litvaniju i Švedsku.

Neke države su navele primjere žrtava koje su regrutirane na internetu među pojedincima voljnim da pružaju seksualne usluge; međutim, nakon regrutiranja bivaju izložene eksploatirajućem radnom vremenu i veoma lošim uvjetima smještaja, i suočene su s mogućnostima zarade koje se drastično razlikuju od onih koje se oglašavaju (dokazi iz Mađarske i Poljske). Dokazi iz Poljske također ukazuju na slučajeve žena koje reklamiraju seksualne usluge a koje su na meti trgovaca ljudima, zastrašivane i primorane da dijele svoj profit (mehanizam sličan iznudi).

Postoje brojni dokazi iz nekoliko država o internet stranicama koje se koriste za **oglašavanje seksualnih usluga**. U okviru takvih oglasa nalaze se i oglasi povezani s uslugama koje pružaju žrtve trgovine ljudima. Kako su napomenuli britanski nadležni organi, web-lokacije za usluge za odrasle (ASW) „su i dalje najznačajniji **omogućivač seksualne eksploatacije** povezane s trgovinom ljudima u Ujedinjenom Kraljevstvu". ASW lokacije su „privlačne za počinioce jer često zahtijevaju malo verifikacije korisnika i omogućavaju pristup velikoj bazi potencijalnih klijenata" (prijava britanskih nadležnih organa). Prema dokazima iz Finske, „IKT platforme, naročito stranice za oglašavanje zasnovane na forumima, glavni su modus operandi kada je riječ o marketingu i kontaktiranju klijenata u kontekstu trgovine ljudima". Francuski nadležni organi navode da je internet koristilo 65% identificiranih žrtava seksualne eksploatacije tokom 2019. godine; ovo je povećanje u odnosu na 49% u prethodnoj godini. Jedno od ključnih pitanja koje su britanski nadležni organi istakli u prijavi – a koje se primjećuje i kod drugih – jeste da se „oglasima koje objavljuju trgovci ljudima daje legitimitet njihovim pojavljivanjem pored oglasa koje objavljuju autonomni seksualni radnici". Prema nadležnim organima u Finskoj, „žrtve trgovine ljudima i seksualni radnici koji nisu žrtve koriste iste stranice". Nadležnim organima često predstavlja izazov da razvrstaju oglase povezane s trgovinom ljudima od onih koje objavljuju nezavisni seksualni radnici (vidjeti također Poglavlje 2).

Tehnologija se može koristiti za **koordinaciju aktivnosti tokom faze eksploatacije**, kao i za uspostavljanje kontakta s potencijalnim klijentima (uključujući pregovaranje o cijenama, određivanje lokacija i sklapanje dogovora). Ključno je to da tehnologija omogućava **razdvajanje** između mjesta gdje se seksualna aktivnost izvodi i mjesta gdje se vrši koordinacija. Ovo ima važne implikacije u pogledu provođenja zakona. Naprimjer, nadležni organi Bosne i Hercegovine iznijeli su dokaze o lancu koji eksploatira žene iz Bosne koje pružaju seksualne usluge u Njemačkoj i Austriji – tim uslugama su koordinirali i upravljali počinioci sa sjedištem u Bosni i Hercegovini. Ovo uključuje aktivnosti kao što je upravljanje online profilima žrtava i zakazivanje sastanaka s klijentima. Dokazi iz Francuske ukazuju na prisustvo platformi za upravljanje pozivima i upravljanje sastancima na daljinu s Kipra (za mreže na ruskom govornom području) i iz Kine (za mreže na kineskom govornom području). U brojnim slučajevima koje je švedska policija analizirala tokom 2019. godine, postojale su „sumnje da su aktivnosti prostitucije organizirane od strane kriminalnih mreža sa sjedištem u državama porijekla žena ili kroz povezanost s agencijom u trećoj državi". U istom izvještaju su

također identificirane slike različitih žena koje su povezane s istim ili veoma sličnim adresama e-pošte i/ili istim brojevima mobilnih telefona. Nadležni organi su ovo protumačili kao indikatore znakova upozorenja. Švedski nadležni organi su također naišli na slučajeve nepismenih Nigerijki i Rumunki koje su imale profil na ASW.

Ovo ukazuje na to da je takve profile izradio i njima upravljao neko drugi – još jedan potencijalni znak upozorenja.

Države su pružile dokaze o tehnološkim alatima koje trgovci ljudima koriste za **praćenje i kontrolu žrtava** tokom faze eksploatacije. U slučaju koji su prijavili slovenački nadležni organi, trgovci ljudima su tražili od žrtava da putem interneta prijave svaku pruženu uslugu. Žrtve su također morale prijaviti druge žrtve kako bi trgovci ljudima imali potpunu kontrolu nad njihovim aktivnostima. U drugim slučajevima, određene aplikacije su korištene za praćenje lokacije žrtve.

Na kraju, pored dvije „glavne" oblasti regrutiranja i eksploatacije, postoje dokazi da se tehnologija koristi kao pomoćno sredstvo logistike trgovine ljudima, uključujući kupovinu avionskih karata, kao i, u nekim slučajevima, pribavljanje lažnih putnih i drugih isprava (dokazi s Kipra). Aplikacije i web-lokacije se također mogu koristiti za rezerviranje nekretnina u kojima se pružaju seksualne usluge (dokazi iz Francuske, Estonije, Ujedinjenog Kraljevstva i Španije). Iako su dio trgovine ljudima, takve aktivnosti su pomoćne uz dvije osnovne aktivnosti regrutiranja i eksploatacije.

Kao **trendovi u nastajanju** u kontekstu seksualne eksploatacije primjetan je porast slučajeva **emitiranja uživo** seksualnih aktivnosti koje izvode žrtve trgovine ljudima. Iako je emitiranje uživo često povezano sa seksualnim zlostavljanjem djece, više država je ukazalo na činjenicu da emitiranje uživo može također uključivati i odrasle žrtve trgovine ljudima. Kiparski nadležni organi primijetili su sve češće korištenje web-kamera za prijenos uživo. Prema španskim nadležnim organima, trgovci ljudima „sve više" koriste web-stranice za emitiranje videozapisa kako bi plasirali usluge koje pružaju žrtve trgovine ljudima. Slično tome, irski nadležni organi su primijetili brz porast takozvanih aplikacija za videopozive po principu „plati koliko koristiš", kao što su Escortfans i Onlyfans, koje zamjenjuju tradicionalne web-platforme pružajući mogućnost za gledanje pratnje u online chat prostorijama za privatno ili javno dopisivanje. Irski nadležni organi su tvrdili da je „priroda ovih aplikacija i web-lokacija učinila gotovo nemogućim da se sazna da li neko dobrovoljno koristi platforme ili trpi eksploataciju" (sličan trend je primijećen i u Finskoj). Ovaj segment tržišta se navodno „eksponencijalno proširio" od izbijanja pandemije COVID-19. Kako su napomenuli holandski nadležni organi, „očekuje se da će se broj platformi još više povećati u (skoroj) budućnosti". Ovaj trend se proteže i na stranice i aplikacije za upoznavanje, web-stranice za oglašavanje seksualnih usluga, kao i na društvene medije koji se primarno ne fokusiraju na seksualne usluge, ali se mogu koristiti u tu svrhu.

Kiparski nadležni organi su također primijetili povećanje upotrebe aplikacija za kontrolu žrtava, npr. korištenje automatiziranih poruka koje se šalju na mobilni telefon trgovca ljudima svaki put kada žrtva izvrši određenu radnju (npr. otvori ulazna vrata). Švicarski nadležni organi su slično tome ukazali na otkrivanje aplikacija za lociranje na telefonima žrtava, koje su vjerovatno instalirane bez njihovog znanja. Sličan trend korištenja tehnologije za kontrolu žrtava primijećen je i u Austriji. Pored toga, grčki nadležni organi su prijavili porast broja slučajeva regrutiranja djece migranata putem mobilnih tehnologija u svrhu seksualne eksploatacije.

Nekoliko država je prijavilo **povećanje online interakcija** zbog pandemije COVID-19, čime se povećavaju mogućnosti za trgovce ljudima da uspostave kontakt s ranjivim pojedincima. Rumunski nadležni organi su primijetili porast broja žrtava koje su regrutirane putem interneta tokom posljednjih godina, a naročito nakon mjera za zaštitu javnog zdravlja zbog pandemije. Međutim, kao što navode, u Rumuniji se većina žrtava i dalje regrutira putem direktnog kontakta s prijateljima, partnerima i rođacima. U Francuskoj, nadležni organi su primijetili prelazak s ulične ponude na „diskretniji" sistem zasnovan na oglasima na internetu nakon usvajanja zakona 13. aprila 2016. godine koji kriminalizira kupovinu seksualnih usluga. Oni su također primijetili ubrzanje ovog procesa nakon pandemije COVID-19. Prema švedskom tužilaštvu, upotreba interneta u vezi s trgovinom ljudima u seksualne svrhe je toliko rasprostranjena da sada „teško da postoji slučaj trgovine ljudima u kojem se internet ne pojavljuje" kao dio modusa operandija trgovaca ljudima. Belgijski nadležni organi očekuju porast broja slučajeva ranjive djece ili mladih odraslih koji su regrutirani posredstvom IKT-a u svrhu seksualne eksploatacije – pošto ljudi u ovim starosnim grupama sve više komuniciraju online i putem IKT-a (u tehnološkom okruženju koje se stalno mijenja i koje predstavlja izazov za aktivnosti istražitelja).

1.1.2. Trgovina ljudima u svrhu radne eksploatacije

Dokazi koje su pružile države ugovornice pokazuju da se, u kontekstu trgovine ljudima u svrhu radne eksploatacije, IKT uglavnom koriste za **regrutiranje** žrtava. Prema tvrdnjama njemačkih nadležnih organa, internet i društveni mediji igraju „sve važniju ulogu u uspostavljanju kontakata i regrutiranju u oblasti trgovine ljudima i radne eksploatacije". Ovo mišljenje dijele i španski nadležni organi, prema kojima online regrutiranje u svrhu radne eksploatacije „postaje sve rasprostranjenije". Ovaj proces je vjerovatno ubrzao COVID-19 i posljedični rast prostora na internetu koji zamjenjuju interakcije licem u lice i sastanke. Kako su istakli irski nadležni organi, „ova sve veća upotreba društvenih medija za regrutiranje radnika migranata predstavlja sve veći izazov za organe koji se bore protiv obmanjujućeg i eksploatativnog regrutiranja na mreži". Prema francuskim nadležnim organima, iako se čini da „tradicionalni oblici zapošljavanja (oglasi u novinskim rubrikama za zapošljavanje, mali oglasi, flajeri, usmene preporuke itd.) i dalje preovladavaju, upotreba oglasa na internetu je sve rasprostranjenija". Ovo je povezano s velikim porastom upotrebe IKT-a od strane onih koji traže posao.

Dokaze o **obmanjujućim/lažnim oglasima za posao** u kontekstu regrutiranja u svrhu radne eksploatacije pružilo je više država, uključujući Austriju, Hrvatsku, Kipar, Estoniju, Finsku, Francusku, Grčku, Litvu, Litvaniju, Republiku Moldaviju, Norvešku, Poljsku, Portugal, Rumuniju, Švedsku i Švicarsku. Bugarski nadležni organi su istakli prisustvo oglasa na raznim stranicama za traženje posla u kojima „poslodavac" obećava velike plaće, besplatan prijevoz, besplatan smještaj i bonuse za poslove koji ne zahtijevaju razvijene vještine ili tečno poznavanje lokalnog jezika. Takvi oglasi su često dio modusa operandija trgovaca ljudima koji žele regrutirati radnike koji bi potom radili u uvjetima eksploatacije. Ovo se može primijetiti i u dokazima koje su pružili njemački nadležni organi, prema kojima „neki počinioci u početku nude zaposlenje na raznim internet portalima. Poslovi bi trebali biti dobro plaćeni, a radno vrijeme je navodno uređeno". Međutim, po dolasku u Njemačku, radnici „nisu dobili zvaničan ugovor o radu, niti su plaćeni kao što im je obećano. Često ne primaju nikakvu zaradu ili dobijaju samo djelić obećane naknade". Slični oglasi su primijećeni i u Španiji, gdje se „mnoge

žrtve trgovine ljudima u svrhu radne eksploatacije regrutiraju preko internet stranica za oglašavanje", navode nadležni organi.

Postoje dokazi iz Ujedinjenog Kraljevstva o lažnim oglasima za zapošljavanje koji su kružili društvenim medijima koji promoviraju mogućnosti zapošljavanja za visoko plaćenu radnu snagu/građevinarstvo u Londonu – u stvarnosti, kako su istakli nadležni organi, „ovo često nije slučaj i posao ne postoji". Što se tiče sadržaja oglasa, britanski nadležni organi su napomenuli da je „većina oglasa za posao koje su koristili trgovci ljudima zasnovana na nejasnim obećanjima o dobrom poslu, visokim zaradama i dobrim uvjetima, bez navođenja konkretnih oblika rada ili visine zarade. Međutim, u manjini zabilježenih slučajeva, oglasi za posao su ipak sadržavali ove detalje. Kod radne eksploatacije, više nego kod seksualne eksploatacije, uobičajeno je da se opiše sektor rada, iako se također redovno prijavljuju obmane". Počinioci ulažu velike napore da naizgled stvore legitimitet iza kojeg mogu sakriti svoju pravu prirodu: „Počinioci koji posjeduju kompanije u kojima se vrši eksploatacija također koriste internet omogućivače koji odražavaju legitimne operatere na istom tržištu, koriste imenike usluga i usluge mapiranja kako bi istakli radno vrijeme i usluge koje se nude" (dokazi iz Ujedinjenog Kraljevstva). Postoje dokazi iz više država koji ukazuju na to da se oglasi/reklame obično postavljaju na „poznate web-stranice za oglašavanje", kako u državi porijekla žrtve (dokazi iz Litvanije), tako i u državi eksploatacije (dokazi iz Francuske i Grčke). Drugi modus operandi, opisan u prijavi britanskih nadležnih organa, sastoji se od toga da počinioci koriste „internet platforme da identificiraju uloge ili slobodna radna mjesta na kojima će žrtve biti zaposlene i otvaraju bankovne račune za primanje zarada" (ovo je tzv. „model neposlodavca").

Različite države mogu tumačiti trgovinu ljudima u svrhu radne eksploatacije na različite načine, a granice između trgovine ljudima, zloupotrebe rada i nepoštovanja propisa mogu biti zamagljene i mogu varirati od države do države (konceptualno, one se mogu kretati u rasponu ozbiljnosti od nepoštovanja propisa do situacija u kojima se oduzimaju pasoši i ozbiljno ograničava sloboda kretanja). Naprimjer, britanski nadležni organi su primijetili da neki oglasi otvoreno upućuju na visine zarada koje su ispod nacionalne minimalne zarade; međutim, „velika je vjerovatnoća da se ovi [oglasi] odnose na zloupotrebe na radu i nepoštovanje propisa, a ne na trgovinu ljudima". Trgovci ljudima mogu „izbjeći prihvatanje obaveze isplate bilo kojeg iznosa, što također smanjuje potencijal da privuku pažnju organa za provođenje zakona i regulatornih organa". Ovo još jednom ukazuje na poteškoće s kojima se nadležni organi suočavaju prilikom identificiranja i uklanjanja takvih oglasa.

Oglasi se ne objavljuju samo na web-lokacijama za male oglase za zapošljavanje, već se objavljuju i distribuiraju na društvenim medijima, naprimjer u **specijaliziranim grupama za traženje posla i grupama za uzajamnu pomoć** (npr. „Bugari koji žive u inostranstvu" ili „Nguoi tim viec", što znači „ljudi u potrazi za poslom" na vijetnamskom jeziku). Nekoliko država je istaklo značaj stranica koje imaju za cilj da podstaknu razmjenu informacija među radnicima migrantima kao prostora za regrutiranje na meti trgovaca ljudima – prostora koji je često loše reguliran jer takve stranice mogu voditi pojedinci ili udruženja s nedovoljnim resursima. U nekim slučajevima, takvi oglasi se mogu širiti preko grupa za traženje posla kreiranih u aplikacijama za razmjenu poruka kao što je Telegram.

Oglasi mogu sadržavati veoma obmanjujuće informacije o uvjetima rada i naknadama, a često i mogućnost kontaktiranja „poslodavca" ili „agencije" samo preko šifriranih aplikacija kao što su Viber ili WhatsApp. Takve objave mogu doći do široke publike uz veoma male (ili nikakve)

troškove. U društvenom eksperimentu, nevladina organizacija iz Bugarske objavila je oglas za posao na Facebook-stranici nudeći posao u Danskoj u „berbi zelene srne" (igra riječima koja potječe od bugarskog idioma „poslati nekoga po zelenu srnu", što znači poslati nekoga u uzaludnu potragu), uz izuzetno visoku zaradu po satu. Za manje od sedmicu dana, više od 150 kandidata je dostavilo svoje biografije. Kao što je navedeno u nekoliko prijava, nivo tehničkih vještina potrebnih za korištenje online resursa i društvenih medija u svrhu trgovine ljudima je relativno skroman i sličan je vještinama koje većina korisnika interneta obično posjeduje (uzgred govoreći, ovo je daleko od nivoa sofisticiranih hakera i cyber kriminalaca).

Prema dokazima iz Bugarske, oglasi se često odnose na poslove u poljoprivredi (sezonski radnici), na gradilištima, u fabrikama i u ugostiteljskom sektoru. Ostali sektori koji se smatraju ugroženim su usluge u domaćinstvu i usluge njege. Njemački nadležni organi su identificirali kao rizično oglašavanje putem interneta u sljedećim sektorima: sezonski poljoprivredni radovi, usluge čišćenja, etno restorani, građevinarstvo, prehrambena industrija, transport i ljepota (saloni za nokte i masažu). Portugalski nadležni organi su prijavili nekoliko slučajeva koji su povezani s veoma obmanjujućim/lažnim oglasima za poslove u sektoru poljoprivrede i građevinarstva. Švedski nadležni organi su označili usluge čišćenja, građevinarstvo, restorane i salone za nokte. Osim toga, kiparski nadležni organi su označili ponude lažnih obrazovnih mogućnosti na privatnim univerzitetima i koledžima.

Kao **trend u nastajanju** u kontekstu radne eksploatacije, bugarski nadležni organi su prijavili porast slučajeva regrutiranja putem interneta i društvenih mreža. Vjeruje se da je ovo ubrzano izbijanjem pandemije COVID-19 i povezanim mjerama za zaštitu javnog zdravlja. Slično povećanje broja oglasa na društvenim mrežama su, između ostalih, primijetili kiparski, njemački i francuski nadležni organi. U Francuskoj su nadležni organi počeli primjećivati korištenje grupa za samopomoć u zajednici za regrutiranje i kontrolu žrtava i za prijenose sredstava. Na kraju, Francuska i Ujedinjeno Kraljevstvo su ukazali na povećanje mogućnosti za iskorištavanje žrtava povezanih s „ekonomijom honorarnih poslova", pošto se identifikacijski dokumenti ne provjeravaju redovno i pojedinci mogu raditi na tuđi račun. Naprimjer, treća strana može primiti sve zarade na svoj bankovni račun i samo manji dio prenijeti na radnika. Prema britanskim nadležnim organima, „ovaj modus operandi je identificiran kao tehnika koja omogućava zloupotrebe na radu i rad na crno, dok nivo kontrole koji vlasnik računa ima nad finansijama radnika predstavlja rizik od trgovine ljudima". Ovo gledište dijele i francuski nadležni organi, koji su primijetili da „iako za sada nije zvanično otkriven nijedan slučaj trgovine ljudima, za neke samozaposlene radnike se smatra da organiziraju oblike eksploatacije tako što daju u podzakup svoj račun neregularnim migrantima, tjerajući ih da rade bez zarade ili s veoma malom zaradom". Na kraju, belgijski nadležni organi su primijetili da je moguće nabaviti falsificirane dokumente u grupama koje oglašavaju svoje usluge putem šifriranih aplikacija za komunikaciju; takvi dokumenti se onda mogu koristiti za omogućavanje radne eksploatacije (npr. falsificirane lične isprave i vozačke dozvole, lažni ugovori o radu i lažne radne dozvole).

1.1.3. Mračna mreža i kriptovalute

Sve u svemu, države ugovornice nisu prijavile nikakve dokaze o značajnoj upotrebi mračne mreže u kontekstu trgovine ljudima. Ograničeni izneseni dokazi odnose se samo na širenje materijala o seksualnom zlostavljanju djece. Postoje neki dokazi iz Francuske da trgovci ljudima kupuju podatke o kreditnim karticama na mračnoj mreži, a zatim ih koriste za

rezerviranje soba u hotelima i apartmanima za iznajmljivanje – međutim, čini se da je ova aktivnost prilično ograničena i pomoćna. Norveški i francuski nadležni organi su primijetili da se seksualno zlostavljanje prijenosi uživo na mračnoj mreži, ali iz pruženih dokaza nije jasno da li ovi prijenosi uživo uključuju uglavnom djecu ili također uključuju i odrasle žrtve. Sve u svemu, vrlo je vjerovatno da mračna mreža igra veoma ograničenu ulogu u ovom trenutku, pošto i tokom regrutiranja i eksploatacije trgovci ljudima nastoje doprijeti do najšire moguće publike – a to je teško usaglasiti s mračnom mrežom u njenom trenutnom uređenju i nivou korištenja. Platforme s velikim brojem korisnika su poželjnije za regrutiranje (zaista, jedna od ključnih prednosti tehnologije je mogućnost da se dopre do velike grupe pojedinaca uz relativno male troškove). Slično tome, oglasi za seksualne usluge na internetu zahtijevaju kontakt sa širom publikom – nešto što nije moguće u tajnovitijoj mračnoj mreži.

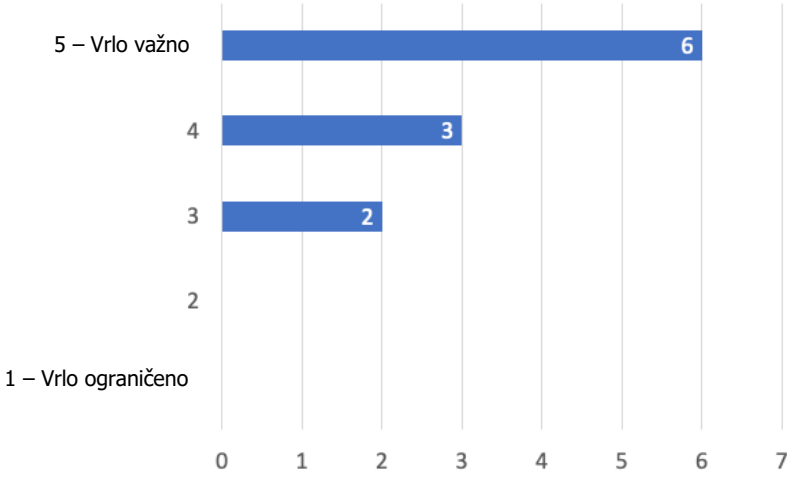
Čini se da korištenje kriptovaluta nije rasprostranjeno u kontekstu trgovine ljudima (s druge strane, postoje dokazi o njihovoj upotrebi za kupovinu prijenosa seksualnog zlostavljanja djece uživo na mračnoj mreži). Prijenosi novca se i dalje obavljaju tradicionalnim metodama, npr. preko kompanija kao što su Western Union ili MoneyGram ili, u nekim slučajevima, korištenjem pojedinaca (takozvanih „mazgi"). U nekim slučajevima mogu se koristiti neformalni sistemi za prijenos novca, kao što je Hawala. Neke države su počele prijavljivati prijenose novca putem aplikacija za razmjenu poruka (npr. WeChat). Vjerovatno je da će finansijsko-tehnološki proizvodi, npr. prijenosi novca preko aplikacija, igrati sve veću ulogu u budućnosti – jer razvijaju veći otisak u širem društvu (slično važi za kriptovalute, kada – i ako – postignu veći opticaj). Konačno, postoje dokazi o korištenju kartica i vaučera koji ne sadrže lične podatke (kao što su PaySafe kartice) za plaćanje online usluga, npr. za kupovinu oglasnih prostora na web-stranicama za usluge za odrasle.

1.2. Dokazi prikupljeni od nevladinih organizacija

Tri od četiri nevladine organizacije koje su konsultirane za potrebe izrade ove studije smatraju da je utjecaj tehnologije na trgovinu ljudima „veoma važan" ili „važan", pri čemu nijedna NVO ne ukazuje na „ograničen" ili „veoma ograničen" utjecaj (slika 2).[5]

[5] Jedna NVO nije dala odgovor na ovo pitanje.

Slika 2. Utjecaj tehnologije na trgovinu ljudima: NVO



Napomena: N = 11

Sve u svemu, kvalitativni dokazi koje su dostavile NVO koje direktno pružaju pomoć žrtvama trgovine ljudima daju sličnu sliku kao dokazi koje su pružile države ugovornice. NVO su primijetile korištenje interneta i društvenih medija u svim fazama trgovine ljudima, a naročito u vezi s (a) regrutiranjem; (b) eksploatacijom; i (c) vršenjem kontrole i pritiska nad žrtvama.

Među nevladinim organizacijama preovladava mišljenje da se utjecaj tehnologije na trgovinu ljudima povećao tokom pandemije COVID-19. Međutim, pandemija je možda samo ubrzala već postojeći trend. Kako je primijetila KOK – njemačka mreža koja okuplja 37 NVO koje pružaju specijalizirane usluge savjetovanja za žrtve trgovine ljudima – „već nekoliko godina savjetovališta izvještavaju o sve većoj ulozi interneta i društvenih medija u trgovini ljudima".

Članovi La Strada International, evropske NVO platforme koja okuplja 30 organizacija za borbu protiv trgovine ljudima u 23 evropske države, prijavili su slučajeve trgovine ljudima koji su regrutirani putem različitih online platformi, uključujući društvene medije i web-stranice za upoznavanje, kako u svrhu seksualne, tako i u svrhu radne eksploatacije. Ovi slučajevi su se ticali regrutiranja i odraslih i djece. Prema podacima koje je pružila CKM, NVO iz Holandije, online kontakti igraju naročito važnu ulogu kada se žrtve i počinioci međusobno ne poznaju: u skoro 80% ovih slučajeva prvi kontakt se ostvaruje online, npr. putem društvenih medija ili aplikacija za upoznavanje (dokaze pružila La Strada International). Ovo je naročito izraženo kod maloljetnih žrtava. Na osnovu intervjua sa žrtvama trgovine ljudima, albanska NVO „Different and Equal" primijetila je da su društveni mediji „postali glavno sredstvo" preko kojeg počinioci regrutiraju žrtve. Ovo je naročito slučaj s „djevojčicama [regrutiranim] u svrhu seksualne eksploatacije". U Švicarskoj, FIZ je također primijetio novi trend regrutiranja u svrhu trgovine ljudima putem različitih platformi društvenih medija, kao i aplikacija za upoznavanje. Općenito posmatrano, postoji opća saglasnost o činjenici da je upotreba – i značaj – tehnologije u slučajevima trgovine ljudima u porastu – i da se takva uzlazna putanja ubrzala tokom posljednjih godina.

1.2.1. Trgovina ljudima u svrhu seksualne eksploatacije

Strategije i mehanizmi koji predstavljaju osnovu za regrutaciju putem društvenih medija o

kojima izvještavaju NVO u skladu su s dokazima o kojima je već bilo riječi u odjeljku 1.1.1 iznad. Postoje dokazi o takozvanoj strategiji „ljubavnika", odnosno uspostavljanju lične/romantične veze putem društvenih medija kako bi se žrtva kasnije podvrgla eksploataciji. U tu svrhu se koriste lažni profili na društvenim medijima. Žrtve su obično maloljetne ili mlade odrasle osobe. La Strada Moldova je istakla da su posebno ugrožena djeca iz ruralnih područja, iz socijalno ugroženih porodica ili djeca u lošoj materijalnoj situaciji.

NVO su istakle mehanizme slične onima o kojima je bilo riječi ranije u ovom izvještaju u vezi s fazom eksploatacije. Oni uključuju korištenje web-lokacija za oglašavanje seksualnih usluga. Organizacija KOK (Njemačka) je primijetila da je policiji i savjetodavnim službama teže prići pojedincima koji oglašavaju seksualne usluge na internetu u odnosu na one koji pružaju iste usluge u registriranim ustanovama – što čini identifikaciju slučajeva trgovine ljudima težom.

Dalje, u slučaju seksualne eksploatacije, smještaj se može rezervirati online preko specijaliziranih stranica (dokazi iz Francuske dobijeni od organizacije La Strada International).

1.2.2. Trgovina ljudima u svrhu radne eksploatacije

Što se tiče regrutiranja u svrhu radne eksploatacije, NVO su pružile dodatne dokaze za mehanizme o kojima je već bilo riječi u odjeljku 1.2.2 iznad, naročito o korištenju lažnih i grubo obmanjujućih oglasa za posao na internetu. Naprimjer, u Albaniji je NVO „Different and Equal" primijetila online oglase za posao koji su povezani s eksploatatorskim praksama usmjerenim i na muškarce i na žene. U Srbiji je NVO „Astra" izrazila zabrinutost da bi čak i agencije koje su zvanično registrirane pri Agenciji za privredne registre i s redovnom licencom mogle oglašavati nezakonite poslove. Također su primijetili „velik broj" „neovlaštenih" oglasa, odnosno oglasa pojedinaca za koje se tvrdilo da su predstavnici agencija, kao i oglasa koji su povezani s eksploatatorskim praksama. Većina oglasa na internetu, smatraju oni, „ne podliježe nikakvom obliku kontrole ili nadzora". Njemačke i švicarske NVO otkrile su i dokaze o regrutiranju putem interneta za poslove koji ili ne postoje ili su podložni uvjetima eksploatacije. Ovo postoji u kontekstu „proliferacije regrutiranja za poslove putem interneta", kako je istakla organizacija Migrant Right Centre Ireland.

U prijavama nevladinih organizacija nema dokaza da tehnologija igra ključnu ulogu tokom faze eksploatacije u kontekstu radne eksploatacije. Međutim, naglašeno je da poslovi u ekonomiji honorarnih poslova, a naročito online platforme za hranu i druge isporuke, mogu biti podložni zloupotrebi od strane trgovaca ljudima. Kako je primijetila francuska NVO „Comite Contre l'Esclavage Moderne" (CCEM, francuska članica La Strada International), iako do sada nije identificiran nijedan slučaj trgovine ljudima u ovom kontekstu, procedure koje trenutno primjenjuju online platforme za isporuku mogu omogućavati trgovcima ljudima da zapošljavaju žrtve koristeći tuđi identitet.

1.2.3. Kontrola i pritisak nad žrtvama

NVO su primijetile da se tehnologija koristi za **vršenje kontrole nad žrtvama**, naročito u kontekstu seksualne eksploatacije. Bilo je slučajeva u kojima su se trgovci ljudima oslanjali na videonadzor, mobilne telefone, aplikacije i softvere za praćenje lokacije (dokazi koje je pružila La Strada International). Počinioci također mogu koristiti IKT za prijetnje porodici i prijateljima, npr. putem društvenih medija, ako žrtva odluči pobjeći iz situacije u kojoj se nalazi (dokazi koje je pružio KOK, Njemačka). Slične dokaze prikupila je i NVO „Astrée" u Švicarskoj.

Osim toga, žrtve mogu biti predmet **ucjena** putem društvenih medija i drugih online platformi.

Ovo je često povezano s prijetnjom otkrivanja „kompromitirajućih" informacija, uključujući fotografije i druge lične podatke (KOK izvještava o slučaju trgovca ljudima koji je ucjenjivao svoju žrtvu prijeteći da će objaviti njen HIV status na mreži Facebook).

Ono što je najvažnije, NVO su istakle da trgovci ljudima mogu koristiti IKT, uključujući društvene medije i šifrirane aplikacije, da **nastave kontakt** sa žrtvom trgovine ljudima čak i nakon što je žrtva napustila situaciju eksploatacije – često kako bi je spriječili da podnese pritužbu i traži pravdu. U Holandiji, CKM je utvrdio da je to slučaj kod otprilike jedne trećine žrtava s kojima su razgovarali (dokazi koje je pružila La Strada International).

1.2.4. Trendovi u nastajanju

Organizacije KOK i La Strada Moldova su zabilježile povećanje eksploatacije djece putem **web-kamera i društvenih medija**. Kako navodi La Strada Moldova, počinioci stupaju u kontakt s djecom na društvenim mrežama ili **putem online igrica**, sprijatelje se s njima ili simuliraju romantičnu vezu. Ponekad se počinioci predstavljaju kao predstavnici agencija za modeling. Od djeteta se zatim traži da podijeli intimne fotografije koje se zatim koriste za njegovu ucjenu. U tom trenutku, počinioci traže od svojih žrtava da izrade i dijele seksualno eksplicitniji sadržaj, kao i da učestvuju u izradi i emitiranju seksualnih radnji uživo.

U nekim slučajevima, žrtve su pod pritiskom da regrutiraju drugu djecu ili se sastaju van mreže radi izvođenja seksualnih radnji (KOK je primijetio slične obrasce).

Općenito govoreći, La Strada International i KOK su ukazali na sve veće ranjivosti nastale **otkrivanjem velike količine ličnih podataka** na društvenim medijima i drugim online platformama, kao i na sve veću otvorenost s kojom pojedinci mogu uspostavljati intimne kontakte s nepoznatim ljudima na online platformama.[6] Ovo je izraženije među mlađim generacijama. Iako tehnologija može pružiti značajne mogućnosti i prednosti – uključujući obogaćivanje razmjene – ona također može pogoršati ranjivosti. Naprimjer, dijeljenje seksualno eksplicitnih fotografija (seksting) može predstavljati rizik vezan za trgovinu ljudima, kao i uopće rizik od ucjenjivanja. Iako još uvijek nedostaju statistički podaci, istraživanje koje je naručila La Strada Moldova 2020. godine koje je uključivalo reprezentativni uzorak djece uzrasta 9–17 godina pruža neke zanimljive uvide u kontekst. Ovaj rad je otkrio da 13% djece u Republici Moldaviji smatra da je dijeljenje intimnih fotografija na mreži normalno među ljudima koji se vole;[7] 35% je komuniciralo s nepoznatim ljudima na mreži, a 20% se sastajalo van mreže s ljudima koje su upoznali na internetu (među njima, 2% je izjavilo da je uznemireno onim što se desilo na tom sastanku).

1.3. Dodatni dokazi prikupljeni na osnovu analize okruženja

Iako tehnologija može utjecati na trgovinu ljudima tokom svih njenih faza, njena uloga je od posebnog značaja u odnosu na dvije faze procesa: regrutiranje i eksploataciju (Latonero 2012; Di Nicola i drugi 2017, između ostalih).

Tehnologija može igrati ulogu u fazi **regrutiranja** time što olakšava identifikaciju, lociranje i uspostavljanje kontakta s potencijalnim žrtvama. Glavna promjena koju je donijela tehnologija

[6] Također treba napomenuti da društveni mediji i općenito IKT također mogu pomoći organizacijama civilnog društva da identificiraju i uspostave kontakt s potencijalnim žrtvama trgovine ljudima (o ovoj temi će biti više riječi u Poglavlju 3).

[7] Samo 1% ispitanika je izričito reklo da je podijelilo intimne (seksualno eksplicitne) fotografije i videozapise. Ovaj rezultat, međutim, treba tumačiti oprezno jer je na njega mogao utjecati efekat društvene poželjnosti.

jeste proširenje dometa trgovaca ljudima u potrazi za žrtvama, uz smanjenje „operativnih troškova" identifikacije i kontakta s potencijalnim žrtvama (Raets i Janssens 2018). Međutim, imajući u vidu da kasnije interakcije licem u lice i dalje igraju ključnu ulogu, trgovci ljudima se i dalje suočavaju s ograničenjima razmjera njihovih operacija. Kako su u igri različiti mehanizmi u zavisnosti od vrste eksploatacije, ključno je razdvojiti regrutiranje u svrhu seksualne eksploatacije od regrutiranja u svrhu radne eksploatacije.[8]

Kada je riječ o regrutiranju žrtava za **seksualnu eksploataciju**, tehnologija može pomoći pri regrutiranju na dva načina:

a. Može olakšati kreiranje i širenje **oglasa za posao na internetu** koji promoviraju mogućnosti za rad, najčešće u inostranstvu, u brojnim sektorima u rasponu od administracije, čišćenja ili brige o djeci (Europol 2014) do zabave, modelinga, usluga pratnje i seksualne industrije (VE 2007; UN.GIFT 2008; Di Nicola i drugi 2017).

b. Može olakšati identifikaciju i kontakt s potencijalnim žrtvama, često ranjivim pojedincima, putem društvenih medija i drugih aplikacija za lični kontakt (vidjeti, naprimjer, Di Nicola i drugi 2017).

Ovo se može smatrati specifičnom vrstom **vrbovanja na internetu**. Pristup zasnovan na tehnologiji se često primjenjuje u modelu regrutiranja „momak". Konkretne web-lokacije i aplikacije („aplikacije") koje se koriste podliježu promjenama u zavisnosti od online ponašanja i preferencija koje su specifične za određenu državu. Neki izvori su ukazivali na pojavu prakse pribavljanja „kompromitirajućih informacija" tokom regrutiranja, a zatim ucjenjivanja žrtava kako bi se ostvarila kontrola (praksa slična „seksualnoj iznudi"; Europol 2020).

Kada je riječ o regrutiranju u svrhu **radne eksploatacije**, tehnologija uglavnom pomaže regrutaciji putem širenja oglasa za posao na internetu. Specifični sektori su identificirani kao posebno ugroženi: veća je vjerovatnoća da će žene biti regrutirane za poslove u vezi s ličnom njegom, kućnom njegom, frizerskim uslugama i čuvanjem djece, dok je veća vjerovatnoća da će muškarci biti regrutirani za poslove u vezi s poljoprivredom, građevinarstvom, transportom i preuzimanjem i dostavljanjem humanitarnih torbi (Europol 2014; Di Nicola i drugi 2017; vidjeti također projekat Fine Tune 2011 i VE 2007). Dodatni identificirani sektori uključuju: ugostiteljstvo, preradu hrane i pakovanje (Fine Tune Project 2011). Oglasi se mogu objavljivati na legitimnim web-lokacijama koje su dostupne širokoj javnosti, na *ad hoc* web-lokacijama i/ili distribuirati putem društvenih medija.

Iako se čini da određeni izvori naglašavaju fizičku odvojenost između trgovaca ljudima i žrtava postignutu zahvaljujući tehnologiji (OSCE 2020), stvarnost je složenija. Postoje jaki dokazi koji ukazuju na to da upotreba tehnologije više dopunjuje nego što zamjenjuje lične interakcije van mreže. Tehnologiju i interakcije licem u lice je najbolje posmatrati kao integrirane. Vrlo je vjerovatno da stepen utjecaja tehnologije zavisi od faktora specifičnih za određene rizične populacije u određenim državama, uključujući: (a) korištenje interneta i društvenih medija uopće; (b) korištenje interneta i društvenih medija prilikom traženja posla; i (c) tehnološke pismenosti određenih rizičnih grupa.

Istraživanja pokazuju da se žrtve najčešće – ali ne uvijek – regrutiraju u državi porijekla, a zatim iskorištavaju u inostranstvu. Ovaj zaključak je već naveden u izvještaju Vijeća Evrope (2007), a naknadni, iako ograničeni, dokazi samo dodatno potkrepljuju ovu ideju. Sve ukazuje na to da će vjerovatno biti potrebne bilateralne i multilateralne akcije kako bi se stalo na kraj

[8] Nema dokaza da se tehnologija koristi u regrutiranju za druge vrste eksploatacije, uključujući i prisilno prosjačenje.

takvim pojavama.

Kada je riječ o **fazi eksploatacije**, tehnologija može igrati ulogu u vezi sa seksualnom eksploatacijom. Međutim, u ovom pregledu nema puno dokaza o primjetnoj ulozi tehnologije u kontekstu radne eksploatacije (Di Nicola i drugi 2017; Raets i Janssens 2018, između ostalih).

Kada je riječ o **seksualnoj eksploataciji**, tehnologija stupa na scenu na dva različita načina:

a. Može olakšati **kontrolu** koju trgovci ljudima vrše nad žrtvama korištenjem GPS-a ili drugih mobilnih aplikacija, čime se ograničava potreba da trgovci ljudima budu fizički blizu žrtava. Ucjena i upotreba kompromitirajućih informacija protiv žrtava su također pomenuti kao moguće strategije za vršenje kontrole (Raets i Janssens 2018). Na osnovu rijetkih dokaza, može se zaključiti da je ucjenjivanje žrtava primijećeno u relativno malom broju slučajeva analiziranih u Holandiji (8,8% slučajeva, bez datuma; izvor: OSCE 2020).

b. Može olakšati **prodaju** seksualnih usluga koje pružaju žrtve trgovine ljudima putem online oglasa usmjerenih na krajnje korisnike. Takvi oglasi se često objavljuju na specijaliziranim web-lokacijama ili *ad hoc* web-lokacijama.

Sve u svemu, utjecaj tehnologije na fazu **transporta** se smatra ograničenim, jer žrtve često putuju dobrovoljno i počinju doživljavati prinudu tek kada stignu do države odredišta (faza eksploatacije; dokazi agencija za provođenje zakona iz Bugarske, Rumunije i Italije izneseni u Di Nicola i drugi 2017). Korištenje tehnologije u ovoj fazi uglavnom se odnosi na mobilne telefone i aplikacije koje se koriste za organiziranje putovanja i koordinaciju vremena i mjesta sastanaka, kao i korištenje interneta za kupovinu karata i organiziranje putovanja. Iako trgovci ljudima mogu koristiti mračnu mrežu za kupovinu falsificiranih karata, kao i kompromitiranih podataka o kreditnim karticama koje se zatim koriste za kupovinu (lažnih) putnih isprava, detaljna procjena više izvora, kako akademskih tako i javno dostupnih dokumenata organa za provođenje zakona, sugerira da je upotreba mračne mreže i dalje veoma ograničena.

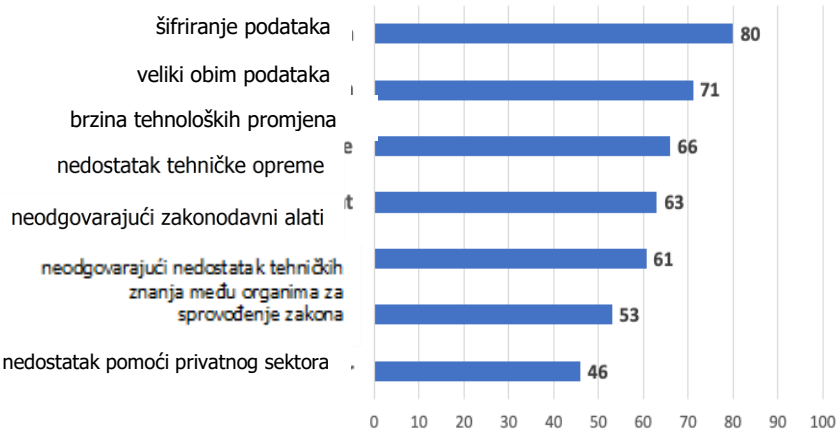
2. Izazovi tokom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom tehnologije

Ovo poglavlje istražuje izazove koji nastaju kao posljedica upotrebe tehnologije u kontekstu trgovine ljudima. U ovom poglavlju se ne bavimo širim izazovima s kojima se suočavaju države ugovornice, a koji nisu direktno povezani s upotrebom tehnologije. Ovo poglavlje prvo istražuje izazove koji se tiču istrage, a zatim slijede izazovi koji se odnose na krivično gonjenje i međunarodnu saradnju na osnovu dokaza koje su dostavile države ugovornice. Onda slijede dokazi prikupljeni od nevladinih organizacija, kao i pregled postojeće literature.

2.1. Izazovi tokom istrage

Državama ugovornicama je predstavljena lista od sedam potencijalnih izazova tokom istraga koji su identificirani na osnovu pregleda postojeće baze znanja, kao i ranijih radova koje su pripremili GRETA, Grupa eksperata Vijeća Evrope za borbu protiv trgovine ljudima, i Vijeće Evrope, uključujući i Radionicu iz 2019. godine pod naslovom „Pojačavanje borbe Vijeća Evrope protiv trgovine ljudima u digitalnom dobu".[9] Slika 3. predstavlja **nivo ozbiljnosti** za svaki od sedam izazova.[10]

Slika 3. Nivoi ozbiljnosti izazova tokom istraga



Napomena: Raspon rezultata = [0, 100]

Šifriranje podataka se smatra najvećim izazovom (rezultat 80). Na suprotnom kraju skale nalazi se nedostatak pomoći kompanija iz privatnog sektora, koji se smatra najmanjim izazovom. Svi izazovi, osim pomoći kompanija iz privatnog sektora, imaju rezultat veći od 50, što znači da se njihov ukupni utjecaj smatra većim od „malog" problema.

Ovi izazovi se redom razmatraju u sljedećim odjeljcima: šifriranje podataka (2.1.1), veliki obim podataka koji se obrađuju (2.1.2), nedostatak tehničke opreme (2.1.3), nedostatak tehničkih

[9] https://www.coe.int/en/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

[10] Za svaki izazov, od država ugovornica je zatraženo da procijene njegovu ozbiljnost koristeći skalu od tri stepena („obično nije problem", „mali problem" i „veliki problem"). Takve informacije su zatim pretvorene u nivo time što im je dodijeljena vrijednost od 0, 1 i 2 redom za „nije problem", „mali problem" i „veliki problem". Rezultati su zatim prikazani u rasponu [0, 100].

znanja među organima za provođenje zakona (2.1.4) i brzina tehnoloških promjena (2.1.5). Izazovi koji se odnose na pomoć privatnog sektora razmatraju se u odjeljku 4. ovog poglavlja, dok se izazovi koji proizilaze iz zakonodavnih instrumenata razmatraju u poglavlju 5. Treba napomenuti da su neki od izazova isprepleteni, iako se razmatraju odvojeno. Naprimjer, šifriranje (i dešifriranje) podataka zahtijeva stalna ulaganja u tehnologiju, kao i u razvoj stručnosti osoblja organa za provođenje zakona. Od država ugovornica je također zatraženo da navedu sve druge izazove s kojima se suočavaju pored sedam prethodno navedenih. O tim dodatnim izazovima će biti više riječi u odjeljku 2.1.6 u nastavku.

2.1.1. Šifriranje podataka

Šifriranje podataka se smatra najvećim izazovom s kojim se suočavaju nadležni organi kada provode istrage o trgovini ljudima posredstvom IKT-a. Iako se utjecaj TOR/mračne mreže ili šifriranih telefonskih mreža kao što je Encrochat smatra marginalnim, države su ukazivale na izazove koje donose protokoli za šifriranje koji se koriste u često korištenim aplikacijama i online uslugama (kao što su WhatsApp i Telegram). Šifriranje podataka može „onemogućiti vraćanje podataka tokom forenzičke istrage" (albanski nadležni organi). Nadležni organi Bosne i Hercegovine tvrde da „sve više istraga vodi do šifriranog HHD-a, zaključanih telefonskih uređaja, memorijskih kartica i šifriranih podataka". Prema nadležnim organima Islanda, većina problema s kojima se policija suočava potječe od „anonimnih i šifriranih naloga e-pošte i aplikacija, kao što su Proton-mail ili [pribavljanje] informacija o f.ex. pretplatniku". Praćenje i nadzor su također ograničeni, ako ne i nemogući – čak i uz zakonski nalog i suprotno drugim vrstama komunikacije. Austrijski nadležni organi su ukazali na nemogućnost da se internet telefonija (VOIP) stavi pod nadzor, dok su francuski nadležni organi istakli „nemogućnost praćenja sistema za trenutnu razmjenu poruka (WhatsApp, Messenger, Tik Tok, Wechat, Snapchat)", čime se stvara „velika prepreka za istrage (poteškoće u identifikaciji počinilaca i žrtava, u uspostavljanju veza među pojedincima i u prikupljanju dokaza o prinudi i podređenosti)".[11] Belgijski nadležni organi su dalje primijetili da istražne aktivnosti koje se provode u zatvorenim šifriranim kanalima zahtijevaju korištenje doušnika i tajnih agenata – a to može biti problematično u određenim državama (uključujući Belgiju). Nadležni organi u Irskoj su izrazili stav da „šifriranje postaje sve jače" – što je ponovilo i nekoliko drugih država ugovornica. Raznovrsnost šifriranih tehnologija dostupnih široj javnosti raste, sa sve više aplikacija za trenutnu razmjenu poruka koje su dizajnirane da maksimalno pojačaju šifriranje i maksimalno smanje količinu generiranih korisničkih podataka (npr. Threema ili Signal).

Kao što je navedeno u prijavi koju je podnijela Švicarska, utjecaj šifriranja varira u zavisnosti od toga da li istražitelji imaju pristup fizičkom uređaju ili ne. Ako je uređaj fizički u rukama istražitelja, onda je „šifriranje podataka manji problem, a podatke mogu dešifrirati specijalizirane policijske službe" (slično navodi i Luksemburg). Međutim, policajci s ovim tehničkim vještinama su malobrojni i ove službe će vjerovatno biti preopterećene – što dovodi do odlaganja istraga. Ako agencije za provođenje zakona nemaju pristup fizičkoj podršci, onda su „istrage otežane" (prijava koju je podnijela Švicarska). U nekim državama, naprimjer u Ujedinjenom Kraljevstvu, policijske snage imaju ovlaštenje da od osobe zahtijevaju da preda lozinku ili PIN za svoj mobilni telefon. Međutim, kako se ističe u dokazima koje su dostavili britanski organi, problemi i dalje ostaju: „čak i nakon hapšenja i zapljene takvih uređaja, mogu

[11] Ovo je također primijećeno u dokazima koje su dostavili grčki nadležni organi.

se javiti prepreke za pristup važnim komunikacijama", naročito kod uređaja s visokim nivoom sigurnosnih funkcija. Ovo su ponovili i belgijski nadležni organi, koji su ukazali na poteškoće u dešifriranju najsofisticiranijih algoritama (zato su pozvali na više ulaganja u nove alate za dešifriranje).

Nekoliko država je nagovijestilo postojanje alata za dešifriranje bar nekih vrsta algoritama. Jasno je, međutim, da je ovo okruženje koje se neprekidno razvija i zahtijeva (velika) ulaganja, kako u obuke, tako i u softver. Koraci preduzeti za prevazilaženje ovog problema uključuju uspostavljanje jedinica/centara za borbu protiv cyber kriminala čiji je zadatak rad s tehnologijom za dešifriranje. To je slučaj, naprimjer, s Norveškom. Slično tome, Francuska trenutno radi na razvoju uređaja za razbijanje lozinki „na centralnom nivou".

Slovenački nadležni organi su otvorili pitanje troškova vezanih za dešifriranje elektronskih podataka. Takvi troškovi nastaju kao posljedica potrebe za angažiranjem specijaliziranog, visoko obučenog osoblja, kao i kupovine specijaliziranih dijelova softvera koji mogu zaobići šifriranje. Štaviše, kako se protokoli za šifriranje neprestano razvijaju, postoji potreba da se softver stalno ažurira, što je često praćeno ogromnim naknadama za licencu.

Osim toga, moglo bi biti korisno udružiti resurse na nadnacionalnom nivou za potrebe razvoja tehnoloških proizvoda, kao što su softver za dešifriranje i skeniranje mreže radi prikupljanja podataka, kako su, naprimjer, predložili nadležni organi iz Švedske. Sve u svemu, iz dostavljenih dokaza proizlazi da se više može učiniti u pogledu **podsticanja razmjene znanja i udruživanja radi zajedničkog razvoja tehnologije** u različitim državama. Bliža i adekvatno finansirana tehnička saradnja se pokazala veoma uspješnom, naprimjer u infiltraciji u šifriranu mrežu za razmjenu poruka Encrochat koju koriste organizirane kriminalne grupe na visokom nivou širom Evrope (ovo je dovelo do više istraga i suđenja visokog profila u Francuskoj, Holandiji, Ujedinjenom Kraljevstvu i Švedskoj, između ostalih država).

U nekim slučajevima, kako su istakli francuski nadležni organi, šifriranje se može prevazići korištenjem alternativnih istražnih tehnika, naprimjer korištenjem „tehničkog nadzora telefonskih linija žrtava [koji] ostaje efikasno sredstvo dok se čeka tehnologija koja će omogućiti da se zaobiđe šifriranje".

2.1.2. Velike količine podataka

Elektronske komunikacije i IKT uređaji generiraju sve veću količinu podataka, što zauzvrat može predstavljati ogroman napor za istražitelje. Kako je istaklo nekoliko država, velika količina generiranih podataka utječe na mogućnost njihovog izdvajanja, što zahtijeva moćnu tehničku opremu. Jednako izazovna je analiza i pažljivo ispitivanje velikih količina informacija. Pametni telefoni imaju sve veći kapacitet memorije; dokazi koje generiraju korisnici mogu biti dostupni u više oblika: (dugačka) dopisivanja, ali i fotografije, snimci i glasovne poruke za čiju su analizu potrebne „sedmice" (dokazi iz Švicarske). Ovaj izazov je posebno naglašen u slučajevima kada se „ne može izvršiti pretraga po specifičnim ključnim riječima i [istražitelji] moraju pregledati sve podatke" (dokazi iz Švicarske). Prema švicarskim nadležnim organima, „iskustvo i praksa su pokazali da se količina podataka značajno povećala s modernim društvenim medijima, što potencijalno dovodi do veoma dugih istražnih aktivnosti […] koje mogu istražitelja držati zauzetim mjesecima i dovesti do uskih grla u resursima".

Velika količina podataka često zahtijeva specijalizirane dijelove softvera, kao i posebnu obuku o tome kako da se podaci sistematiziraju i pretražuju u okviru tako velikog broja dokaza.

Prema britanskim nadležnim organima, „internet tržišta i društvene mreže generiraju ogromnu količinu podataka [koju] može biti teško raščlaniti, a skupo je licencirati ili razvijati alate koji mogu efikasno analizirati ove podatke". Francuski nadležni organi su podjednako naglasili potrebu za razvojem alata koji bi mogli pomoći istražiteljima u rukovanju velikim količinama podataka, naprimjer pomoću algoritama vještačke inteligencije (AI) (slično su istakli i nadležni organi Španije). Prema norveškim nadležnim organima, količina elektronskih podataka čini „istrage složenijim, s potrebom za korištenjem istražnih metoda zasnovanih na tehnologiji".[12] Takve metode, međutim, često „dovode do velike količine podataka [od kojih] je samo mali dio […] koristan za istragu".

Postoji opća saglasnost da je razvoj kapaciteta za rukovanje velikim količinama elektronskih dokaza od ključnog značaja. Međutim, takav kapacitet se treba stalno ažurirati kako bi se držao korak s „internet omogućivačima koji se stalno mijenjaju zbog brzine tehnoloških promjena" (prijava britanskih nadležnih organa). Ovo ponavljaju i holandski nadležni organi, koji su ukazali na sve veću količinu podataka koje generiraju online platforme i društveni mediji, kao i na izazov koji donosi **promjena obrazaca ponašanja** njihovih korisnika, zbog čega je „teško otkriti gdje treba tražiti". Dostupnost digitalnih alata smatra se prvim (neophodnim) korakom; međutim, stalno prilagođavanje tehnološkoj i bihevioralnoj digitalnoj sredini predstavlja izazovan, ali neophodan sljedeći korak.

Problem dodatno pogoršava to što se velike količine podataka često trebaju obrađivati i analizirati u kratkom roku. Naprimjer, kada se osumnjičeni privede, službenici su pod vremenskim pritiskom da vrlo brzo pregledaju veliku količinu elektronskih dokaza – kako ističu slovenački nadležni organi. Ograničeno vrijeme koje je često istražiteljima na raspolaganju da pregledaju materijal zahtijeva „**bolju tehnologiju za pretragu i sortiranje informacija**" (dokazi iz Ujedinjenog Kraljevstva). Štaviše, nekoliko država ugovornica je istaklo da su elektronski podaci prikupljeni u kontekstu istraga trgovine ljudima često na jeziku koji istražitelji najčešće ne govore, što zahtijeva duge i skupe prijevode (ovo pitanje je posebno akutno među državama odredišta).

2.1.3. Nedostatak tehničke opreme

Nekoliko država je istaklo nedostatak tehničke opreme kao veliki izazov za provođenje istraga. Ovo uključuje često nedovoljan broj mašina koje mogu izvršavati specijalizirane zadatke, kao što je razbijanje šifri, kao i poteškoće u praćenju razvoja softvera i hardvera. Kao što je već spomenuto, specijalizirani softveri i hardveri mogu biti skupi i često zahtijevaju stalna ažuriranja i skupe ugovore o licenciranju kako bi pratili korak s brzinom tehnoloških promjena. Ovo može imati značajan utjecaj na budžet policije. Države s manjom kupovnom moći teško ispunjavaju zahtjeve u pogledu tehničke opremljenosti. Da nije bilo podrške međunarodnih partnera i donatora iz privatnog sektora, neke države bi već bile izgurane s međunarodnog tržišta specijaliziranih tehničkih alata (ovo izričito navode nadležni organi iz Albanije, ali također proizlazi iz prijava drugih država). Međutim, ovo nipošto nije pitanje ograničeno na države s manje raspoloživih resursa. Njemačka, Belgija, Švedska, Francuska i Ujedinjeno Kraljevstvo, između ostalih, izrazili su ozbiljnu zabrinutost zbog cijene specijaliziranog softvera i hardverske opreme.

Većina slučajeva trgovine ljudima je međunarodne prirode i često uključuje žrtve iz manje

[12] Nadležni organi iz Portugala su iznijeli isto opažanje.

bogatih država koje se eksploatiraju u bogatijim državama. Ovo u konkretnim slučajevima stvara potrebu za međunarodnom saradnjom među državama. To se također pretvara u često zanemarenu potrebu za ojačanim programima tehnološke pomoći koje podržavaju države odredišta u korist država izvora (tj. država porijekla žrtava) – pored postojećih multilateralnih programa, poput onih koje vodi Evropska unija, a koji već pružaju finansijsku podršku za nadogradnju tehnološke opreme.

2.1.4. Nedostatak tehničkog znanja među organima za provođenje zakona

Upotrebljivost same tehničke opreme je ograničena ako nema adekvatnih obuka koje su dostupne agencijama za provođenje zakona. Općenito govoreći, ulaganja u ljudski kapital, odnosno u obuke i tehničko znanje policijskih službenika, jednako su važna kao i ulaganja u softver i hardver – ako ne i važnija. Države ugovornice često spominju potrebu da se osiguraju takve obuke i dodatna tehnička znanja za policijske službenike. Prema riječima nadležnih organa u Belgiji, „imperativ" je da se smanji „**digitalna podjela između počinilaca i policijskih snaga**". Države ugovornice su identificirale različite potrebe za znanjem.

Prvo, postoji potreba za razvojem znanja o pojavi novih trendova i promjenama u korištenju tehnologije od strane počinilaca i žrtava. Drugo, države su istakle značaj razvoja znanja o pojavi novih aplikacija i usluga na tehnološkom tržištu koje karakteriziraju brze promjene. Treće, postoji potreba da se prati korak s razvojem novih sigurnosnih protokola i metoda šifriranja. Najvažnije je pak to da znanje treba mudro rasporediti unutar organizacije. Naprimjer, nedostatak specijaliziranih službenika na lokalnom nivou može stvoriti **uska grla u istragama**, ako je potrebno više puta tražiti pomoć od (preopterećene) centralizirane jedinice. Ovo je ključno pitanje na koje države trebaju obratiti odgovarajuću pažnju – i to je dokazano u prijavama nekoliko država ugovornica, uključujući Albaniju, Belgiju, Island, Francusku, Portugal, Slovačku i Sloveniju (vidjeti Poglavlje 4 za detaljnije diskusije o obukama).

Nekoliko država je istaklo potrebu za **organiziranjem dodatnih tehničkih obuka za „opće" policijske službenike**. Pored obuka za specijalizirane službenike s bogatim tehničkim znanjem u vezi sa specifičnim dijelovima softvera ili tehnikama dešifriranja, postoji potreba da se svim službenicima osigura osnovni skup digitalnih vještina i tehničkih znanja. Ključno je da službenici koji prvi izlaze na mjesto zločina posjeduju takva znanja. Kako su primijetili albanski nadležni organi, greške koje naprave osobe koje prve izlaze na mjesto zločina „mogu biti fatalne kada je riječ o prikupljanju elektronskih dokaza, [koji] onda postaju nevažeći za dalju analizu". Za najveći broj službenika potrebno je organizirati odgovarajuću obuku o prikupljanju i rukovanju **elektronskim dokazima**. Štaviše, razvoj stručnosti u ovoj oblasti treba biti redovna tema u nastavnim planovima i programima obuka za policijske službenike.

Pored toga, iako bi osnovni nivo tehničkog znanja bio prava prednost za sve istražitelje, mogu se desiti složeniji slučajevi u kojima će možda biti potrebno formirati timove s multidisciplinarnim skupovima vještina (npr. okupljanjem istražitelja, stručnjaka za finansijski i visokotehnološki kriminal). Države bi možda željele razmotriti uvođenje – ili unapređenje – odredbi koje omogućavaju brzo formiranje takvih timova, kad god je to potrebno, ili čak da interdisciplinarni timovi postanu sastavni dio savremenog policijskog rada. Ovo bi se moglo proširiti na međunarodne zajedničke istražne timove, npr. uključivanjem stručnjaka za tehnologiju i komunikacije u takve timove (što su istakli bugarski nadležni organi).

Švicarski nadležni organi primjećuju da je „držanje koraka s tehnološkim napretkom veliki izazov za organe za provođenje zakona", a današnjim istražiteljima je potrebna ekspertiza i za trgovinu ljudima i za IKT, uključujući korištenje društvenih medija i tehničke vještine. Francuski nadležni organi su izrazili potrebu da obuče više osoblja za korištenje novih tehnologija, kao i za finansijske istrage. Nadležni organi Bugarske su izvijestili o primjeru u kojem je u saradnji s francuskim nadležnim organima korištena kombinacija istražnih tehnika na mreži i van mreže. Polazeći od otkrića pornografskih slika djece, istražitelji su uspjeli prvo identificirati IP adresu, a zatim je fizički locirati u hotelu. Kada su upali u hotel, pronašli su brojne žene koje su bile prisiljene pružati seksualne usluge i došli do niza Facebook pseudonima drugih žrtava, koje su potom identificirane pomoću njihovih Facebook profila. Na kraju je identificirano 60 žrtava trgovine ljudima u svrhu seksualne eksploatacije, jedno dijete žrtva koje je bilo prinuđeno proizvoditi pornografski materijal, kao i 18 počinilaca. Ovaj slučaj ukazuje na potrebu da istražitelji budu dobro upućeni u online i offline istražne tehnike, jer je sve veća vjerovatnoća da će se obje tehnike morati koristiti tokom istraga trgovine ljudima. To bi, naravno, zahtijevalo kontinuiranu obuku.

2.1.5. Brzina tehnoloških promjena

Brzi tempo tehnoloških promjena je sveobuhvatno pitanje koje utječe na sve gore navedene izazove: šifriranje, obuku policajaca, tehnološku opremu i prikupljanje elektronskih dokaza. Molimo pogledajte diskusiju iznad za više detalja.

2.1.6. Dodatni izazovi tokom istraga

Brojne države su označile problem u vezi s (neadekvatnim) **obavezama čuvanja podataka** koje su nametnute pružaocima internet usluga (ISP) i u vezi s njihovim utjecajem na istrage. U Bugarskoj, naprimjer, postojeće zakonodavstvo zahtijeva od pružalaca internet usluga da čuvaju takve podatke šest mjeseci – trajanje koje se smatra neadekvatnim za razvoj jakih istraga. Dužinu čuvanja podataka također su naveli nadležni organi Holandije i Malte. Norveški nadležni organi su napomenuli da, prema nacionalnom zakonodavstvu, pružaocima internet usluga nije dozvoljeno čuvati informacije o IP adresama duže od 21 dan i od njih se ne traži da čuvaju podatke o vezi između pretplatnika i IP adrese. Bugarski i rumunski nadležni organi pozvali su na usaglašavanje nacionalnih propisa koji uređuju čuvanje podataka o internet saobraćaju, kao i istražnih praksi u vezi s prekršajima posredstvom IKT-a.

Zabrana trojanaca (tj. špijunskog softvera) smatra se dodatnim izazovom za istrage uz pomoć IKT-a, jer agencijama za provođenje zakona nije dozvoljeno ući u domove i druge prostorije da instaliraju špijunski softver na uređaje koje koriste pojedinci koji su predmet istrage. Nadležni organi tvrde da bi takvi alati omogućili agencijama za provođenje zakona da ublaže probleme u vezi sa šifriranjem, kao i poteškoće u prisluškivanju VOIP razgovora. Belgijski nadležni organi pozvali su na izmjene pravnog okvira kako bi se olakšao istražni rad pomoću novih tehnologija. Oni su istakli potrebu za pojednostavljenjem procedura i pravnih sredstava uzimajući u obzir modus operandi počinilaca.

Bugarski nadležni organi su pokrenuli pitanje u vezi s elektronskim dokazima, posebno ističući potrebu da se uvedu međunarodni zahtjevi koji bi od pružalaca internet usluga tražili da implementiraju odgovarajuće sigurnosne protokole koji sprečavaju bilo kakvo **neovlašteno mijenjanje podataka,** kako tokom čuvanja, tako i tokom prijenosa organima za provođenje

zakona.

Holandski nadležni organi su pokrenuli pitanje vezano za primjenu **zakona o privatnosti**, naprimjer u kontekstu korištenja sistema za skeniranje mreže radi prikupljanja podataka.

Nadležni organi u Španiji su zatražili da veći broj zaposlenih bude specijaliziran za borbu protiv trgovine ljudima i napredne vještine korištenja računara. Nadležni organi iz Belgije su iznijeli isto opažanje.

Moldavski nadležni organi su ukazali na poteškoće u zadržavanju kvalificiranih praktičara jer službenici s iskustvom često napuštaju specijalizirane jedinice kako bi se pridružili drugim sektorima pravosuđa ili privatnom sektoru, i naglasili su značaj redovnih provjera motivacije za privlačenje i zadržavanje talenata.

Austrijski nadležni organi su istakli problem s kaznama koje su predviđene za trgovinu ljudima u njihovom nacionalnom Krivičnom zakoniku, a koje predviđaju kaznu zatvora između šest mjeseci i 10 godina. Iako je ova kazna dovoljna za praćenje poruka po nalogu suda, ona ne daje policijskim snagama pravo da koriste vizuelni i akustični nadzor (tj. audionadzor privatnih razgovora i privatnih prostorija).

Britanski nadležni organi su primijetili izazove kada je riječ o IP adresama i elektronskim dokazima. IP adrese su početna tačka u istrazi i, kada se pribave, organi za provođenje zakona moraju upariti te IP adrese s različitim korisničkim imenima i korisnicima. Međutim, korisnička imena se mogu promijeniti u bilo kojem trenutku i osumnjičeni ih često koriste naizmjenično. Od ključnog je značaja da organi za provođenje zakona provjeravaju kontinuitet IP adresa u odnosu na korisnička imena. Pored toga, u virtuelnim chat sobama, neki korisnici se mogu vidjeti na ekranu – i njihov identitet je dokazan – ali možda ima i drugih koji nemaju uključene web-kamere. Neki osumnjičeni mogu dijeliti uređaje s drugima, naprimjer ako se nalaze u domaćinstvu s više stanara, što zauzvrat može otežati njihovu identifikaciju.

Britanski nadležni organi su također pokrenuli pitanje postupanja s neiskorištenim elektronskim materijalom, posebno u kontekstu obaveza po osnovu GDPR-a. U istom smislu, holandski nadležni organi smatraju da međunarodni propisi o zaštiti podataka „ometaju prikupljanje, čuvanje i obradu informacija pribavljenih tehnološkim istražnim tehnikama (kao što su sistemi za skeniranje mreže radi prikupljanja podataka)", čime „sprečavaju optimalnu upotrebu [takvih] tehnika".

ZOOM | Izazovi u otkrivanju slučajeva trgovine ljudima posredstvom IKT-a

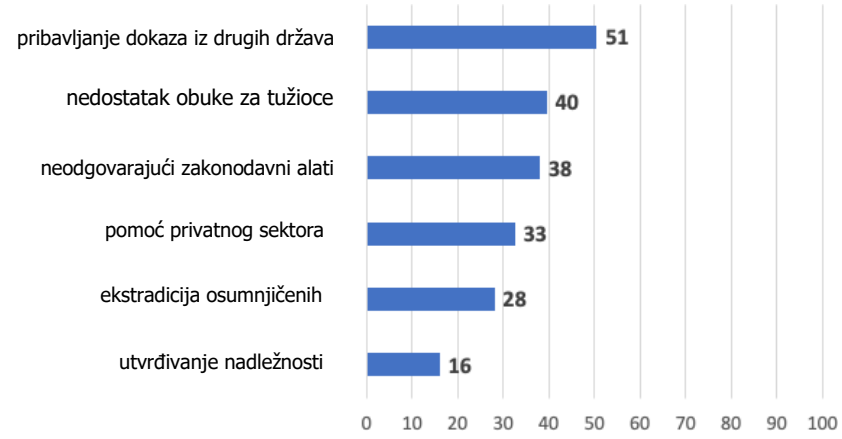
Istrage i krivično gonjenje zavise od otkrivanja slučajeva. U nastavku su navedeni izazovi koje su identificirale države kada je riječ o otkrivanju trgovine ljudima posredstvom IKT-a:

- Internet predstavlja veoma velik prostor za praćenje, a obim online aktivnosti/interakcija neprekidno raste. Online resursi obuhvataju veoma širok i raznolik spektar, od stranica za oglašavanje na mreži i web-lokacija za odrasle, do platformi društvenih medija, chat soba i potencijalno mračne mreže. Nadzor nad takvim prostorom zahtijeva ogromne resurse i podliježe zakonskim ograničenjima (zakoni o privatnosti i ograničenja korištenja sistema za skeniranje mreže radi prikupljanja podataka u nekim državama).
- Ručno pretraživanje web-lokacija na internetu je izuzetno izazovno, dok velike količine nestrukturiranih podataka otežavaju skeniranje mreže radi prikupljanja podataka (ako je to uopće dozvoljeno nacionalnim zakonodavstvom). Broj online oglasa (otvorenih i malih oglasa) za seksualne i neseksualne usluge često je prevelik za ručno pretraživanje.
- Poteškoće prilikom identifikacije počinilaca i žrtava, jer mogu koristiti nadimke i pseudonime tokom svojih online aktivnosti. Softver za anonimizaciju (npr. VPN) i upotreba šifrirane komunikacije između trgovaca ljudima i žrtava dodatno otežavaju identifikaciju. Razgovori između trgovaca ljudima i žrtava odvijaju se u zatvorenim grupama (npr. Facebook, WhatsApp, Telegram).
- Ponašanje korisnika interneta koje se brzo mijenja (npr. nova tehnologija se pojavljuje, nove web-lokacije/aplikacije postaju popularne za kratko vrijeme). Pored toga, brzo se pojavljuju novi alati, podstaknuti jakom konkurencijom u tehnološkom sektoru, koji trgovcima ljudima mogu pružiti nova sredstva za povezivanje i eksploataciju žrtava.
- Izazovi prilikom sortiranja online oglasa kako bi se identificirali oni koji se odnose na trgovinu ljudima u kontekstu seksualnih i neseksualnih usluga. Oglasi za seksualne usluge koje objavljuju žrtve trgovine ljudima često koriste iste stranice, istu terminologiju i iste formulacije kao oni koje objavljuju nezavisni seksualni radnici. „Znaci upozorenja" za identifikaciju oglasa povezanih s radnom eksploatacijom još uvijek su nedovoljno razvijeni ili se ne koriste dosljedno.
- Odsustvo specijaliziranih jedinica u policiji i/ili nedostatak specijaliziranih istražitelja za slučajeve trgovine ljudima s naprednim vještinama korištenja računara. Nedostatak službenika obučenih za izvođenje tajnih operacija na internetu (npr. stvaranjem i održavanjem „lažnog" profila).
- Nedostatak obuka za policijske službenike o specifičnostima trgovine ljudima posredstvom IKT-a (npr. modus operandi počinilaca, platforme na kojima se trgovina odvija, kako tajno pristupiti trgovcima ljudima i kreirati kredibilne profile na internetu).
- Mogućnost uklanjanja/mijenjanja razgovora (elektronskih dokaza) od strane trgovaca ljudima.
- Proces slanja zahtjeva kompanijama koje upravljaju društvenim medijima (često sa sjedištem u stranoj državi) koji oduzima mnogo vremena i nedostatak reakcije nekih kompanija.
- Kratki periodi čuvanja IP adresa i poteškoće oko pristupanja takvim podacima.
- Jezičke barijere.

2.2. Izazovi tokom krivičnog gonjenja

Državama ugovornicama je predstavljena lista od šest potencijalnih izazova tokom krivičnog gonjenja, a koji su identificirani na osnovu pregleda trenutne baze znanja, kao i ranijih radova koje je pripremilo Vijeće Evrope, uključujući i radionicu iz 2019. godine pod naslovom „Pojačavanje borbe Vijeća Evrope protiv trgovine ljudima u digitalnom dobu".[13] Slika 4. predstavlja **nivo ozbiljnosti** za svaki od šest izazova.[14]

Slika 4. Nivoi ozbiljnosti izazova tokom krivičnog gonjenja



Napomena: Raspon rezultata = [0, 100]

Sve u svemu, izazovi tokom krivičnog gonjenja imaju niže ocjene od onih tokom istrage, pri čemu je samo za „pribavljanje dokaza iz drugih država" ocjena nešto viša od 50 (ocjene veće od 50 ukazuju na to da se izazov često doživljava kao ozbiljniji od samo „manjeg problema"). Razlog je vjerovatno činjenica da, ako je slučaj zaista stigao u fazu krivičnog gonjenja, većina prepreka je uspješno otklonjena tokom faze istrage.

U nastavku navodimo još neke kvalitativne dokaze o tri izazova: utvrđivanje nadležnosti, ekstradicija osumnjičenih i obuka tužilaca. Izazovi koji se odnose na pomoć privatnog sektora razmatraju se u odjeljku 2.4, dok su izazovi koji proizilaze iz zakonodavnih instrumenata razmatrani u poglavlju 5. Izazovi u vezi s pribavljanjem dokaza iz drugih država razmatrani su u odjeljku 2.3, i predstavljaju prepreke međunarodnoj saradnji.

Utvrđivanje nadležnosti: Dok se generalno smatra da je utvrđivanje nadležnosti manji izazov među državama ugovornicama, povremeni problemi mogu se pojaviti u slučajevima koji su omogućeni IKT-om, a tiču se istovremenih nadležnosti. U nekim slučajevima mogu se pojaviti izazovi pri identifikaciji osumnjičenih i, što je najvažnije, pri utvrđivanju njihove lokacije, što znači povezivanje određene IP adrese s određenom osobom, a zatim te osobe s lokacijom u određenoj državi.

[13] https://www.coe.int/en/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

[14] Za svaki izazov, od država ugovornica je zatraženo da procijene njegovu ozbiljnost koristeći skalu od tri stepena („obično nije problem", „mali problem" i „veliki problem"). Takve informacije su zatim pretvorene u nivo time što im je dodijeljena vrijednost od 0, 1 i 2 za „nije problem", „mali problem" i „veliki problem". Rezultati su zatim prikazani u rasponu [0, 100].

- *Ekstradicija osumnjičenih*: Sve u svemu, ovo se posmatra kao relativno mali problem. Evropski nalog za hapšenje (EAW) i Evropski nalog za istragu (EIO) dva su važna alata koja su „omogućila da se efikasno (i također određenom brzinom) odgovori na izazove koje predstavlja transnacionalnost" (portugalski nadležni organi). Kao primjer dobre prakse spominje se rad Eurojusta. Nadležni organi Švicarske su ukazali na prepreke s kojima se suočavaju jer nisu u mogućnosti izdati evropski nalog za hapšenje i evropski nalog za istragu. Slično tome, britanski nadležni organi su naveli da „izlazak Ujedinjenog Kraljevstva iz EU može utjecati na ekstradiciju" jer „zabrana državljanstva nekih država znači da [Ujedinjeno Kraljevstvo] više ne može izručiti neke državljane EU i zahtijeva diskusiju o tome koja država vrši krivično gonjenje". Razlike u zakonima o trgovini ljudima između država mogu stvoriti izazove u pogledu ekstradicije osumnjičenih.
- *Obuka tužilaca*: Nekoliko država je istaklo značaj odgovarajuće obuke za tužioce o trgovini ljudima posredstvom IKT-a, napominjući da u nekim slučajevima ova obuka nedostaje ili nije adekvatna. Obuka tužilaca se smatra ključnom kako bi se osiguralo da predmeti koji se razvijaju uz pomoć IKT-a budu robusni, da se elektronski dokazi pravilno prikupljaju i koriste i da se predmeti (i dokazi u njima) na odgovarajući način izvode pred sudijom/porotom. Neke države, poput Norveške, planiraju pojačati takvu obuku tako što će dovesti tužioca s iskustvom u predmetima trgovine ljudima koji će držati predavanja kolegama. Osim toga, stručnost možda neće biti stalno dostupna u svim tužilaštvima u državi. Ovaj problem su, između ostalih, primijetili i holandski nadležni organi. Kao odgovor, holandsko tužilaštvo, zajedno s nacionalnom policijom, trenutno procjenjuje nivo stručnosti u ovoj službi. Takav proces unutar državnog praćenja može se smatrati primjerom dobre prakse kako bi se osigurala dosljednost u nivou stručnosti u okviru države. Osim toga, neke države ugovornice su zabilježile slučajeve u kojima tužioci nisu bili upoznati s procedurom traženja elektronskih podataka od privatnih kompanija; u drugim slučajevima, tužioci nisu bili upoznati s procedurama za pribavljanje dokaza od drugih država i traženje njihove saradnje, naprimjer uspostavljanjem zajedničkog istražnog tima ili izdavanjem evropskog naloga za istragu. Unaprijeđena obuka za tužioce bi trebala olakšati proces povezivanja s drugim državama, kao i privatnim kompanijama. Na kraju, države ugovornice su izrazile stav da interdisciplinarnu obuku s elementima trgovine ljudima i IKT-a treba proširiti na sudije.

Osim toga, od država ugovornica je zatraženo da navedu sve **dodatne izazove** s kojima se suočavaju u procesuiranju slučajeva trgovine ljudima posredstvom IKT-a. U nastavku je dat pregled identificiranih izazova:

- Britanski nadležni organi su označili problem u dokazivanju učešća i *mens rea* pojedinačnih počinilaca u slučajevima koji su omogućeni IKT-om kada postoji grupna aktivnost, naprimjer u internet chat sobi gdje jedan ekran možda prikazuje zlostavljanje žrtve trgovine ljudima, dok drugi ekrani možda prikazuju druge korisnike koji učestvuju u aktivnostima odraslih koje se obavljaju uz njihovu saglasnost. Dokazivanje učešća različitih pojedinaca može predstavljati izazov s obzirom na različite uloge.
- Još jedan izazov koji su britanski nadležni organi istakli u prijavi odnosi se na izvođenje dokaza pred porotom (ili sudijom). U slučajevima do kojih dolazi posredstvom IKT-a, izvođenje tehničkih dokaza često radi stručnjak koji je upoznat s tehnologijom (koji objašnjava kako, naprimjer, funkcionira emitiranje uživo iz internet chat soba, koje su njegove funkcije i koji snimci su možda snimljeni, uključujući opis šta kakav snimak prikazuje).

Razvijanje interne stručnosti među službenicima o tome kako efikasno i tačno izvesti

elektronske dokaze sve više dobija na značaju. Srodan izazov odnosi se na izvođenje velikih količina elektronskog materijala pred porotom. Rješenje koje se razmatra u Ujedinjenom Kraljevstvu je upotreba tableta.

2.3. Izazovi međunarodne saradnje

Tokom studije od država ugovornica traženo je da ukažu na izazove s kojima se suočavaju u vezi s transnacionalnim istragama i pravosudnom saradnjom u kontekstu trgovine ljudima posredstvom IKT-a. Većina navedenih izazova nije specifična za trgovinu ljudima posredstvom IKT-a, ali općenito utječe na prekogranične istrage i pravosudnu saradnju, naprimjer, jezičke barijere, različiti pravni osnovi, koordinacija paralelnih istraga, brza razmjena informacija. Međutim, specifičnosti trgovine ljudima posredstvom IKT-a često ih pogoršavaju. Ovo je posebno akutno u slučaju elektronskih dokaza. Pored toga, u kontekstu trgovine ljudima posredstvom IKT-a, primanje uzajamne pravne pomoći i osiguravanje dokaza često imaju kritičnu vremensku komponentu.

2.3.1. Zahtjevi za uzajamnu pravnu pomoć

Većina država ugovornica je označila dugo vrijeme potrebno za obradu zahtjeva za uzajamnu pravnu pomoć (UPP) kao jednu od glavnih prepreka međunarodnoj saradnji. Sve u svemu, postupci traženja uzajamne pravne pomoći smatraju se sporim, ponekad nepredvidivim i takvim da su im potrebni međunarodno dogovoreni jedinstveni obrasci. Kako su primijetili španski nadležni organi, „ima previše izvora informacija koji zahtijevaju sudsko odobrenje kako bi im se pristupilo". Takvi zahtjevi moraju biti obrađeni putem uzajamne pravne pomoći, što zauzvrat komplicira i produžava tok istrage. Postojeći sistem je nekoliko država okarakteriziralo kao „neadekvatan". Zahtjevi za uzajamnu pravnu pomoć između država ugovornica VE mogu se odvijati u okviru dva različita scenarija: (a) u okviru pravosudne saradnje EU (uključujući pomoć Europola i Eurojusta) i (b) van okvira EU. Kako izazovi i procedure mogu biti drastično različiti u zavisnosti od scenarija, važno ih je razmotriti odvojeno.

Saradnja u okviru pravnog okvira EU. Države ugovornice Vijeća Evrope koje su također države članice Evropske unije vide koordinirani okvir policijske i pravosudne saradnje na nivou EU kao koristan i sposoban da ujednači proces. To uključuje rad agencija EU kao što su Eurojust i Europol. Međutim, izazovi i dalje postoje. Prema francuskim nadležnim organima, „instrumenti međunarodne saradnje, iako zanimljivi, ipak su spori: za evropski nalog za istragu (EIO) potrebno je nekoliko mjeseci, a zajednički istražni tim (ZIT) je teško provesti". Jedna od glavnih prepreka provođenju zajedničkih istražnih timova je potreba za identičnom istragom u drugoj državi ili u više njih. Na ovo su također ukazali nadležni organi Norveške.

Saradnja izvan pravnog okvira EU. Ovo se posmatra kao proces koji oduzima više vremena i karakterizira ga veća zamršenost nego u scenariju navedenom iznad zbog nedostatka usaglašenosti između različitih pravnih sistema (kao što su istakli, između ostalog, kiparski i španski nadležni organi). Švicarski nadležni organi su primijetili da odgovor na „zahtjeve za međunarodnu pravnu pomoć često zavisi od dobre volje ili interesa stranih tužilaca". Ovo unosi element nepredvidljivosti i nedosljednosti u proces. Takvi „pregovori između tužilaštava su često dugotrajni". **Jasnije operativne procedure, poboljšana redovna razmjena između kontaktnih tačaka i zahtjevi za UPP, jasno postavljeni** i razmotreni na samom početku, doprinijeli bi usaglašavanju procesa. Nadležni organi u Sjevernoj Makedoniji

primijetili su da svi zahtjevi za uzajamnu pravnu pomoć moraju proći kroz centraliziranu jedinicu u okviru Ministarstva pravde, što stvara usko grlo i često usporava procedure. Predložili su da se osmisle alternativni mehanizmi koji bi omogućili određenim ključnim institucijama da uspostave direktan kontakt sa svojim međunarodnim kolegama (npr. javno tužilaštvo, inspektorat rada, ministarstvo unutrašnjih poslova).

Norveški nadležni organi su ukazali na potrebu da se unaprijede postojeći sporazumi i da se uspostave novi sporazumi s državama porijekla žrtava kada su one van EU. Ovo je pitanje koje su pokrenuli i francuski nadležni organi, koji su naglasili da „određeni broj kriminalnih organizacija koje koriste IKT potječe iz država s kojima je međunarodna saradnja ili nedovoljna ili nepostojeća. To je slučaj s kineskim mrežama i mrežama iz Rusije i Ukrajine". Zahvaljujući IKT-u, ove kriminalne mreže mogu organizirati svoje operacije na način koji omogućava glavnim članovima da kontroliraju aktivnosti prostitucije iz svoje države porijekla – često znajući da zahtjevi za pravosudnu saradnju neće biti pravovremeno ispunjeni, ako uopće i budu ispunjeni. Spora saradnja ili odsustvo saradnje utječu na identifikaciju počinilaca, prikupljanje dokaza i gašenje web-lokacija.

ZOOM | Šta se može naučiti iz pravosudnog okvira EU?

Nema sumnje da pravosudni okvir EU nudi integriraniji pravni prostor koji može olakšati pravosudnu saradnju u poređenju sa situacijom s kojom se države ugovornice suočavaju kada traže saradnju izvan takvog okvira (iako s ograničenjima i izazovima). Koji elementi takvog okvira bi se mogli proširiti izvan saradnje unutar EU? Ovo je teško pitanje koje zahtijeva sveobuhvatnu pravnu analizu, ali ovdje možemo ukratko navesti neke preliminarne sugestije. Prijava nadležnih organa iz Švicarske (tj. države izvan pravosudnog okvira EU) lijepo sumira ključne prednosti okvira EU, a naročito Evropskog naloga za istragu (EIO):

- zasniva se na zajedničkom skupu pravila sa širokom oblašću primjene;
- utvrđuje jasne rokove za prikupljanje dokaza;
- osnovi za odbijanje su ograničeni;
- smanjuje administrativno opterećenje kroz uvođenje jedinstvenog standardnog obrasca;
- osigurava zaštitu osnovnih prava odbrane.

Jasno je da se neke mjere mogu proširiti samo ako su dio sveobuhvatnog skupa zajedničkih pravnih pravila. Međutim, države ugovornice bi možda željele razmotriti koji specifični aspekti EIO mogu funkcionirati van okvira EU. Ovo bi moglo obuhvatiti saradnju između država potpisnica Konvencije Vijeća Evrope o borbi protiv trgovine ljudima i Evropske konvencije o ljudskim pravima. Mjere koje se tiču određivanja rokova za prikupljanje dokaza i smanjenja administrativnog opterećenja kroz uvođenje standardiziranih procedura potencijalno bi se mogle provesti bez suštinskih promjena u nacionalnim pravnim sistemima. Može se predvidjeti i neki poboljšani, zajednički skup pravila, pod uvjetom da država poštuje odredbe Evropske konvencije o ljudskim pravima.

Dodatna pitanja u vezi s UPP-om. Dokazi koje su dostavile države ugovornice također ukazuju na izazove u obradi zahtjeva za UPP koji su rezultat nedostatka osoblja koje je adekvatno obučeno za sastavljanje i obradu takvih zahtjeva – kao i korištenja zastarjele tehnologije. Naprimjer, neke države su navele da ne koriste uvijek sigurnu e-poštu i druge oblike elektronske korespondencije prilikom razmjene dokumenata sa stranim partnerima. Razvijanje upotrebe sigurnih oblika elektronskih komunikacija, uključujući pravila i mjere zaštite, i promoviranje njihovog usvajanja među svim državama ugovornicama, moglo bi donekle doprinijeti poboljšanju međunarodne saradnje među državama. Pored toga, širenje praktičnih informacija o kontaktnim tačkama/namjenskim jedinicama unutar države koje mogu poslužiti kao „privilegirani kontakt" u slučajevima trgovine ljudima, uključujući trgovinu ljudima posredstvom IKT-a, također može olakšati procedure.

2.3.2. Elektronski dokazi

Iako su izazovi u vezi s pribavljanjem elektronskih dokaza često povezani s UPP-om, priroda i relevantnost takvih dokaza predstavlja niz dodatnih izazova koje treba razmatrati odvojeno.

Kako su istakli austrijski i britanski nadležni organi, elektronski dokazi mogu otežati identifikaciju tačne lokacije podataka. Utvrđivanje države u čijoj su nadležnosti podaci nije uvijek jednostavno – što otežava izradu nacrta zahtjeva za uzajamnu pravnu pomoć. Portugalski nadležni organi smatraju da sistem za pribavljanje elektronskih dokaza iz drugih država nije „prikladan za svoju namjenu", i navedeno je da Drugi dodatni protokol uz Budimpeštansku konvenciju (visokotehnološki kriminal)[15] može donijeti unapređenja postojećeg sistema. Slično tome, grčki nadležni organi su pozvali na uspostavljanje zajedničkog pravnog okvira za brzu razmjenu digitalnih dokaza (uz napomenu da postoji zajednički pravni okvir za očuvanje dokaza).

Otvoreno je pitanje o vremenu kada se zakonski može podnijeti zahtjev za dostavljanje elektronskih dokaza. Prema britanskim nadležnim organima, „ponekad organi za provođenje zakona zahtijevaju pristup sadržaju komunikacije prije nego što mogu pokazati opravdani povod, ali preduvjet za dobijanje takve pomoći mora biti zadovoljen prije nego što se sadržaj podijeli". Ovo naročito utječe na rane faze istrage. Slično tome, austrijski nadležni organi su naveli izazov koji podrazumijeva „visok prag potreban za dobijanje podataka o sadržaju od nekih država". Isti organi su pokrenuli pitanje koje vrste informacija je moguće tražiti tokom istrage i po kojem pravnom osnovu (npr. sa sudskim nalogom ili bez njega). Austrijski nadležni organi su pozvali na primjenu „standardiziranog pristupa CID informacijama tokom istraga trgovine ljudima" (npr. traženje informacija o pretplatnicima od operatera mobilnih mreža). Oni su istakli da je „u nekim državama [ovo] moguće samo nakon što nadležni sud pošalje evropski nalog za istragu. U Austriji je to moguće bez sudskog naloga tokom istraga CID".

Kao što je već navedeno ranije u ovom izvještaju (odjeljak 2.1.6), pravila o dužini čuvanja podataka su označena kao naročito problematična. Nekoliko država je izrazilo zabrinutost zbog nepostojanja homogene regulative o čuvanju podataka – čime se ometa razmjena elektronskih dokaza. Neke države možda nemaju zakone o čuvanju podataka.

Konačno, nekoliko država je izrazilo zabrinutost zbog pristupa elektronskim dokazima koji se

[15] Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji je usvojio Komitet ministara Vijeća Evrope - Vijesti (coe.int)

nalaze na računarskim serverima izvan njihove nadležnosti. Iskustva u ovom pogledu variraju u zavisnosti od države i kompanije koja posjeduje podatke. Međutim, postoje brojni dokazi o poteškoćama u identifikaciji kompanije, njenom lociranju, uspostavljanju saradnje i organiziranju prijenosa dokaza. Države ugovornice su izrazile potrebu za sveobuhvatnijim okvirom koji uređuje čuvanje i prijenos elektronskih dokaza, kao i za zajedničkim pravnim okvirom koji zamjenjuje postojeće *ad hoc* bilateralne radne sporazume između države i privatne kompanije koja drži podatke.

2.4. Izazovi tokom saradnje s privatnim kompanijama

Studija je istraživala izazove s kojima se države ugovornice suočavaju u borbi protiv trgovine ljudima kada rade s IKT kompanijama i pružaocima internet usluga, uključujući pružaoce sadržaja i društvene medije. Iako se neki od ovih izazova preklapaju s pitanjima o kojima je već bilo riječi, ipak je korisno ponuditi neka dalja razmatranja o problemima koje su istakle države ugovornice. U nastavku je dat pregled takvih izazova:

- Dobijanje pravovremenog odgovora od pružalaca internet usluga i pružalaca sadržaja. Obraćanje pružaocima putem molbi poslatih preko relevantnih organa može dovesti do dugog čekanja s rizikom da sadržaj bude izbrisan do trenutka kada se postupi po zahtjevu. Francuski nadležni organi su istakli dugo vrijeme potrebno za odgovor na zahtjeve za dostavljanje metapodataka u vezi s nalozima povezanim s počiniocima; za podatke o sadržaju često treba postojati zahtjev za uzajamnu pravnu pomoć, za koji je potrebno po nekoliko mjeseci da se realizira pošto se kompanije često nalaze izvan nadležnosti države koja upućuje zahtjev (i Evropske unije).

- Pojašnjavanje pravnih zahtjeva u skladu s kojima IKT kompanije i pružaoci internet usluga funkcioniraju. Austrijski nadležni organi su izrazili zabrinutost da „međunarodni pružaoci usluga često nameću formalističke, pravno neopravdane zahtjeve agencijama za provođenje zakona kao preduvjete za pružanje informacija i predaju korisničkih podataka i sadržaja. Izvršavanje naloga tužilaštva je ponekad veoma komplikovano". Prema tvrdnjama nadležnih organa iz Belgije, odbijanja često nisu adekvatno opravdana i objašnjena. Nadležni organi Bosne i Hercegovine su ukazali na poteškoće u dobijanju podataka koji nisu lični podaci tokom istraga (prije nego što se može izdati sudski nalog). Identifikacija pružalaca internet usluga sama po sebi može predstavljati izazov – kako su istakli nadležni organi Finske.

- Francuski nadležni organi su istakli probleme u vezi s nepriznavanjem tužilaštva kao nezavisnog sudskog organa prilikom izdavanja zvaničnog zahtjeva za traženje podataka; dodatni problem su zahtjevi kompanija da objelodane veliku količinu dokaza iz istrage koja je u toku prije nego što pravna služba kompanije može donijeti odluku o predaji podataka.

- Belgijski nadležni organi su primijetili nedostatak povratnih informacija o internim operacijama koje provode kompanije, npr. u vezi s uklanjanjem sadržaja. Također su prijavili poteškoće u komunikaciji s kompanijama – koje uključuju česte promjene osoblja za kontakt.

- Kao što je već navedeno, države su kao ključne izazove navele nedostatak usaglašenog zakonodavstva oko čuvanja podataka i neadekvatne zakonske odredbe. U Norveškoj, naprimjer, pružaocima internet usluga nije dozvoljeno čuvati podatke o IP adresama duže od 21 dan i od njih se ne traži da čuvaju podatke o vezi između pretplatnika i IP adrese. Prema norveškim nadležnim organima, to „otežava policiji da identificira osumnjičene za trgovinu ljudima posredstvom IKT-a". Ovaj problem se pogoršava kada se radi o kompanijama koje su

osnovane da pružaju anonimne i šifrirane usluge.

- Moldavski nadležni organi su prijavili nedostatak određene kontakt-tačke u privatnim kompanijama koje upravljaju društvenim medijima i drugim aplikacijama za umrežavanje. Predloženo je da se uspostavi kontaktna tačka za svaku državu/područje (u zavisnosti od broja korisnika). (Može se misliti i na kontaktne tačke određene na osnovu jezika koji se govori). Moldavski nadležni organi su predložili da uspostavljanje kontaktnih tačaka bude obavezno za pružaoce internet usluga, pružaoce sadržaja i društvene medije. Slovački nadležni organi su istakli problem jezičkih vještina u kompanijama, jer su primijetili da velikim kompanijama koje posluju u više država često nedostaje osoblje koje posjeduje jezičke i pravne vještine relevantne za svaku državu u kojoj posluju.

- Pružaocima internet usluga nije uvijek jasno koje su nacionalne agencije odgovorne za određene odluke, npr. uklanjanje nezakonitog sadržaja. Slovački nadležni organi su predložili da se uvede uloga „pouzdanog čuvara sadržaja", odnosno da se identificiraju određene agencije koje imaju zadatak da se povezuju s međunarodnim pružaocima usluga kako bi uklonili sadržaje i postupali po drugim zakonskim odredbama. Pouzdani čuvar sadržaja bi imao otvoren kanal komunikacije s kompanijama i izgradio bi uzajamno povjerenje.

Nekoliko država, uključujući Kipar, Irsku, Litvu, Luksemburg, Maltu, Holandiju i Ujedinjeno Kraljevstvo, navelo je da su pružaoci internet usluga, pružaoci sadržaja i kompanije društvenih medija generalno sarađivali kada se radi o pitanjima koja su vezana za trgovinu ljudima i seksualnu eksploataciju djece. Međutim, britanski nadležni organi su istakli potrebu da se napravi korak dalje i sarađuje s online kompanijama „na **osmišljavanju mogućnosti** za trgovinu ljudima na njihovim web-lokacijama i radu u saradnji s organima za provođenje zakona kako bi se spriječila pojava trgovine ljudima".

Kiparski nadležni organi su naveli korištenje platforme Sirius za olakšavanje prekograničnog pristupa elektronskim dokazima koji vodi Europol kao primjer dobre prakse. Takva platforma daje agencijama za provođenje zakona mogućnost da direktno komuniciraju s privatnim kompanijama radi čuvanja i objelodanjivanja podataka. Ovo su istakli i francuski nadležni organi (Projekat E-Evidence).

2.5. Dokazi prikupljeni od nevladinih organizacija

Pored dokaza prikupljenih od država ugovornica, u okviru studije se od nevladinih organizacija koje pružaju pomoć žrtvama tražilo da ukažu na izazove koje primjećuju u kontekstu trgovine ljudima posredstvom tehnologije.

2.5.1. Izazovi tokom identifikacije i istrage

Sve u svemu, dokazi prikupljeni od nevladinih organizacija su u skladu s izazovima koje su navele države ugovornice i o kojima je bilo riječi ranije u ovom poglavlju. Konkretnije, NVO su istakle sljedeći skup faktora koji ometaju otkrivanje trgovine ljudima posredstvom tehnologije i naknadne istrage:

- Nedostatak kapaciteta među organima za provođenje zakona, uključujući nedostatak obuke, hardvera i softvera, kao i ograničenu upotrebu specijalnih istražnih tehnika. Neke NVO su primijetile nedostatak specijalizacije policije i pravosuđa u pogledu trgovine ljudima u vezi s tehnologijom, kao i nedostatak kapaciteta u oblasti velikih količina podataka. Međutim, alati za „struganje" interneta koje je isprobala organizacija Hope Now (Danska) u periodu 2016–

2018. postigli su skromne rezultate.

- Tehnološko okruženje koje se brzo mijenja, kao i modus operandi počinilaca. Profesionalcima je teško pratiti korak s trgovinom ljudima posredstvom tehnologije, što ometa njihovu sposobnost da brzo identificiraju slučajeve i pokreću istrage. Znanje o tehničkom okruženju i praksama često se ne razmjenjuje (npr. među organima za provođenje zakona, privatnim kompanijama, NVO, akademskom zajednicom).

- Korištenje privatnih foruma, chat soba ili šifriranih aplikacija za kontakte između počinilaca i žrtava. Ovo otežava (a) otkrivanje takvih kontakata i (b) njihovo pribavljanje kao dokaza koji će se koristiti na sudu. NVO su predložile navođenje informacija/upozorenja o sigurnom korištenju privatnih kanala komunikacije.

- Poteškoće u razotkrivanju anonimnih počinilaca tokom emitiranja eksploatacije uživo putem interneta, kao i poteškoće u prikupljanju dokaza o takvim zlostavljanjima, osim ako se ne naprave snimci ekrana predmetnih videosnimaka.

- Profesionalci smatraju da je teško utvrditi da li osoba koja stoji iza online profila/oglasa dobrovoljno pruža navedene usluge na osnovu javno dostupnih informacija (npr. u slučaju online oglasa za seksualne usluge). To je zato što počinioci mogu kreirati i upravljati online profilima u ime svojih žrtava. Štaviše, počiniocima je lako ponovo kreirati profile kada im se zabrani pristup.

- Pravila o zaštiti podataka i privatnosti mogu ometati identifikaciju žrtava, kao i trgovaca ljudima. Pravila GDPR-a ograničavaju upotrebu tehnologije za otkrivanje digitalnih tragova koje ostavljaju i žrtve i počinioci (na društvenim medijima, na internetu, ali i u vezi s finansijskim računima). Nedostaje sveobuhvatna analiza digitalnih tragova usredsređena na žrtve, uključujući, naprimjer, nekretnine, bankovne račune, transakcije na bankomatima, transakcije kreditnim karticama i medicinske kartone, kako bi se olakšala istraga.

- Nedostatak interdisciplinarne tehnološke saradnje između privatnih kompanija, javnih agencija i NVO kako bi se u potpunosti iskoristila sve veća količina podataka o trgovini ljudima. Fondacija Sustainable Rescue Foundation je navela sljedeće faktore koji ometaju međusektorsku saradnju u pogledu razmjene podataka:
    - nezavisni centri ne uspijevaju privući agencije za provođenje zakona ili vladu;
    - nedostatak tehnološke strategije u nacionalnim akcionim planovima za borbu protiv trgovine ljudima;
    - IT grupe pri organima za provođenje zakona koje nemaju kapacitet ili budžet za pravovremeni razvoj, testiranje, implementaciju, obuku, ažuriranje i održavanje aplikacija za otkrivanje trgovine ljudima;
    - poteškoće oko dijeljenja podataka o žrtvama;
    - komercijalni interesi.

- Ograničene istrage finansijskih institucija o trgovini ljudima. Mogućnosti identifikacije na osnovu podataka iz sistema Upoznaj svog klijenta (KYC) ne koriste se zbog nedostatka obuke i svijesti o trgovini ljudima, kao i zbog složenosti sistema prijavljivanja (kvalitet upozorenja, veoma veliki broj lažno pozitivnih prijava, dugo vrijeme potrebno za odgovor itd.)

- Nedostatak ulaganja u sposobnosti vještačke inteligencije (AI) i korištenje mašinskog učenja za operacije, predviđanje i prevenciju. Fondacija Sustainable Rescue Foundation je ukazala na upotrebu mašinskog učenja u medicinskom sektoru kao naprimjer gdje se

„informacije dijele između klinika, bolnica, ljekara i akademske zajednice bez kršenja zakona o privatnosti. Ovo se postiže korištenjem načela FAIR pri pregledu podataka (engleski akronim dobijen od termina: vidljivi, pristupačni, interoperabilni, ponovo upotrebljivi) za podudaranje metapodataka i vanjskog učenja za dubinsku analizu iz različitih izvora". Također su istakli da „trenutno nije u toku takvo ulaganje ili takva strategija u organizacijama za trgovinu ljudima".

- Nedostatak razmjene podataka između različitih subjekata na lokalnom, regionalnom, nacionalnom ili međunarodnom nivou zbog nedostatka operativnih sposobnosti u okviru organa za provođenje zakona i ograničenja utvrđenih nacionalnim zakonodavstvom. Pored toga, podaci se često prikupljaju u nestrukturiranom obliku, što otežava razmjenu i dalju analizu dokaza.

- NVO koje pružaju direktnu podršku žrtvama trgovine ljudima, putem online platformi, chat konsultacija i telefonskih linija za pomoć, nemaju kapacitete, resurse i tehničke alate da redovno otkrivaju online eksploataciju koja se vrši posredstvom tehnologije.

- Nedostatak svijesti o rizicima i potencijalnim posljedicama u vezi s upotrebom tehnologije među ljudima koji su u opasnosti od trgovine ljudima. Ovo je naročito akutno kod djece i mladih. Općenito govoreći, postoji nedostatak svijesti u široj javnosti o trgovini ljudima posredstvom tehnologije, što dovodi do nedovoljnog prijavljivanja.

2.5.2. Izazovi saradnje s organima za provođenje zakona

Sve NVO prijavljuju neki oblik saradnje s agencijama za provođenje zakona, uključujući signaliziranje slučajeva trgovine ljudima ili pružanje pomoći žrtvama na zahtjev nadležnih organa. Kada je riječ o njihovoj saradnji s organima za provođenje zakona, NVO su istakle sljedeće izazove:

- Suprotstavljeni ciljevi ili različiti pristupi između nevladinih organizacija i organa za provođenje zakona, uključujući odluke o tome da li slučaj treba dalje istraživati.

- Pitanja koja se tiču zaštite i privatnosti podataka.

- Nedostatak povratnih informacija o slučajevima koje su NVO prijavile nadležnim organima.

- Nedostatak resursa za podršku saradnji između organa za provođenje zakona i nevladinih organizacija (ovo je istaknuto i u vezi s inovativnim „terenskim laboratorijama" uspostavljenim u Holandiji, u čijim odborima je fondacija Sustainable Rescue Foundation).

- Kada je riječ o djeci, postoji nedostatak obuke među organima za provođenje zakona o tome kako da pristupe maloljetnim žrtvama i da ih ubijede da sarađuju tokom istrage. La Strada Moldova je istakla da istrage koje uključuju djecu imaju dodatnu složenost kada je riječ o upravljanju dokazima, jer „djeca obično osjećaju krivicu, prijekor ili stid zbog onoga što im se desilo, ne sarađuju, ne žele da roditelji saznaju šta im se desilo ili da druge osobe vide njihove seksualno eksplicitne videomaterijale. U strahu, mnoga od njih odbijaju podnijeti pritužbu", čime onemogućavaju dalju istragu agencija za provođenje zakona.

2.6. Tehnološke kompanije

Kompanija Facebook je navela da korisnici „rijetko prijavljuju" sadržaje koji se odnose na trgovinu ljudima. Kompanija je dalje primijetila da nedovoljno prijavljivanje može biti posljedica brojnih faktora, uključujući: (a) žrtve trgovine ljudima možda nemaju slobodu da prijave ili možda nisu svjesne svojih uvjeta eksploatacije; (b) kupci usluga koje pruža žrtva trgovine ljudima možda nisu svjesni da kupuju uslugu od žrtve trgovine ljudima ili su odvraćeni od prijavljivanja „jer žele iskoristiti nedozvoljene ili znatno jeftinije usluge koje se pružaju eksploatacijom". U drugim slučajevima, primjećuje se da „za određene oblike trgovine ljudima, kao što je kućno ropstvo, pošto to može biti općeprihvaćena pojava u nekim regionima, posmatrači ne shvataju da mogu ili da trebaju prijaviti ovakve sadržaje".

Što se tiče izazova za saradnju s organima za provođenje zakona, IBM je primijetio da postoji „određeni broj prepreka"; prije svega, istakao je „zabrinutost u pogledu zakonitosti takve saradnje, naročito u vezi s pitanjima privatnosti podataka i pravnom složenošću situacije u kojoj nadležnost ima više država". IBM je pozvao na „pojašnjenja o međunarodnim pravnim dozvolama za prikupljanje i dijeljenje podataka (s ovlaštenim organima za provođenje zakona)". Facebook je naveo da prekogranična priroda eksploatacije ljudi „predstavlja izazov". Naprimjer, napomenuo je da se počinioci mogu nalaziti u drugoj državi od one u kojoj se nalaze žrtve trgovine ljudima i zlostavljane osobe: shodno tome, „više država može biti nadležno za vođenje istrage protiv kriminalne mreže. Koordinacija između organa za provođenje zakona u EU i šire dodaje dodatnu složenost naporima u borbi protiv trgovine ljudima".

2.7. Dodatni dokazi prikupljeni na osnovu analize okruženja

Pored dokaza koje su pružile države ugovornice, NVO i tehnološke kompanije, u okviru studije je također provedeno uredsko istraživanje dostupne baze dokaza o izazovima u vezi s otkrivanjem, istragom i krivičnim gonjenjem slučajeva trgovine ljudima posredstvom interneta i tehnologije.

Od posebnog interesa su dokazi koji se odnose na izazove pri **identifikaciji oglasa za posao povezanih s trgovinom ljudima**. Predloženo je da bi identifikacija oglasa, a ne žrtava, mogla predstavljati dobar način da se iskoristi tehnologija: ovo seže do podsticajnih radova VE (2007) i projekta Fine Tune (2011). Projekat Fine Tune (2011) ponudio je preliminarnu listu **znakova upozorenja u kontekstu radne eksploatacije**. To uključuje: (a) nerealno visoke plaće za nekvalificirane poslove; (b) opise poslova bez detalja, uključujući opis uloge, lokacije, mjesta rada i dnevnog radnog vremena; (c) odsustvo adrese kompanije ili agencije koja zapošljava; i (d) odsustvo kontakt-podataka osim broja telefona ili generičke adrese e-pošte. Međutim, dokazi ukazuju da je identifikacija pravih pozitivnih slučajeva (tj. oglasa u vezi s trgovinom ljudima) i dalje veoma izazovna. Nekoliko autora je ukazalo na **poteškoće u sortiranju** pravih oglasa od onih koji se odnose na trgovinu ljudima, uprkos naporima uloženim u razvoj **indikatora potencijalnog rizika** (kao i ponovnom tumačenju općih indikatora UNODC-a i MOR-a kako bi se prilagodili online kontekstu: Di Nicola i drugi 2017; Raets i Janssens 2018; Volodko i drugi 2019):

a. U skupu od 430 litvanskih online oglasa za posao koje su analizirali Volodko i drugi (2019), 98,4% sadržavalo je najmanje jedan indikator trgovine ljudima, što ukazuje na to da su takvi indikatori često uobičajena karakteristika tržišta rada s niskim kvalifikacijama. Određeni nivo nade, međutim, potječe iz nalaza da je samo 15% oglasa sadržavalo više od

pet indikatora što ukazuje na to da bi se uz dalje usavršavanje i odgovarajuće analitičke tehnike neke strategije za smanjenje štete mogle efikasno primijeniti.

b. Pored usavršavanja dostupnog skupa znakova upozorenja (i njihovog stalnog ažuriranja, što predstavlja dodatni izazov), kao potencijalni put naprijed predloženi su računarski pristupi zasnovani na „struganju" interneta, obrada prirodnog jezika, prepoznavanje subjekata i „oznaka" i općenito tehnike mašinskog učenja (Volodko i drugi 2019, između ostalih; također vidjeti UN Delta 8.7). Iako potencijalno obećava, ovaj put otvara nove izazove, uključujući: (1) potrebu da se utvrdi „osnovna istina" za modele, što se može postići samo kroz blisku saradnju između agencija za provođenje zakona i privatnog sektora; (2) potrebu da se iskoristi znanje iz privatnog sektora, pošto agencije za provođenje zakona interno jedva da imaju potrebne vještine; (3) potrebu da se pažljivo procijene etička pitanja u vezi s tehnikama mašinskog učenja velikih razmjera; i (4) potencijal za diskriminatorne prakse, kao i pitanja zaštite podataka i razmjene informacija između različitih subjekata.

U nekim slučajevima, oglasi za posao u modelingu, zabavi i – u nekim državama – seksualnim uslugama u inostranstvu mogu se koristiti za regrutiranje pojedinaca koji potom bivaju primorani na seksualnu eksploataciju. Predloženo je nekoliko znakova upozorenja kako bi se oglasi u vezi s trgovinom ljudima odvojili od legitimnih oglasa, uključujući oglase koji su: (a) loše napisani i nejasni; (b) previše obećavaju; (c) preširoki su; (d) ne navode državu odredišta (upućuju na „egzotične destinacije"); i (e) ne sadrže puno ime kontakt-osobe, agencije za zapošljavanje i/ili kompanije koja bi zaposlila uspješnog kandidata (Di Nicola i drugi 2017). Međutim, preliminarni pokušaji da se pregledaju javno dostupni dokazi korištenjem ovih kriterija još jednom su ukazali na poteškoće u odvajanju oglasa povezanih s trgovinom ljudima od lažno pozitivnih oglasa.

Otkrivanje slučajeva seksualne eksploatacije na osnovu **online oglasa za seksualne usluge** podjednako je izazovno, tj. razvrstavanje seksualnih usluga koje pružaju žrtve trgovine ljudima od onih koje pojedinci dobrovoljno pružaju na osnovu jedinstvenog teksta i vizuelnih prikaza uključenih u oglas. Predloženi su neki indikatori eksploatacije, uključujući neslaganja između opisa profila, slika i lokacija; takva neslaganja se također mogu unakrsno provjeriti na više web-lokacija (Di Nicola i drugi 2017). Pokazalo se da brojevi telefona igraju ključnu ulogu, naprimjer, u otkrivanju prisustva istog broja telefona u oglasima, na web-lokacijama i objavama koje se pripisuju različitim osobama (potencijalan znak upozorenja). Predloženo je da se prepoznavanje lica može koristiti kao tehnika za uočavanje nedosljednosti i znakova upozorenja, slično pristupu usvojenom u otkrivenim seksualnim materijalima koji prikazuju maloljetnike (Raets i Janssens 2018).

Međutim, preliminarni pokušaji da se proširi gore navedena strategija otkrivanja ukazali su na jasne izazove. U svojim pokušajima da identificiraju žrtve seksualne trgovine u SAD-u putem online oglasa za poslovnu pratnju, Ibanez i Ganzan (2014, 2016a i 2016b) koristili su brojeve telefona i indikatore kretanja, ali nisu dali jake rezultate. Pored toga, neki od indikatora koje su naveli Ibanez i Gazan 2014. prilično su zbunjujući i možda uopće ne ukazuju na trgovinu ljudima; u nekim slučajevima, mogu čak ukazivati na suprotnu situaciju.

3. Strategije i dobre prakse

Nakon razmatranja izazova, studija se sada okreće istraživanju strategija koje su države ugovornice razvile za otkrivanje i istragu trgovine ljudima posredstvom interneta i tehnologije, za njegovanje međunarodne saradnje i za identifikaciju i pomoć žrtvama. Zatim slijedi diskusija o dokazima koje su pružile NVO i tehnološke kompanije o istim problemima.

3.1. Otkrivanje slučajeva trgovine ljudima posredstvom IKT-a

3.1.1. Opće strategije

Države su navele da primjenjuju različite strategije za otkrivanje slučajeva trgovine ljudima posredstvom interneta i IKT-a. Često se navodi strategija **nadgledanja interneta**, uključujući foruma i, u nekim slučajevima, TOR mreže (mračne mreže). Ovo se često kombinira s upotrebom **obavještajnih podataka iz otvorenih izvora (OSINT)**, veoma čestom istražnom strategijom koja podrazumijeva prikupljanje podataka s društvenih medija i iz drugih javno dostupnih online izvora o mreži kontakata određenog pojedinca, njegovim životnim uvjetima i finansijskoj situaciji. OSINT se može koristiti „proaktivno", npr. za otkrivanje potencijalnih slučajeva trgovine ljudima, za identifikaciju potencijalnih počinilaca i žrtava ili za pribavljanje svježih informacija. Neke države su formirale **„cyber patrole" sa specijaliziranim službenicima** zaduženim za provođenje OSINT istraga na internetu. Neke države dozvoljavaju tajne istrage na internetu (cyber infiltracija). U Holandiji specijalizirani istražitelji s „**digitalnim znanjem**" mogu biti angažirani u istragama trgovine ljudima kako bi prikupili online dokaze o trgovini ljudima. Finski nadležni organi su ukazali na nedavno uspostavljanje podjedinice za borbu protiv trgovine ljudima na internetu u okviru Nacionalnog istražnog tima (također su prijavili prisustvo ogranka za online obavještajnu djelatnost koji radi na internetu, uključujući mračnu mrežu).

Vezano za OSINT istrage, države navode da koriste **tehnike analize društvenih mreža** kako bi se razumjele i rekonstruirale mreže kontakata počinioca i/ili žrtve. Primjera radi, ako je žrtva A povezana s osobom koja vrši regrutiranje B, onda se mogu procijeniti svi kontakti osobe koja vrši regrutiranje B kako bi se identificirale potencijalne žrtve. **Informacije o povezanostima** su ključne i sve više ih koriste policijski organi kroz takozvanu „analizu veza" ili sofisticiranije tehnike „analize društvenih mreža".

Dodatne **proaktivne strategije** uključuju upotrebu tehnoloških alata za traženje dokaza na mreži (npr. sistemi za skeniranje mreže, vidjeti također u nastavku) i strateške istrage o modusu operandiju počinilaca u oblasti trgovine ljudima u pogledu IKT-a. Generiranje – i ažuriranje – ovakvog strateškog (šireg) znanja o toj pojavi može pružiti informacije za holistički pristup, kao i za specifične, usmjerenije istrage. Međutim, nisu sve države ugovornice navele da koriste „strategije". Nekoliko država ugovornica je izričito navelo da njihove istrage o trgovini ljudima posredstvom IKT-a ostaju „reaktivne".

Nadležni organi su prijavili uspostavljanje direktnog kontakta s pružaocima online usluga kako bi se identificirali slučajevi trgovine ljudima posredstvom IKT-a. U državama u kojima je oglašavanje seksualnih usluga na mreži zakonito nadležni organi mogu „izvršiti ciljano filtriranje telefonskih brojeva i [analizu] korisničkih podataka povezanih s [pretpostavljenim] počiniocima" (prijava iz Mađarske). Kantonalne policijske snage u Švicarskoj vrše „ciljane provjere" online oglasa za seksualne usluge kako bi se otkrile potencijalne žrtve trgovine

ljudima.

Neke agencije za provođenje zakona u Ujedinjenom Kraljevstvu koriste **alate za „struganje" interneta** posebno razvijene za izdvajanje informacija s web-lokacija kako bi identificirale rizike i ranjivosti na web-lokacijama za usluge za odrasle (ASW). Britanske policijske snage vrše pregledanje web-lokacija za ASW kako bi prikupile podatke koji se potom koriste za analizu aktivnosti na ASW i potencijalno pretvaranje ovih podataka u obavještajne podatke po kojima se može djelovati.

Nekoliko država je navelo dostupnost **mehanizma za korisnike interneta da prijave sadržaje i web-lokacije** za koje sumnjaju da su povezani s nezakonitim aktivnostima, uključujući seksualnu i radnu eksploataciju (vidjeti u nastavku za više primjera).

3.1.2. Strategije specifične za određenu državu

Kako bismo dalje istražili različite strategije koje su države razvile za borbu protiv zloupotrebe interneta, uključujući online oglase za posao, u kontekstu trgovine ljudima posredstvom tehnologije, sada donosimo kratak pregled mehanizama i inicijativa specifičnih za određenu zemlju. Takve strategije treba čitati zajedno s dobrim praksama o kojima se govori u sljedećem odjeljku, kao i s raspravom o nacionalnim pravnim okvirima koji se odnose na identifikaciju i uklanjanje internetskog sadržaja u vezi s trgovinom ljudima koji su uključeni u Web-prilog. U Albaniji postoji **mehanizam dozvola** u vezi s online oglasima za posao, a njih izdaju/kontroliraju institucije (koje nisu navedene u prijavi).

Austrijski nadležni organi intenzivirali su proaktivne pretrage na različitim online platformama od izbijanja pandemije COVID-19 kako bi identificirali žrtve i počinioce trgovine ljudima koristeći **posebne softverske tehnologije** (npr. sisteme za skeniranje mreže radi prikupljanja podataka), **službenike specijalizirane za obavještajne podatke iz otvorenih izvora** (OSINT), kao i **tajne agente** (tajne istrage na internetu). Aktivnosti zajednički provode istražitelji za trgovinu ljudima i službenici specijalizirani za IT. Vjeruje se da bi ovaj model mogao ponuditi šablon za buduće istrage.

Belgijski nadležni organi naveli su da trenutni „abolicionistički model" usvojen u vezi s prostitucijom onemogućava zaključivanje ugovora s web-lokacijama koje objavljuju oglase za seksualne usluge. Ovo se smatra „ograničenjem" postojećeg zakonodavstva. NVO „Child focus" trenutno razvija kampanju za podizanje svijesti za klijente koji koriste web-lokacije na kojima se objavljuju oglasi za seksualne usluge, kako bi bili obaviješteni o riziku da naiđu na maloljetnu osobu. Ova kampanja se provodi u saradnji s predmetnim web-lokacijama.

Hrvatski nadležni organi su prijavili da vrše **provjere profila na društvenim mrežama** pojedinaca koji su povezani s konkretnim krivičnim istragama, npr. istragama seksualnog zlostavljanja i seksualne eksploatacije djece, kako bi se identificirale potencijalne žrtve i osobe koje vrše regrutiranje. Takve provjere vrše specijalizirani službenici za visokotehnološki kriminal.

Na Kipru postoje kampanje za podizanje svijesti koje organizira Odjeljenje za visokotehnološki kriminal (CCD), a koje su namijenjene školskoj deci i njihovim roditeljima kao dio Nacionalne strategije za bolji internet za djecu. Od 2014. godine CCD također vodi platformu za prijavljivanje visokotehnološkog kriminala (www.cyberalert.cy).

U Estoniji građani mogu kontaktirati „**web-službenike**" kako bi prijavili sadržaj društvenih medija koji je potencijalno povezan s nezakonitim aktivnostima, uključujući trgovinu ljudima.

Francuski zakon dozvoljava istražiteljima da se **cyber infiltriraju u kriminalne mreže.** Agencije za provođenje zakona zapošljavaju istražitelje za cyber patroliranje internetom kako bi **otkrile oglase i identificirale kriminalne mreže.** Operacije ciljanog nadzora na određenim internetskim forumima se također provode, uz korištenje tehnika tajne istrage gdje je to potrebno. Istražitelji također koriste internetske oglase za unakrsnu provjeru geografskih podataka prikupljenih preko drugih izvora kako bi identificirali mjesta koja se koriste za trgovinu ljudima. Informacije prikupljene iz različitih izvora se sistematiziraju i koriste za **rekonstrukciju kriminalnih mreža, odnosno odnosa između određenih mjesta, počinilaca i žrtava**. Pored toga, francuske agencije za provođenje zakona rade na uspostavljanju **protokola saradnje** s kompanijama koje upravljaju društvenim mrežama i online privatnim platformama za iznajmljivanje kako bi podstakle pružanje informacija. Pošto pružaoci internetskog sadržaja mogu u nekim slučajevima biti preopterećeni obimom zahtjeva za prijenos informacija i dostavljanje dokaza, nadležni organi su predložili da se **osmisle direktnije – i pojednostavljene – procedure koje podržavaju saradnju** između pružalaca sadržaja i organa za provođenje zakona. Naprimjer, „Wannonce", francuska stranica koja se koristi za oglase povezane s maloljetnom prostitucijom, šalje organima za provođenje zakona vezu koja omogućava direktnu pretragu u njihovoj bazi podataka nakon dostavljanja adrese e-pošte. Konačno, član 6(I)(7) Zakona br. 2004-575 od 21. juna 2004. godine o „Povjerenju u digitalnu ekonomiju" (LCEN) zahtijeva od pružalaca pristupa internetu i hostova web-lokacija da pomognu u borbi protiv širenja materijala koji se odnose na određena krivična djela, uključujući trgovinu ljudima. Od njih se zahtijeva da postave lako dostupan i vidljiv mehanizam koji omogućava svakoj osobi da označi sumnjivi materijal. Kompanije su također dužne blagovremeno obavijestiti javne organe o svim nedozvoljenim radnjama koje su im prijavljene i koje provode korisnici njihovih usluga. Građani mogu prijaviti nezakonite sadržaje na internetu policiji i žandarmeriji putem web-lokacije (www.internet-signalement.gouv.fr). Prijavljeni sadržaj ispituje PHAROS (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements), specijalizirana policijska jedinica.

U Finskoj služba za zaštitu djece i telefonska linija za prijavu (Nettivihje) nude način za prijavu online materijala za seksualno zlostavljanje djece i trgovinu djecom. Nettivihje blisko sarađuje s Nacionalnim istražnim biroom i njegovim timom specijaliziranim za seksualne zločine. Finska policija također ima online mehanizam za prijavu sumnjivih aktivnosti na internetu, uključujući materijale potencijalno povezane sa seksualnim prijestupima nad djecom. Ovaj obrazac se potencijalno može proširiti izvan domena seksualne eksploatacije djece.

U Njemačkoj policija je (u maju 2020. g.) počela koristiti **alat za automatsko pretraživanje** za analizu velike količine podataka koji su objavljeni na web-lokacijama za oglase za odrasle. Alat za pretraživanje strukturira podatke kako bi pomogao u izdvajanju relevantnih informacija. Ovo se postiže u kombinaciji s upotrebom specifičnih indikatora. Nadležni organi smatraju da je upotreba ovog automatiziranog alata „veoma korisna".

Grčki nadležni organi spominju **praćenje web-lokacija i foruma koji objavljuju oglase za posao** ili usluge kako bi otkrili slučajeve trgovine ljudima na internetu. Ovo se postiže kroz blisku saradnju između Jedinica za borbu protiv trgovine ljudima Policije Grčke i Odjeljenja za visokotehnološki kriminal. Pored toga, Odjeljenje za visokotehnološki kriminal Policije Grčke razvilo je aktivnosti za podizanje svijesti i edukaciju koje se fokusiraju na odgovornu upotrebu novih tehnologija i rizike na internetu, naprimjer, „Seminari za dan sigurnog surfanja" i web-lokacija i aplikacija „Cyberkid", koja služi za informiranje učenika, roditelja i nastavnika o

nasilju na internetu i rizicima s kojima se oni mogu suočiti na web-lokacijama društvenih mreža.

NVO „Smile of the Child" redovno organizira događaje na Dan sigurnog interneta (9. februar).

Na Islandu policija Rejkjavika održava takozvane „**sedmice interneta**", tokom kojih pregleda popularne web-lokacije koje reklamiraju seksualne usluge u potrazi za slučajevima trgovine ljudima. U slučaju sumnjivih aktivnosti, policija traži sudski nalog za prisluškivanje telefonskih brojeva navedenih u oglasima i pokretanje istrage.

U Irskoj Jedinica za koordinaciju i istragu trgovine ljudima An Garda Síochána (irske policije) udružuje snage s različitim društvenim medijima i kompanijama za zapošljavanje kako bi podigla svijest o potencijalnim oglasima za posao koji su povezani s trgovinom ljudima. Irske i neke međunarodne IKT kompanije obično sarađuju kada An Garda Síochána zatraži uklanjanje sadržaja s interneta za koji se smatra da je nezakonit.

U Latviji postoji zvanična web-lokacija za oglase za posao koju vodi Državna agencija za zapošljavanje. Web-lokacija nastoji spriječiti slučajeve radne eksploatacije **nudeći siguran prostor za oglašavanje.**

U Republici Moldaviji trenutno ne postoje posebni automatizirani mehanizmi za identifikaciju oglasa i sadržaja na internetu koji su potencijalno povezani s trgovinom ljudima, a nadležni organi trenutno sarađuju s Holandijom na nabavci sistema za skeniranje mreže koji su razvili holandski organi za provođenje zakona.

U Holandiji **policija može postaviti lažne profile na internetu** (lokprofiel) kako bi identificirala – a zatim istražila – slučajeve trgovine ljudima i počinioce. Pored toga, Ministarstvo pravde i sigurnosti trenutno istražuje ulogu tehnologije u svim fazama trgovine ljudima kroz stručne sastanke i istraživanja koja se provode u saradnji s Centrom za borbu protiv eksploatacije djece i trgovine ljudima (CKM).

U Norveškoj Centar za visokotehnološki kriminal trenutno razvija **bazu podataka o seksualnim oglasima na internetu** koji su objavljeni na lokalnoj web-lokaciji. Takve informacije će pružiti osnovu za dalju analizu.

U Sloveniji je 2005. godine osnovan Centar za sigurniji internet kako bi se podigla svijest i pomoglo u otkrivanju nezakonitih sadržaja na internetu. Centar nudi tri glavne usluge: (a) **centar za podizanje svijesti** o odgovornom korištenju interneta i novih tehnologija (Safe.si), koji ima za cilj da djeci, tinejdžerima, roditeljima, nastavnicima i socijalnim radnicima pruži online/offline aktivnosti, obrazovanje, radionice, sadržaje, kampanje za podizanje svijesti; (b) telefonsku liniju za pomoć djeci, mladima i roditeljima (također poznatu kao „Tom telefon") s profesionalnim savjetnicima koji nude savjete o sigurnosti na internetu, također i putem **sobe za chat na internetu**; (c) anonimno online prijavljivanje nezakonitog sadržaja na internetu.

U Španiji nadležni organi koriste **praćenje društvenih medija** posredstvom cyber patrola koje su fokusirane na otkrivanje žrtava trgovine ljudima. Ove aktivnosti provodi Centralna istražna jedinica Guardia Civil specijalizirana za trgovinu ljudima, a same aktivnosti su intenzivirane tokom pandemije COVID-19. Policía National je također nedavno osnovala istražnu grupu specijaliziranu za slučajeve trgovine ljudima na internetu (Operativna grupa VI za borbu protiv cyber trgovine ljudima s Centralnom brigadom Policía Nacional za borbu protiv trgovine ljudima).

U Švedskoj policija vrši **redovan nadzor web-lokacija** koje oglašavaju aktivnosti prostitucije kako bi se identificirali mjesto i vrijeme takvih aktivnosti (prema švedskom zakonu, sve kupovine seksualnih usluga su nezakonite).

U Švicarskoj neke kantonalne policijske snage koriste **tajne istrage za provjeru oglasa** na web-lokacijama za odrasle, kao i pojedince koji su uključeni u otkrivanje slučajeva trgovine ljudima.

U Ujedinjenom Kraljevstvu Agencija za borbu protiv zlostavljanja na radu i organiziranog kriminala, zajedno s organizacijom Crimestoppers, koristila je Facebook da informira tražioce posla o lažnom oglašavanju poslova na društvenim medijima. Tim je **kreirao oglase za posao na mreži Facebook** koji su pružali hipervezu ka web-lokaciji organizacije Crimestoppers, koja je zauzvrat pružala informacije o indikatorima rizika pri traženju posla u građevinskoj industriji. Kampanja je bila usmjerena na Rumune starosti od 18 do 34 godine i dosegla je preko 900.000 ljudi. Došlo je do povećanja od 13% u prijavama koje se odnose na trgovinu ljudima i od 400% u prijavama o trgovini ljudima koje se odnose na žrtve iz Rumunije. U okviru višeagencijskog pristupa (projekt AIDANT) koji okuplja Nacionalnu agenciju za borbu protiv kriminala, granične snage, imigracijske službe, Poresku službu i carinu Njenog Veličanstva, Agenciju za borbu protiv zlostavljanja na radu i organiziranog kriminala i policijske snage, nadležni organi **smišljaju i testiraju nove metodologije za prijavljivanje u industriji**. Jedinica NCA za borbu protiv trgovine ljudima u svrhu modernog ropstva (MSHTU) radi na podizanju standarda na web-lokacijama za usluge za odrasle (ASW) tako što poboljšava način na koji kompanije identificiraju trgovinu ljudima i eksploataciju na svojim platformama i prijavljuju to organima za provođenje zakona. Policijske snage također koriste automatizirane istraživačke procedure iz otvorenih izvora za prikupljanje informacija iz oglasa na web-lokacijama za usluge za odrasle (ASW). Britanski nadležni organi smatraju da je gašenje ASW-a rizično, jer vjerovatno neće dovesti do eliminacije potražnje, ali bi umjesto toga dovelo do izmještanja oglašavanja na druge platforme na štetu žrtava trgovine ljudima i dobrobiti seksualnih radnika. Pored toga, razvijena je aplikacija Farm Work Welfare s ciljem da se dopre do sezonskih radnika i poslodavaca u sektoru poljoprivrede i proizvodnje hrane, a postavljena je i glasovna shema za radnike (SAFERjobs, www.safer-jobs.com) koja omogućava transparentnost lanaca snabdijevanja i prikupljanje obavještajnih podataka o zloupotrebama na tržištu rada. Protiv organizacija za koje se utvrdi da ne poštuju propise izriču se izvršne mjere i šalju se poruke njihovim krajnjim korisnicima kako bi se podigla njihova svijest, što bi potencijalno dovelo do gubitka posla (strategija „imenuj i osramoti").

U Ukrajini su nadležni organi počeli blokirati online kanale na Telegramu koji šire informacije o seksualnoj eksploataciji.

3.2. Istraga slučajeva trgovine ljudima posredstvom IKT-a

Ovaj odjeljak istražuje strategije i dobre prakse koje su osmislile države ugovornice kako bi povećale efikasnost istraga o trgovini ljudima posredstvom IKT-a (takve strategije i dobre prakse treba čitati zajedno sa strategijama koje se odnose na identifikaciju slučajeva o kojima je bilo riječi iznad jer identifikacija i istraga mogu biti usko povezane).

Nekoliko država je istaklo značaj **stalnog organiziranja obuka i razvojnih aktivnosti zasnovanih na najboljim lokalnim i globalnim praksama** za službenike za provođenje zakona. Uspostavljanje i obuka specijaliziranih jedinica za borbu protiv trgovine ljudima posredstvom IKT-a spominje se kao važna strategija. Općenito govoreći, mnoge države

ugovornice smatraju da je **ulaganje u ljudski kapital** jednako ključno kao ulaganje u tehnološku opremu. Među specijaliziranim profilima koje su države identificirale kao ključne za efikasno istraživanje trgovine ljudima posredstvom IKT-a postoje službenici specijalizirani za „nove tehnologije", „operativni kriminalistički analitičar", „tajne istrage" i „istražitelji podataka iz otvorenih izvora – OSINT" (oznake su one navedene u francuskoj prijavi, ali druge države su ukazale na slične profile). Kao što su grčki nadležni organi primijetili, treba osigurati obuku ne samo o tome kako se koriste tehnološki alati već i o „njihovom etičkom korištenju u pogledu poštovanja ljudskih prava i zaštite podataka" (više o obuci navedeno je u sljedećem poglavlju).

Način na koji se obuka trenutno provodi razlikuje se od države do države. Jedan model je da se nacionalnim centrima za visokotehnološki kriminal, tamo gdje su uspostavljeni, povjeri zadatak razvoja alata i tehnika te stjecanja povezanih znanja, a zatim i zadatak širenja ovog znanja među policijskim jedinicama i/ili nuđenja pomoći integracijom drugih specijaliziranih jedinica, npr. jedinice za borbu protiv trgovine ljudima. Jasno je da je znanje o „naprednim istragama i analizi računarske tehnologije, uključujući sigurnost tragova i dokaza s digitalnih uređaja, IKT sistema i od pružalaca internetskih usluga", ključna prednost (norveška prijava). Nekoliko država (ali ne sve) navelo je da imaju posebnu jedinicu koja se bavi kriminalom s velikom tehnološkom komponentom, npr. jedinice/centre za cyber kriminal ili jedinice za visokotehnološki kriminal. Druge policijske jedinice, npr. specijalizirane jedinice za borbu protiv trgovine ljudima, mogu tražiti pomoć od takvih jedinica.

Nekoliko država je primijetilo značaj uključivanja specijaliziranih istražnih službenika s „**digitalnim znanjem**" u istrage slučajeva trgovine ljudima. Takvi službenici se mogu angažirati da traže tragove trgovine ljudima na internetu. Jedan operativni model koji su predložili francuski nadležni organi podrazumijevao bi prisustvo osoblja posebno obučenog za provođenje istraga na internetu i društvenim mrežama koje je integrirano u svaku jedinicu specijaliziranu za borbu protiv trgovine ljudima. Ono što je najvažnije, ovo osoblje bi moglo biti iz redova policijskih službenika s policijskim ovlaštenjima ili ostalih policijskih službenika, npr. formiranjem grupa za tehničku podršku za „tradicionalne" istražitelje. Ova ideja se **udaljava od tradicionalnog policijskog modela** zasnovanog na policajcima pod zakletvom i usvaja princip – koji već primjenjuju neke policijske uprave – da službenici koji nisu pod zakletvom imaju više tehničku ulogu (npr. analitičari).

Pored organiziranja obuke za službenike, bugarski nadležni organi su istakli značaj angažiranja IT stručnjaka u istragama trgovine ljudima, kao i poboljšane saradnje s privatnim sektorom. Ovo su ponovili i kiparski nadležni organi, koji su kao potencijalnu dobru praksu naveli formiranje timova istražitelja i analitičara specijaliziranih za trgovinu ljudima i visokotehnološki kriminal. Vrijednost **međuagencijskog istražnog rada** uz učešće i saradnju širokog spektra specijaliziranog osoblja također je naglašena u prijavi Švicarske, u kojoj su, naprimjer, uspostavljeni zajednički timovi, i ovaj model bi se mogao proširiti na trgovinu ljudima posredstvom IKT-a.

Njemački nadležni organi su ukazali na značaj poboljšanja **razmjene znanja** među institucijama i **jačanja IKT vještina** među policijskim službenicima. Prema španskim nadležnim organima, ključno je i „povećati svijest o kriminalu preko interneta" i „uključiti stručnjake za tehnološki kriminal u istrage trgovine ljudima od samog početka". Nekoliko država je navelo da treba organizirati i/ili ojačati obuke o tome kako da se nadgledaju i koordiniraju istrage trgovine ljudima s velikom tehnološkom komponentom, jer elektronski

dokazi postaju sve značajniji u slučajevima trgovine ljudima.

Postoji opća saglasnost o **značaju nabavke i pristupa specijaliziranom softveru** za poboljšanje istraga o trgovini ljudima posredstvom IKT-a. U Holandiji nadležni organi su kreirali alat za skeniranje mreže za prikupljanje i sistematizaciju velikih količina podataka. Holandski organi za provođenje zakona trenutno testiraju alat na konkretnim slučajevima trgovine ljudima kako bi izgradili pravosudni okvir. Prema holandskim nadležnim organima, sistem za skeniranje mreže „fokusira se na reklame s rizikom od seksualne eksploatacije i trenutno je u fazi testiranja"; nadležni organi također rade na utvrđivanju da li „postoji dovoljna pravna osnova i praktična upotrebljivost za njegovu upotrebu u formalnim istragama".

Slično tome, nekoliko drugih država, uključujući Estoniju, Republiku Moldaviju i Grčku, istaklo je **značaj velikih količina podataka, kao i poboljšanje sposobnosti za obradu velikih količina podataka**. Razvijanje ili nabavka alata koji mogu automatski preuzimati web-lokacije i druge vrste elektronskih informacija smatra se ključnim u vođenju istraga. Naprimjer, Biro litvanske kriminalističke policije je 2020. godine nabavio licencu za softver za prikupljanje informacija iz online izvora i licencu za specijalizirani softver za analizu takvih informacija. Međutim, nije važna samo sposobnost prikupljanja podataka. Najvažnije je da takvi alati također moraju biti u stanju da **čuvaju takve informacije na siguran način** kako bi se mogle pouzdano koristiti „kao dokaz na sudu ili kao obavještajne informacije kako bi se izgradio slučaj" (prijava Švedske).

Druge dvije vrste alata smatraju se ključnim za provođenje djelotvornih istraga u slučajevima trgovine ljudima posredstvom IKT-a. Prvo, alati za preuzimanje informacija s mobilnih telefona kada šifra nije dostupna (prijava Švedske). Drugo, razvoj i uvođenje alata koji omogućavaju dešifriranje razgovora preko aplikacija za ličnu komunikaciju. Švedski nadležni organi su istakli da bi takvi alati također trebali biti u stanju dešifrirati razgovore u realnom vremenu. U Austriji Kriminalistička obavještajna služba razvija poseban softver za ispitivanje mobilnih telefona radi identifikacije žrtava trgovine ljudima.

Švicarski nadležni organi su istakli potrebu za povećanjem **tajnih istraga** – kroz ulaganje u obuku specijaliziranih službenika. Slično tome, istakli su značaj policijskih službenika posebno obučenih u oblasti trgovine ljudima. Norveški nadležni organi smatraju tajne istrage „najefikasnijim istragama", posebno kada se kombiniraju s prikupljanjem velikih količina podataka iz OSINT web-pretraga, kao i podataka o transferima/tokovima novca. U Holandiji policija trenutno testira upotrebu „mamac profila" za identifikaciju trgovaca ljudima tokom njihovog pokušaja da regrutiraju potencijalne žrtve. Slično tome, španski nadležni organi su istakli potrebu za prilagođavanjem nacionalnog zakonodavstva kako bi se u potpunosti iskoristile mogućnosti koje pružaju tajne istrage na internetu.

Britanski nadležni organi procjenjuju da je **slojevitost informacija** ključna za istraživanje trgovine ljudima posredstvom IKT-a. Obogaćivanje obavještajnih slika kombinacijom istraživanja podataka iz otvorenih izvora i sistema za provođenje zakona smatra se dobrom praksom. Također su predložili udaljavanje od jednostavnih lista indikatora. Naprimjer, primijetili su da u kontekstu seksualne eksploatacije istražitelji obično prate proces od tri koraka, za razliku od propisane liste indikatora, kako bi identificirali visokorizične oglase na ASW-u. Prema takvom procesu, rizik se identificira tamo gdje su ASW oglasi dio mreže, gdje su prisutni indikatori prinude i kontrole i gdje je autentičnost naloga za oglašavanje sumnjiva.

Nekoliko država je primijetilo značaj unapređenja prekogranične saradnje i osiguravanja brze razmjene podataka na operativnom nivou. Austrijski nadležni organi su kao primjer dobre prakse naveli **međusobnu razmjenu službenika** s državama porijekla žrtava. Općenito govoreći, ojačana međunarodna saradnja s istražnim organima u državama porijekla smatra se dobrom praksom.

Finski nadležni organi su istakli značaj provođenja **strateške analize** kako bi se prikupilo znanje o novonastalim trendovima i ažurirale informacije o modusu operandi (uključujući tehnologiju i web-lokacije koje koriste počinioci). Ovaj stav podržavaju i poljski nadležni organi. Prepoznato je da je stalno praćenje ove pojave teška i vremenski zahtjevna aktivnost, koja dodatno opterećuje (često) već preopterećene policijske resurse. Međutim, pristup ažuriranoj bazi znanja, uključujući tehnike regrutiranja koje koriste počinioci, smatra se veoma efikasnim sredstvom za prevenciju i borbu protiv trgovine ljudima. Ova vježba prikupljanja znanja treba imati međunarodnu dimenziju – idealno uz određeni stepen međunarodne koordinacije. Na osnovu ovih zajedničkih dokaza, pojedinačne države tada mogu pokrenuti ciljane policijske operacije i zaključiti sporazume o saradnji kad god je to relevantno.

Nekoliko država je primijetilo da bi istrage mogle biti **olakšane lakšim čuvanjem dokaza i pristupom na međunarodnom nivou**. Ovo se potencijalno prevodi u olakšane i pojednostavljene procedure za postupanje po upitima upućenim jedinicama nadležnim za čuvanje podataka u stranim državama (zahtjevi za čuvanje podataka), kao i u olakšavanje zahtjeva za uzajamnu pravnu pomoć. Kako su, između ostalog, istakli poljski nadležni organi, „privatni sektor je taj koji najčešće posjeduje informacije od značaja za organe za provođenje zakona (npr. podaci o pretplatnicima)", a „efikasno i brzo pribavljanje takvih podataka od strane policije važno je za pozitivno rješenje istrage".

3.3. Poticanje međunarodne saradnje

Razmišljajući o svom iskustvu u postupanju u prekograničnim slučajevima trgovine ljudima posredstvom IKT-a, države su identificirale sljedeće „dobre principe" za poticanje međunarodne saradnje:

- korištenje resursa dostupnih u agencijama kao što su Europol i Eurojust, kao i uspostavljanje zajedničkih istražnih timova;
- uspostavljanje kontakta s drugim stranama u **ranoj fazi** istrage. Ovo zahtijeva organizacijske mjere koje olakšavaju takve brze interakcije (npr. kroz jasnoću procedura i jasne kontaktne tačke);
- razvijanje veoma dobrog **razumijevanja pravnog konteksta i mogućnosti** saradnje s predmetnom državom ili državama kako bi se izbjegle blokade i osigurala blagovremena saradnja;
- održavanje **koordinacijskih sastanaka** radi razmjene informacija i dokaza što je brže moguće, kako bi se utvrdila zajednička strategija od samog početka, kako bi se olakšala realizacija zahtjeva za međunarodnu pravnu pomoć i kako bi se uklonile prepreke u vezi s prihvatljivošću dokaza u predmetnoj državi;
- razvijanje **zajedničkog razumijevanja** standardiziranih pristupa i osiguravanje **transnacionalne interoperabilnosti** agencija za provođenje zakona kroz transnacionalne obuke.

Pored ovih općih principa, postoji i niz konkretnih primjera dobre prakse koje su identificirale države ugovornice. Takve prakse se mogu grupirati u šest glavnih kategorija koje su opisane u nastavku.

Zajednički istražni timovi. Primjer dobre prakse međunarodne pravne saradnje koju su prijavili bugarski nadležni organi je zajednički istražni tim osnovan 2019. godine zajedno s Francuskom – i uz pomoć Eurojusta – koji se bavi borbom protiv trgovine ljudima, seksualnog zlostavljanja djece i trgovine trudnicama radi prodaje njihove djece. ZIT je proveo veliki broj istražnih aktivnosti u Bugarskoj, Francuskoj, Njemačkoj i Grčkoj. Općenito govoreći, nekoliko prijava navodi zajedničke istražne timove kao primjer dobre prakse. Kako su objasnili austrijski nadležni organi, oni omogućavaju „razmjenu informacija kada su u pitanju transnacionalne istrage uz manje birokratije, kao i podjelu nadležnosti između sudskih organa koji učestvuju".

Saradnja između inspektorata rada. Izvršna agencija bugarskog Općeg inspektorata rada istakla je značaj koordiniranih inspekcija i istraga koje se zajednički provode u svim državama u složenim prekograničnim slučajevima koji uključuju potencijalnu radnu eksploataciju među radnicima upućenim na rad u inostranstvo.[16] Zajedničke akcije koje su provele inspekcije rada Bugarske i Francuske (projekt Eurodétachement) smatraju se primjerima dobre prakse. Aktivnosti su uključivale zajedničke inspekcije u kompanijama za privremeno zapošljavanje koje šalju radnike u Francusku, kao i informativne sastanke za bugarske radnike koji su upućeni na rad u inostranstvo ili direktno zaposleni u Francuskoj (uglavnom u poljoprivredi). Održani su i online sastanci radi razmjene informacija i dobrih praksi o prekograničnim inspekcijama. Ovaj primjer je naročito interesantan jer pokazuje **značaj nepolicijske saradnje** – koliko i policijske – u borbi protiv trgovine ljudima. Ipak, takvoj saradnji obično se posvećuje ograničena pažnja u izvještajima o politici. Države ugovornice bi možda željele razmotriti načine za poboljšanje saradnje između organa koji nisu policijski organi – naročito u kontekstu trgovine ljudima u svrhu radne eksploatacije.

Strateška saradnja. Njemački nadležni organi istakli su značaj strateške saradnje, naprimjer preko OA 7.1 projekta EMPACT koji se zasniva na Europolu (Evropska multidisciplinarna platforma protiv prijetnji od kriminala). Ovaj projekt se fokusira na trgovinu ljudima na internetu. U okviru projekta EMPACT, Holandija i Ujedinjeno Kraljevstvo razvijaju vizuelni pregled trgovine ljudima posredstvom IKT-a.

Aktivnosti cyber patrola u koordinaciji EU/međunarodnih aktera. Holandski i portugalski nadležni organi su naveli EMPACT dane zajedničkih akcija/koordinirane akcije cyber patrola na internetu/mračnoj mreži kao primjer dobre prakse u međunarodnoj saradnji. Obavještajni podaci se prvo prikupljaju u pojedinim državama, a zatim se prelazi na koordinirane akcije.

Korištenje mreže oficira za vezu. Poljski i francuski nadležni organi istakli su značaj akreditiranih oficira za vezu za olakšavanje razmjene informacija. Francuski nadležni organi su ukazali na slučaj u kojem je podrška rumunskih oficira za vezu sa sjedištem u Francuskoj omogućila istovremeno hapšenje u obje države. Na ovaj način nadležni organi su mogli srušiti čitavu transnacionalnu kriminalnu mrežu, uključujući i njenog šefa, koji je upravljao operacijama u Francuskoj dok je živio u Rumuniji. Norveški nadležni organi su istakli prednost postojanja kontaktne tačke na Filipinima za razmjenu informacija o aktuelnim slučajevima, čime se izbjegavaju dupliranja u istragama i sukobi. Preko kontaktne tačke norveški i filipinski nadležni organi su bili u mogućnosti da razmijene iskustva, trendove i studije, uključujući i u pogledu trgovine ljudima posredstvom interneta.

[16] Prema Direktivi 96/71/EZ i Informacijskom sistemu unutrašnjeg tržišta (IMI).

3.4. Identifikacija žrtava i pomoć žrtvama

Ovaj odjeljak se fokusira na načine na koje države ugovornice koriste tehnološke alate u vezi s: (a) identifikacijom žrtava; (b) pomoći i (c) širenjem informacija među ugroženim zajednicama.

3.4.1. Tehnološki alati za identifikaciju žrtava trgovine ljudima

Čini se da se tehnološki alati zasnovani na **prepoznavanju lica** često koriste u slučajevima seksualne eksploatacije djece (CSE), npr. za unakrsno provjeravanje fotografija u postojećim međunarodnim bazama podataka, kao što je baza podataka NCMEC (Nacionalni centar za nestalu i eksploatiranu djecu, SAD) ili Interpolova ICSE.[17] Međutim, čini se da je upotreba takvih alata ograničenija izvan oblasti seksualne eksploatacije djece. Finski nadležni organi su naveli da provode testove alata za prepoznavanje lica kako bi identificirali žrtve seksualne eksploatacije na internetu, posebno u kontekstu web-kamera. Također su predložili da se upotreba takvih alata može proširiti kako bi obuhvatila širi spektar situacija trgovine ljudima. Latvijski nadležni organi su spomenuli upotrebu specijaliziranog softvera za prepoznavanje fotografija (PhotoDNK, Clear View) u pojedinačnim slučajevima. U Mađarskoj se tokom istrage može koristiti ciljana upotreba alata za prepoznavanje lica kako bi se identificirale potencijalne žrtve. Među nekoliko država koje su navele da koriste tehnološke alate za identifikaciju žrtava trgovine ljudima pomoću velikih količina podataka, Njemačka je nedavno uvela alat za skeniranje web-lokacija koje sadrže oglase za seksualne usluge kako bi se pomoglo u identifikaciji žrtava trgovine ljudima. Austrijski istražitelji imaju pristup **sistemima za skeniranje mreže radi prikupljanja podataka** i (pod određenim uvjetima) alatima za prepoznavanje lica. U Ujedinjenom Kraljevstvu nadležni organi koriste alate za „struganje" na internetu za prikupljanje i analizu podataka s web-lokacija za usluge za odrasle (ASW) kako bi se pomoglo u identifikaciji žrtava trgovine ljudima.

Što se tiče upotrebe **indikatora trgovine ljudima** (**„znaka upozorenja"**), nekoliko država je prijavilo da se oslanja na indikatore za potrebe identifikacije slučajeva trgovine ljudima; međutim, ovo su „opći" indikatori trgovine ljudima i nisu specifični za trgovinu ljudima posredstvom IKT-a. Ovo nije iznenađujuće, budući da je razvoj indikatora („znakova upozorenja") specifičnih za trgovinu ljudima posredstvom IKT-a daleko od jednostavnog – kao što je detaljno razmotreno u Poglavlju 2. Norveški nadležni organi su naveli da, iako „imaju skup indikatora za identifikaciju žrtava trgovine ljudima", predmetni skup treba revidirati i proširiti kako bi bio prikladan „okruženju istrage kriminala u vezi s IKT-om". Ovaj posao trenutno obavlja Norveška nacionalna ekspertna grupa za borbu protiv trgovine ljudima.

Britanski nadležni organi izvijestili su da koriste listu indikatora za pomoć pri **identifikaciji žrtava na ASW-u**. Njihovo iskustvo u korištenju ovakvih indikatora zajedno s alatom za „struganje" interneta posebno je značajno. Prema dostavljenim dokazima, iako ovi indikatori mogu pružiti određenu pomoć, oni se „trebaju koristiti u kombinaciji s analizom mreže i procjenom autentičnosti naloga kako bi se osigurala najbolja praksa". Ovo ukazuje na poteškoće u automatizaciji identifikacije žrtava – i na granice pretjeranog oslanjanja na unaprijed utvrđenu listu indikatora. Štaviše, britansko iskustvo pokazuje značaj kombiniranja

[17] Među tehnološkim alatima koje države koriste u borbi protiv seksualne eksploatacije djece (CSE) nalaze se „Gridcop" i „IcacCops". Islandska policija koristi „Griffeye" za obradu, sortiranje i analizu fotografija i videozapisa zaplijenjenih tokom istraga CSE-a i vrši unakrsne provjere ovih fotografija s međunarodnim bazama podataka.

različitih metoda, uključujući **analizu društvenih mreža** i **ljudsku procjenu** dokaza. Ponovo se jasno primjećuje ključna uloga analitičara/istražitelja – kao i potreba da se oni djelotvorno obuče. Alati mogu biti veoma dragocjeni u vršenju redukcije podataka i rukovanju velikim količinama informacija; međutim, potrebno je da ih koriste dobro obučeni operateri sa znanjem o specifičnoj temi/problemu (npr. trgovina ljudima).

Korištenje vještačke inteligencije i tehnoloških alata za identifikaciju žrtava ima svoje izazove, uključujući **etička pitanja** i potencijal za diskriminaciju (npr. profiliranje zasnovano na diskriminatornim kriterijima; vidjeti i diskusiju u Poglavlju 6). Švedska policijska uprava je izrazila zabrinutost u vezi s „upotrebom AI tehnologije za identifikaciju žrtava trgovine ljudima".

Na kraju, Ured grčkog nacionalnog izvjestioca i Laboratorij za prava Univerziteta u Nottinghamu uvode projekt koji koristi satelitske podatke i metode daljinskog otkrivanja za praćenje radnih uvjeta i mobilnosti radnika migranata u poljoprivredi. Grčki izvjestilac je u procesu razvoja daljih tehnoloških aplikacija za identifikaciju žrtava trgovine ljudima u sektoru poljoprivrede i učinio je razvoj novih tehnoloških aplikacija ključnom komponentom Nacionalnog akcionog plana 2019–2023.

3.4.2. Inicijative zasnovane na tehnologiji za pomoć žrtvama i širenje informacija među ugroženim zajednicama

Ovaj odjeljak predstavlja pregled inicijativa zasnovanih na tehnologiji koje su osmišljene da pomognu žrtvama i šire informacije među ugroženim zajednicama. Imajte na umu da su inicijative o kojima se govori u nastavku identificirane od strane država ugovornica.

Mehanizmi za prijavljivanje na internetu i telefonske linije za pomoć. Nekoliko država ima uspostavljene mehanizme za anonimno prijavljivanje viktimizacije, kao i za primanje početne pomoći putem telefonske linije za pomoć. Neke telefonske linije za pomoć nude 24-satnu podršku i mogu uputiti žrtve na socijalne službe, kao i objasniti procedure i prava. U Holandiji postoji nekoliko organizacija koje nude **digitalnu pomoć putem funkcije chata** („Fier" i „Slachtofferhulp Nederland" su dvije od tih organizacija). Takve organizacije nude početno savjetovanje, pomoć i mogućnost anonimnog prijavljivanja seksualne eksploatacije. Funkcija chata nije samo reaktivna već služi i za proaktivno uspostavljanje kontakta s pojedincima u riziku. Holandsko ministarstvo pravde i sigurnosti trenutno istražuje kako se ovaj alat može dalje razvijati u saradnji s relevantnim zainteresiranim stranama. U Francuskoj Ministarstvo unutrašnjih poslova vodi platformu za prijavljivanje seksualnog i rodno zasnovanog nasilja (PVSS). Žrtve mogu stupiti u kontakt sa zvaničnikom putem **sistema za razmjenu poruka/online chata**, podnijeti prijavu i dobiti prvu pomoć.

Zvanični online materijali. Informativni materijali koje pripremaju nadležni organi često se postavljaju na zvanične web-lokacije. U Austriji, naprimjer, informacije za žrtve trgovine ljudima koje priprema Savezno ministarstvo unutrašnjih poslova, kao i nevladine organizacije, dostupne su na nekoliko jezika na različitim online platformama i društvenim medijima. Na web-lokaciji Federalnog ministarstva pravde žrtve trgovine ljudima mogu pristupiti materijalima na 16 jezika o svojim pravima na psiho-socijalnu i pravnu podršku. U Poljskoj Ministarstvo unutrašnjih poslova i uprave i Ministarstvo vanjskih poslova vodili su online informativnu kampanju putem web-lokacije „e-konsulat" s banerom koji prikazuje informacije o trgovini ljudima na nekoliko jezika i preusmjerava online posjetioce na Konsultantski i interventni centar za žrtve trgovine ljudima (KCIK). Pored zvaničnih kanala, nekoliko država

je istaklo važnu ulogu koju imaju NVO u širenju informacija putem svojih web-lokacija, kao i zvaničnih naloga na društvenim medijima kao što su Facebook, Instagram i YouTube.

Online alati i aplikacije. Nacionalna komisija Bugarske za borbu protiv trgovine ljudima pokrenula je online alat za prevenciju u okviru godišnje kampanje za prevenciju trgovine ljudima u svrhu radne eksploatacije. Internetski alat je kreiran u saradnji s češkom NVO i bio je namijenjen Bugarima koji traže posao u Češkoj. Alat je pružio informacije o uvjetima rada i rizicima od kršenja prava radnika. Kako je primijetila navedena bugarska komisija, „efikasnost ovog pristupa je naglašena činjenicom da je ubrzo nakon što je alat počeo funkcionirati, napravljen lažni alat s ciljem da privuče potencijalne žrtve radne eksploatacije". U Litvaniji je nedavno razvijena aplikacija pod nazivom „Raktas" (dostupna u prodavnici Google Play) kako bi se podigla svijest Litvanaca koji žive i rade u inostranstvu o ranim znacima trgovine ljudima. Kao budući razvoj, aplikacija će uključivati mogućnost za chat preko kojeg će litvanska žrtva ili potencijalna žrtva trgovine ljudima moći kontaktirati litvansku NVO u realnom vremenu i zatražiti podršku. Portugalska Uprava za uvjete rada razvila je aplikaciju „ACT" – Agir Contra o Tráfico. Nadležni organi Estonije prijavljuju upotrebu masovnog obavještavanja putem SMS/tekstualnih poruka kao dio kampanje protiv seksualne eksploatacije. Španija je 2017. godine pokrenula mobilnu aplikaciju „Chicas Nuevas 24 horas: Happy" kako bi omogućila mladim ljudima da otkriju, kroz videoigru, putovanje djevojke (Happy) od njenog rodnog grada u Nigeriji do iskustva seksualne eksploatacije u Španiji.

Kampanje za podizanje svijesti na internetu. U Bugarskoj Nacionalna komisija za borbu protiv trgovine ljudima (NCCTHB) svake godine provodi tri nacionalne kampanje za prevenciju i informiranje s nizom događaja koji se fokusiraju na prevenciju trgovine ljudima u svrhu prinudnog rada i seksualne eksploatacije. Materijali se također distribuiraju putem interneta. Tokom kampanje oktobar/novembar 2018. godine kampanja je došla do preko dva miliona bugarskih aktivnih korisnika na mrežama Facebook i Instagram. Generalno, aktivnosti NCCTHB i povezani online alati za prevenciju redovno se objavljuju na društvenim medijima. Takve objave imaju oko 100.000 pregleda godišnje. Pored toga, diskusije o IKT-u, internetu, društvenim medijima i utjecaju novih tehnologija na trgovinu ljudima, kao i o njihovoj upotrebi za regrutiranje i eksploataciju žrtava, uključeni su u različite aktivnosti za podizanje svijesti na nacionalnom i lokalnom nivou, usmjerene prije svega na mlade ljude i studente. Izvršna agencija Generalne inspekcije rada organizira i učestvuje u informativnim kampanjama o rizicima u vezi s radom u inostranstvu; također upravlja i telefonskom linijom za savjetovanje i prijavljivanje koja je otvorena i za bugarske državljane koji rade u inostranstvu.

U Irskoj aktuelna kampanja pod nazivom „Blue Blindfold" koju vodi Ministarstvo pravde redovno širi informacije među ugroženim zajednicama putem namjenske web-lokacije, štampanih medija i kampanja na društvenim mrežama.

U Njemačkoj Savezno ministarstvo za ekonomsku saradnju i razvoj razvilo je projekte s državama partnerima za prevenciju i borbu protiv trgovine ljudima. Naprimjer, u okviru projekta „Sprečavanje trgovine ljudima na Zapadnom Balkanu i podrška žrtvama" Regionalna inicijativa za migracije, azil i izbjeglice (MARRI) izradila je smjernice i informativne materijale za kampanje za podizanje svijesti javnosti i učinila ih je dostupnim na internetu. Imajući u vidu da se internet sve više koristi za regrutiranje žrtava trgovine ljudima, jedan od alata se fokusirao na prijetnje kojima su djeca izložena na internetu.[18]

[18] "Minors at risk of cyber-trafficking" (toolboxes.marri-rc.org.mk/tips/minors-at-risk-of-cyber-trafficking).

U Rumuniji Nacionalna agencija za borbu protiv trgovine ljudima (NAATIP) vodi kampanje na mrežama Facebook, YouTube, a od 2020. godine i na mrežama Instagram, Twitter i LinkedIn. Objave na mreži Facebook stigle su do 2,5 miliona korisnika tokom 2020. godine (+300% u odnosu na prethodnu godinu). Primjeri kampanja uključuju sljedeće:

(a) svakodnevno objavljivanje preventivnih poruka na društvenim mrežama o borbi protiv trgovine ljudima i različitim vidovima eksploatacije (seksualna eksploatacija, radna eksploatacija i prinudno prosjačenje);

(b) online kampanja pod nazivom „The perfect Job – one way illusion" (Savršen posao – iluzija u jednom smjeru) u partnerstvu s OLX iz Rumunije (web-servis koji objavljuje objave) s ciljem prevencije trgovine ljudima kroz povećanje svijesti među ljudima koji traže posao preko online platformi;

(c) angažiranje dva poznata rumunska YouTube vlogera koji zajedno imaju publiku od 1,3 miliona pratilaca kako bi se povećale vidljivost i efikasnost poruka NAATIP-a protiv trgovine ljudima. Vlogeri su snimili dva videosnimka o trgovini ljudima koji su u prvim satima emitiranja postigli oko 100.000 pregleda na mreži YouTube.

Ukratko, važno je napomenuti da, kako su istakli bugarski nadležni organi, efikasna kampanja zahtijeva „mnogo pripremnog rada" kako bi se u potpunosti razumjelo kome je namijenjena i kako bi se adekvatno razvila njena poruka. Na kraju krajeva, to zahtijeva ulaganja. Dobra praksa je rad s privatnim kompanijama na izradi **društvenog oglašavanja**. Ovo se može postići, naprimjer, putem publikacija koje sponzoriraju kanali društvenih medija, kao što su Facebook i Instagram (platforma bi mogla osigurati besplatan prostor, kao i stručnost u dizajniranju kampanje/poruke). Jasno je da ciljane i dobro razvijene online kampanje mogu predstavljati koristan alat. Primjer kampanje koju je vodila bugarska Nacionalna komisija za borbu protiv trgovine ljudima mnogo govori. U okviru kampanje – osmišljene da podigne svijest o trgovini ljudima u svrhu radne eksploatacije – napravljen je i distribuiran vizuelni prikaz primjera obmanjujuće ponude za posao. Korisnici su pogrešno protumačili ponudu za posao kao pravu i počeli zvati kancelariju Nacionalne komisije raspitujući se o poslu (za više detalja o kampanji vidjeti odjeljak 1.1.2). Ovaj primjer pokazuje potencijalni domet/utjecaj obmanjujućih oglasa za posao, ali je također ponudio Komisiji „dobru priliku da informira tražioce posla koji su spremni da prihvate rizične ponude".

Međutim, kako su upozorili bugarski nadležni organi, postoji **rizik od pretjeranog oslanjanja na online kampanje** pri pokušaju da se dopre do potencijalnih žrtava. U nekim slučajevima takve žrtve dolaze iz „ranjivih zajednica" koje karakteriziraju nizak nivo obrazovanja i ograničeno poznavanje tehnoloških alata i resursa. U tim okolnostima pristup zasnovan na direktnom (ličnom) pristupu (i dalje) ima važnu ulogu kao preventivna strategija.

Na kraju, inspiracija za inicijative može poteći iz projekata koji se bave pitanjima sličnim trgovini ljudima posredstvom interneta i tehnologije. U Finskoj, naprimjer, NVO Women's Line pokrenula je projekt pod nazivom Turv@verkko, koji ima za cilj sprečavanje cyber nasilja nad ženama i djevojčicama i pružanje pomoći žrtvama. Slično tome, Youth Exit i Sua varten usmjereni su na mlade korisnike interneta kako bi spriječili seksualno uznemiravanje na internetu. Iako nisu direktno povezane s trgovinom ljudima, takve inicijative mogu ponuditi korisne naznake za razvoj projekata namijenjenih žrtvama trgovine ljudima.

3.5. Dokazi prikupljeni od nevladinih organizacija

NVO su izvijestile o brojnim strategijama za unapređenje pomoći u otkrivanju žrtava i podizanje svijesti u vezi s trgovinom ljudima posredstvom interneta i tehnologije.

La Strada International, KOK (Njemačka), Astrée (Švicarska) i La Strada Moldova naglasili su značaj **odgovarajućih i ažuriranih informacija** kojima žrtve trgovine ljudima i pojedinci podložni eksploataciji i zlostavljanju mogu lako pristupiti na internetu. Ovo bi trebalo uključivati informacije o organizacijama za podršku i njihovim telefonskim linijama za pomoć. Takve online platforme također trebaju **omogućiti samoidentifikaciju** žrtava. La Strada International je istakla da relevantne informacije do kojih dođu NVO treba podijeliti s organima za provođenje zakona – nakon što se dobije saglasnost relevantnih lica. Predviđene su inicijative za povećanje samoprijavljivanja također i u vezi s radnom eksploatacijom, npr. u formi online platformi i aplikacija putem kojih pojedinci mogu anonimno prijaviti zloupotrebe na licu mjesta (dokazi koje je pružila Sustainable Rescue Foundation iz Holandije).

Dostupnost online informacija i mehanizama za samoidentifikaciju treba kombinirati s **kampanjama za podizanje svijesti**. La Strada International smatra da su dvije vrste kampanja posebno važne: (a) one koje su direktno usmjerene na potencijalne žrtve i pojedince koji su u riziku od eksploatacije i zlostavljanja; i (b) one koje su usmjerene na zainteresirane strane da prepoznaju rizike od trgovine ljudima posredstvom tehnologije te da ih prijave. Organizacije Different and Equal (Albanija) i KOK (Njemačka) istakle su značaj edukacije korisnika IKT-a o rizicima vezanim za tehnologiju. One su predložile vođenje širih **kampanja za podizanje svijesti o tome kako trgovci ljudima mogu koristiti tehnologiju** i o rizicima s kojima se pojedinci mogu suočiti (naročito mlađi korisnici). Naglasak treba staviti na regrutiranje, posebno na to kako bi potencijalna eksploatatorska situacija mogla početi (tj. kako trgovci ljudima uspostavljaju prve kontakte). Kompanije koje pružaju online i IKT usluge trebaju učestvovati u ovim naporima. Migrant Rights Centre Ireland je dalje napomenuo da kompanije za društvene medije trebaju raditi na odvraćanju.

Osim toga, nekoliko NVO, uključujući La Strada International i Sustainable Rescue Foundation, podvuklo je značaj povećanja i unapređenja **razmjene podataka** među relevantnim zainteresiranim stranama. Ove razmjene bi trebale obuhvatati najnovija saznanja o rizicima vezanim za tehnologiju.

NVO su istakle značaj razvoja znanja o rizicima vezanim za IKT i općenito o trgovini ljudima posredstvom tehnologije, također među organizacijama koje pomažu žrtvama, uključujući one koje pružaju savjetodavne usluge. Pošto je **očuvanje elektronskih dokaza** ključno za razvoj jakih istraga, od ključnog je značaja da pripadnici prve linije borbe iz redova savjetnika i nevladinih organizacija budu upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem historije chata). Nuđenje sveobuhvatne obuke o sigurnosti i sljedivosti podataka na internetu za savjetnike i NVO smatra se ključnim.

Organizacija FIZ (Švicarska) primijetila je da IKT, uključujući društvene medije i online informacije, može pomoći nevladinim organizacijama da uspostave kontakte s potencijalnim žrtvama i prikupe dodatne informacije o okolnostima eksploatacije. Ako budu upozorene na sumnjivu situaciju, NVO mogu **iskoristiti informacije dostupne na internetu za uspostavljanje kontakta s potencijalnom žrtvom**.

Migrant Rights Centre Ireland i Astrée (Švicarska) predložili su osnivanje namjenskih jedinica za istraživanje digitalnog kriminala koje bi bile stručne za borbu protiv trgovine ljudima

posredstvom tehnologije. Organizacija Praksis (Grčka) pozvala je na jačanje stručnosti organa za provođenje zakona u pogledu IKT-a i pratećih rizika. Štaviše, ona je pozvala na pojačanu saradnju i razmjenu između nadležnih organa i privatnih kompanija.

Dokazi prikupljeni od nevladinih organizacija potvrđuju da korištenje „**znakova upozorenja**" u slučajevima trgovine ljudima posredstvom tehnologije nije rasprostranjeno. NVO prijavljuju korištenje standardnih indikatora, ali pozivaju na **reviziju takvih indikatora** kako bi se razmotrile specifičnosti IKT-a posredstvom tehnologije – naročito u vezi s regrutiranjem i eksploatacijom posredstvom IKT-a. Organizacija KOK (Njemačka) sugerirala je da praćenje web-lokacija na kojima klijenti razmjenjuju iskustva o kupovini seksualnih usluga može pružiti nagovještaje o prisilnoj prostituciji/trgovini ljudima. Pregled „znakova upozorenja" mogao bi uključivati indikatore koji su primjenjivi na takve web-lokacije.

3.5.1. Fokus na inicijative koje se zasnivaju na tehnologiji

La Strada International smatra da njeni članovi i druge NVO „sve više" koriste tehnologiju. Međutim, iako su se „tehnički resursi i mogućnosti enormno povećali", stepen u kojem NVO koriste tehnologiju ostaje „ograničen". Kako navodi La Strada International, tehnologija se uglavnom koristi za registraciju podataka, a zatim i njihovu analizu, kao i za praćenje aktivnosti pružanja pomoći. NVO sve više koriste tehnologiju, uključujući društvene medije, za vođenje kampanja (npr. kampanje za podizanje svijesti; vidjeti u nastavku) i za pružanje informacija, kao i za „stupanje u kontakt s grupama u riziku ili za angažiranje sa zajednicama na internetu" (prijava La Strada International). U okviru ove studije, od nevladinih organizacija je traženo da navedu primjere inicijativa zasnovanih na tehnologiji za poboljšanje otkrivanja trgovine ljudima posredstvom interneta i tehnologije, identifikaciju žrtava i prevenciju budućih slučajeva. U nastavku je dat kratak pregled ovakvih inicijativa na osnovu dokaza koje su pružile NVO.

Samoprijavljivanje putem interneta i kontakt s potencijalnim žrtvama

- Organizacija La Strada Moldova ukazala je na online mehanizme za djecu pomoću kojih mogu sami prijaviti probleme sigurnosti na internetu (www.siguronline.md). To uključuje neprijatne situacije s kojima se dijete moglo suočiti na internetu. Dijete tada stupa u kontakt sa specijaliziranim savjetnikom i, ako se otkriju dokazi o seksualnom zlostavljanju ili eksploataciji na internetu, slučaj se prijavljuje policiji.

- U Švicarskoj organizacija Astrée je primijetila sve veći broj žrtava koje se same prijavljuju za njene usluge, kao i sve veći broj potencijalnih žrtava koje su uputili prijatelji ili klijenti zahvaljujući prisustvu organizacije na internetu. Astrée također nudi online obrazac za uspostavljanje kontakta i traženje pomoći. Dalje, FIZ je ukazao na uspješnu upotrebu platformi društvenih medija za uspostavljanje kontakta s potencijalnim žrtvama trgovine ljudima ako je poznato ime osobe. Web-lokacija Nacionalne platforme protiv trgovine ljudima iz Švicarske sadrži veze do brojnih organizacija koje mogu pružiti pomoć.

- Organizacija Fair Work (Holandija) koristi društvene medije da dopre do migrantskih zajednica kako bi identificirala žrtve trgovine ljudima ili situacije eksploatacije. Fair Work prvo identificira Facebook stranice koje su relevantne za određenu ciljnu grupu, a zatim dijeli informacije preko takvih stranica. Ona kreira anonimne lične naloge, koje vode volonteri, a koji se koriste za prevenciju. Kako radnici migranti često koriste društvene medije za

pronalaženje informacija, ove tehnike se mogu iskoristiti da pomognu pojedincima u riziku „da postanu manje izolirani i više osnaženi" i da smanje rizike od trgovine ljudima (prijava La Strada International). Međutim, ovo nije uvijek lak zadatak, jer „žrtvama nije uvijek lako da znaju gdje tražiti odgovarajuće informacije, kojim informacijama mogu vjerovati,

kome se obratiti te da nađu ko im najbolje može pomoći, naročito ako slabo poznaju državu i svoja prava u toj državi".

- Organizacija La Strada International prijavila je da su neki od njenih članova razvili konsultantske servise za chat na internetu za traženje savjeta i prijavu eksploatacije i zlostavljanja – pored telefonskih linija za pomoć.

- La Strada International je također prijavila da njeni članovi obično koriste online platforme, kao što su Facebook, Instagram, LinkedIn, i vlastite web-lokacije kako bi informirali javnost o svom radu. Slično tome, organizacija KOK (Njemačka) prijavila je da njeni članovi koriste web-lokacije, Facebook i WhatsApp za širenje informacija i uspostavljanje kanala komunikacije za potencijalne žrtve. Ono što je najvažnije, jedna organizacija klijentima nudi broj na WhatsAppu za prijavu znakova potencijalne eksploatacije među seksualnim radnicima.

Mobilne aplikacije za podizanje svijesti i traženje pomoći/informacija

- Organizacija La Strada u Češkoj Republici bila je uključena u kreiranje SAFE, aplikacije koju je razvio IOM Slovačka u obliku interaktivne igre dizajnirane da spriječi trgovinu ljudima. Igrajući igru, korisnici procjenjuju svoj rizik u pogledu trgovine ljudima; aplikacija također sadrži informacije o sigurnom putovanju, radu u inostranstvu i korisnim kontaktima u hitnim slučajevima. Astra (Srbija) je razvila BAN Human Trafficking, aplikaciju čiji cilj je da mlade ljude upozna sa situacijama koje potencijalno dovode do eksploatacije i da pruži savjete za uočavanje takvih situacija. Plan im je da nadograde aplikaciju funkcijom za prijavu eksploatatorskih praksi.

- Organizacija La Strada International je primijetila razvoj aplikacija od strane nevladinih organizacija za prijavu eksploatacije i zlostavljanja, kao što je, naprimjer, aplikacija koju je razvio Unseen (Ujedinjeno Kraljevstvo). U Albaniji organizacija Different and Equal učestvuje u razvoju različitih mobilnih aplikacija (npr. „#raporto #shpeto") koje su namijenjene da pomognu žrtvama trgovine ljudima i rodno zasnovanog nasilja („#GjejZa").

- Organizacija La Strada International je dalje primijetila razvoj aplikacija za podršku ranjivim grupama, naprimjer za pružanje pristupa informacijama ili informacija o radnim pravima u državi odredišta. Jedan od primjera je aplikacija Workenn: igra za integraciju migranata na tržište rada, proizvedena u okviru Sirius projekta za pomoć migrantima koji traže posao. Kao jedan od primjera izvan Evrope možemo spomenuti Apprise Audit – platformu koju su razvili klub Mekong i Univerzitetski institut UN u Makau, koja omogućava sigurne i povjerljive razgovore s radnicima na njihovom maternjem jeziku.

Online kampanje za podizanje svijesti

- Organizacija La Strada Moldova provela je kampanju za podizanje svijesti tokom „Dana sigurnijeg interneta 2019. godine" s ciljem podizanja svijesti o seksualnoj iznudi među mladima. Ljudi su potaknuti da prijavljuju slučajeve putem sigurnog online mehanizma za prijavljivanje (www.siguronline.md). Kampanja je doprla do oko 70.000 online korisnika. Ista organizacija testirala je strategije profiliranja kako bi usmjerila svoje online poruke odabirom

starosne kategorije online korisnika, njihovih interesiranja i profila.

- Organizacija Different and Equal (Albanija) organizirala je nekoliko kampanja za podizanje svijesti na internetu koristeći društvene mreže i aplikacije (uključujući Facebook, Instagram, Twitter, web-lokaciju i YouTube) koje su bile naročito usmjerene na sprečavanje trgovine ljudima, seksualnog zlostavljanja i porodičnog nasilja (kampanja je doprla do oko 15.000 korisnika). Kampanja je pokrenuta, u saradnji s drugim nevladinim organizacijama, tokom pandemije COVID-19.

- Organizacija Novi put (Bosna i Hercegovina) organizirala je nekoliko kampanja za podizanje svijesti koje su bile fokusirane na korištenje tehnologije u vezi s trgovinom ljudima i seksualnom eksploatacijom djece.

- Astra (Srbija) organizirala je kampanje za podizanje svijesti o najvažnijim načinima regrutiranja, uključujući ponude za posao na internetu i vrbovanje preko mreže Facebook i društvenih mreža, kao i o strategijama za kontrolu i eksploataciju žrtava (uključujući praćenje žrtava korištenjem dostupnih opcija za praćenje lokacije u često korištenim aplikacijama).

Ostale inicijative

- Organizacija Astra (Srbija) je 2018. godine provela eksperiment „virtuelne djevojčice" – napravila je profil petnaestogodišnje djevojčice koja koristi internet. U roku od 24 sata ovaj profil je primio preko 3.000 zahtjeva, uključujući ponude za posao i eksplicitne seksualne ponude od odraslih muškaraca (dokazi koje je dostavila La Strada International).

- Organizacija Different and Equal (Albanija) u okviru svog programa reintegracije organizira obuku o korištenju računara i tehnologije, koja uključuje tehnike zaštite podataka.

- La Strada International je prijavila neke javno-privatne inicijative u koje su uključene NVO, npr. projekt koji je pokrenuo Univerzitet u Amsterdamu s velikim holandskim bankama u cilju identifikacije slučajeva trgovine ljudima. U okviru ove inicijative konsultirane su NVO sa sjedištem u Holandiji, uključujući FairWork, CoMensha i La Strada International.

Pogled u budućnost i rješavanje najvažnijih pitanja

Među nevladinim organizacijama vlada opća saglasnost da se više može učiniti kako bi se iskoristila tehnologija, naročito za širenje informacija, pristupanje i komunikaciju s potencijalnim žrtvama – kao i za prijem savjeta i izvještaja. Organizacija FIZ (Švicarska) predložila je da se dalje razvijaju alati za anonimno prijavljivanje nasilja i eksploatacije, i da se osiguraju kontakti s nevladinim organizacijama koje nude usluge zaštite i savjetovanja žrtava. Organizacija KOK (Njemačka) ukazala je na značaj daljeg razvoja vizuelnih materijala, npr. videozapisa, slika i aplikacija, koji će se koristiti tokom obuke, kao i za širenje na internetu, uključujući i među rizičnim zajednicama.

NVO su također otvorile neka **najvažnija pitanja** u vezi s inicijativama i tehnološkim alatima. La Strada International je istakla da se tehnološki alati uglavnom izrađuju u okviru samostalnih projekata i da „često ne uključuju periode testiranja". Dakle, dostupni su nam ograničeni dokazi o njihovoj efikasnosti. Osim toga, kada više nema finansijske podrške za projekt, često ne postoji dugoročna finansijska strategija za promoviranje i korištenje proizvedenih alata. Ovo je naročito problematično jer je za alate potrebno „kontinuirano ažuriranje i obučavanje".

Organizacija La Strada International je dalje primijetila da inicijative „često nemaju dovoljno učešća nevladinih organizacija i drugih zainteresiranih strana koje bi trebale koristiti alate u praksi i stoga trebaju imati određeni osjećaj vlasništva". Također je istakla „da je i dalje nejasno kakav je utjecaj tehnologije na efikasno sprečavanje ili borbu protiv trgovine ljudima", što dovodi u pitanje da li „[su] nadzor i profiliranje na granicama, kao i na drugim lokacijama, zapravo doveli do identifikacije žrtava trgovine ljudima" i da li su lica identificirana pomoću tehnologije tada dobila „pomoć i zaštitu". Organizacija poziva na **više evaluacije i procjene utjecaja** „svih razvijenih tehnoloških alata". „Da li su ovi – često skupi – alati služili potrebama zainteresiranih strana u borbi protiv trgovine ljudima i da li su alati ustvari testirani i dobro korišteni, a ako nisu, zašto nisu?", pitala je ona.

Ono što je najvažnije, NVO su naglasile da, sve u svemu, još uvijek postoji ograničena dostupnost tehnoloških alata koje praktičari mogu koristiti. Da bi odgovarali potrebama nevladinih organizacija, **alati moraju biti „jeftini i laki za upotrebu".** Sustainable Resource Foundation je dalje upozorio da „alati stvaraju višak podataka za različite korisnike", pa je stoga važno da budu razvijeni imajući u vidu specifične potrebe i sveobuhvatnu strategiju kako bi se izbjeglo dupliranje alata koji obavljaju (lake) funkcije, dok im nedostaju alati koji obavljaju više strateške, složenije funkcije.

3.6. Dokazi prikupljeni od tehnoloških kompanija

Facebook je izvijestio o različitim oblicima **saradnje s nevladinim organizacijama** iz cijelog svijeta u cilju kreiranja obrazovnih kampanja koje podižu svijest o rizicima seksualne eksploatacije na internetu – posebno među mladim korisnicima – kao i o pravima potencijalnih žrtava trgovine ljudima i kućnog ropstva. Takve kampanje također pružaju informacije o telefonskim linijama za trgovinu ljudima koje nude pomoć i podršku. Primjera radi, Facebook je naveo kampanju za podizanje svijesti o trgovini radnicima/kućnom ropstvu pokrenutu u martu 2021. godine u partnerstvu s organizacijom Stop the Traffik, koja je imala za cilj da pruži informacije domaćim i niskokvalificiranim radnicima na Filipinima o njihovim pravima, o lokalnim smjernicama za zapošljavanje u inostranstvu i o dostupnim telefonskim linijama za pomoć kako bi se izbjeglo nezakonito regrutiranje i zlostavljanje.

Facebook je također prijavio stvaranje prečice za pružanje informacija i dodatnih resursa ljudima koji pretražuju termine koji se odnose na trgovinu ljudima u cilju seksualne eksploatacije. Takve termine su razvili interni i eksterni stručnjaci.

Da bi ublažio problem nedovoljnog prijavljivanja, Facebook je naveo da radi na „proaktivnom pronalaženju i poduzimanju mjera u vezi sa sadržajima koji se odnose na trgovinu ljudima". Oni su prijavili „povećanje" svoje sposobnosti za „otkrivanje sadržaja koji krše pravila, što predstavlja direktan rezultat velikih ulaganja naših tehničkih i operativnih timova".

IBM i Stop the Traffik, NVO sa sjedištem u Ujedinjenom Kraljevstvu, udružili su se 2014. godine kako bi stvorili platformu Traffik Analysis Hub – novi subjekt koji vodi **zajedničku platformu za dijeljenje podataka** zasnovanu na sigurnom oblaku i analitici višejezičnog sadržaja zasnovanog na vještačkoj inteligenciji i geoprostornoj analitici. Platforma okuplja 95 organizacija iz cijelog svijeta. Cilj platforme jeste poremetiti globalnu trgovinu ljudima time što okuplja NVO (npr. Stop the Traffik, Liberty Shared, Crimestoppers i Save The Children UK), agencije za provođenje zakona (npr. Europol, Interpol i razne policijske organe SAD-a) i finansijske institucije (npr. Western Union, Barclays, Standard Chartered, Lloyds i PayPal). Kao što je primijetio IBM, platforma Traffik Analysis Hub koristi prilagođene modele vještačke

inteligencije specifične za domen za prikupljanje relevantnih podataka u velikom obimu i za klasifikaciju ovih podataka na osnovu klasifikacije koju je razvila stručna zajednica platforme. Podaci se zatim dijele među organizacijama učesnicama. Jedan od ključnih rezultata je „Red-Flag Accelerator", biblioteka tipologija razvijena na osnovu transakcija koje su označene znakovima upozorenja primijećenim na računima žrtava. Ovakvi indikatori znakova upozorenja trebaju biti implementirani u sisteme praćenja finansijskih institucija koje učestvuju u projektu. Pored toga, platforma ima za cilj da razvije alat za predviđanje zasnovan na korelaciji koji pomaže da se identificiraju karakteristike zajednica u riziku koje mogu postati izvori trgovine ljudima.

IBM je također primijetio nedavno pokrenutu **besplatnu online mapu puta za obuku** onih koji su zainteresirani da postanu analitičari podataka u domenu trgovine ljudima. Obuka obuhvata module o trgovini ljudima (uvod u trgovinu ljudima; kako uočiti znakove trgovine ljudima), kao i module o nauci o podacima i primjeni tehnologija u svrhu analitike podataka.

IBM također sponzorira online DataJam takmičenja tokom kojih stručnjaci IBM-a rade s timovima iz različitih sektora na osmišljavanju inovacija u primjeni tehnologije za sprečavanje trgovine ljudima. Neki od primjera uključuju sljedeće:

- alati za „struganje" stranica za oglašavanje za odrasle na internetu i primjenu markera prinudnog učešća (npr. jezik treće strane, više oglasa koji koriste iste identifikatore za kontakt, oglasi koji se odnose na historijski poznate nacionalnosti žrtava) te izvođenje geoprostorne analize klastera na oglasima „od interesa";
- alati za „struganje" poruka na tržištima i forumima u dubokoj/mračnoj mreži, primjenjuju markere specifične za trgovinu ljudima putem vještačke inteligencije, identificiraju teme u trendu i oznake korisnika, kreiraju mrežne modele tema za dalju analizu od strane agencija za provođenje zakona;
- alati za validaciju oglasa za posao na internetu za pametne telefone, koji omogućavaju pojedincima da provjere legitimnost oglasa za posao objavljenog na internetu prije uspostavljanja kontakta.

Kada je riječ o **saradnji s agencijama za provođenje zakona**, Facebook je naveo niz javno-privatnih partnerstava (JPP) u kojima učestvuje, kao što je Interpolova ekspertna grupa za trgovinu ljudima (HTEG) koja se bavi borbom protiv eksploatacije ljudi. Kao dodatni primjer, Facebook je izvijestio o primjeni sistema online zahtjeva za organe za provođenje zakona („LEORS") kako bi se pojednostavili pravni zahtjevi za podatke o nalozima na Facebooku (uključujući zahtjeve koji se odnose na trgovinu ljudima). Zahtjeve podnijete preko sistema LEORS rješavaju timovi sa sjedištem u Sjedinjenim Državama, Irskoj i Singapuru.

3.7. Dodatni dokazi prikupljeni na osnovu analize okruženja

Pored dokaza koje su pružile države ugovornice, NVO i tehnološke kompanije, studija je također uključivala uredsko istraživanje trenutne baze dokaza o strategijama i alatima koji se koriste za borbu protiv trgovine ljudima posredstvom interneta i tehnologije.

Organizacije OSCE i Tech against Trafficking (2020) provele su istraživanje IKT alata i inicijativa razvijenih za borbu protiv trgovine ljudima. Riječ je o 305 alata/inicijativa koje su razvile kompanije iz privatnog sektora, humanitarne organizacije i vlade (ogromna većina na engleskom jeziku). Među ovim alatima: 26% je dizajnirano za identifikaciju žrtava i trgovaca

ljudima; 16% za podizanje svijesti; 14% za upravljanje lancem snabdijevanja; 13% za praćenje trendova i mapiranje podataka; 10% za identifikaciju korporativnog rizika; 9% za angažiranje i osnaživanje radnika i 12% za druge svrhe. Alati i inicijative koje su ispitali OSCE i Tech against Trafficking nastoje postići sljedeći skup ciljeva: (a) širenje informacija u ugroženim zajednicama, uključujući migrante; (b) edukacija o rizicima trgovine ljudima, traženju pomoći i prijavljivanju potencijalnih slučajeva; (c) uklanjanje mogućnosti za eksploataciju; (d) identifikacija žrtava; (e) prikupljanje javno dostupnih informacija za borbu protiv trgovine ljudima; (f) procjenu rizika od trgovine ljudima; (g) praćenje i usklađenost; (h) identificiranje tipologija i postupanje na osnovu njih. Slično tome, Raets i Janssens (2018) su identificirali sljedeće (široke) načine na koje se alati zasnovani na tehnologiji mogu koristiti u borbi protiv trgovine ljudima: (a) agregacija i analiza podataka; (b) lanac blokova za sljedivost i porijeklo (praćenje lanaca snabdijevanja); (c) vještačka inteligencija (AI) i mašinsko učenje za postizanje velike računarske snage; (d) prepoznavanje lica (skeniranje mreže radi prikupljanja podataka); (e) tehnologija za žrtve i preživjele: identificiranje i pružanje podrške žrtvama, pristup na različitim jezicima. Muraszkiewicz (2018) je identificirao skeniranje mreže radi prikupljanja podataka; analitiku podataka; prediktivno nadziranje; korištenje lanca blokova; geografske informacijske sisteme (GIS); online baze podataka i inicijative za grupno djelovanje kao dodatne načine na koje se alati zasnovani na tehnologiji mogu koristiti u borbi protiv trgovine ljudima. Često je nejasno koji od ovih alata zaista funkcioniraju, koji se mogu korisno proširiti i koji zaista donose koristi žrtvama trgovine ljudima (čini se da su neki od ispitanih alata dizajnirani da prikupljaju informacije koje je potom teško koristiti u praksi). Na osnovu informacija koje se koriste kroz tehnologiju treba djelovati. U slučaju o kojem su raspravljali Rende Taylor i Shih (2019) pokazalo se da se rijetko reagira na izvještaje radnika podnijete putem elektronske aplikacije za prijavu povratnih informacija o eksploataciji u lancima snabdijevanja.

U literaturi se navodi da se tehnologija teško može koristiti kao zamjena za praktično znanje na terenu. Štaviše, prema agencijama za provođenje zakona koje su intervjuirali Elliott i McCartan (2013), tehnologije mobilnih telefona, uključujući aplikacije, mogu biti dio alata za borbu protiv trgovine ljudima, ali nisu sveobuhvatno rješenje. Operativno posmatrano, pružaoci internetskih usluga vide se kao subjekti koji drže značajan dio elektronskih dokaza, pa je nekoliko izvora ukazalo na značaj bliske saradnje s privatnim sektorom. Takva saradnja treba obuhvatiti mehanizme koji olakšavaju pribavljanje dokaza, uklanjanje takvih dokaza kad god je to prikladno i brzo prijavljivanje organima za provođenje zakona u određenim slučajevima. Istovremeno, identificirane su brojne prepreke za razmjenu informacija između različitih aktera. To uključuje pitanja privatnosti i sigurnosti podataka. Također su upućeni pozivi za uvođenje zajedničkih međunarodnih (multilateralnih) standarda koji podržavaju saradnju između agencija za provođenje zakona, nevladinih organizacija i privatnog sektora.

Tek veoma mali skup specifičnih alata je više puta spomenut u nekoliko izvora. Ovi alati uključuju: (a) projekt Artemis kompanije Microsoft, koji je razvio alat za otkrivanje tehnika vrbovanja tako što je kreirao ocjenu rizika za razgovore zasnovanu na prošlim slučajevima, a zatim označio one najsumnjivije kako bi ih ljudski moderatori pažljivo ispitali; (b) PhotoDNK kompanije Microsoft, koji stvara jedinstveni digitalni potpis (heš) slike, koji se zatim koristi za otkrivanje seksualne eksploatacije djece.

Međunarodna konfederacija sindikata izvještava o kampanji za podizanje svijesti koju vodi AidRom za pružanje informacija ljudima koji na internetu traže posao u inostranstvu. Ova

kampanja je uključivala savjete o tome kako primijetiti sumnjive oglase i razvila je sljedeće smjernice: „1. Obratite pažnju na izvor objave. Većina specijaliziranih stranica za traženje posla ne provjerava objave agencija za zapošljavanje. 2. Nikada ne prihvatajte ponudu koja je stigla od pojedinaca. 3. Pažljivo pročitajte ugovor o posredovanju. Ako plaćate naknadu, uvjerite se da znate za šta plaćate i šta prihvatate kao uvjete. Kada se jednom potpiše, teško je – ili čak nemoguće – poništiti dogovor. 4. Zatražite što je više moguće detalja o poslu za koji se prijavljujete. 5. Ako posao djeluje previše dobro da bi bio istinit... vjerovatno nije istinit!" Internet se koristi kao sredstvo za zaštitu od regrutiranja u svrhu zloupotrebe.

Nije jasno koliko je ova kampanja trajala i da li je podignuta na viši nivo ili usvojena u drugim državama.

Dva projekta se također često navode kao primjer dobre prakse: Spotlight organizacije Thorn i projekt Polaris, oba sa sjedištem u SAD-u. Spotlight je alat zasnovan na internetu koji je razvijen da pomogne istražiteljima da identificiraju djecu žrtve trgovine ljudima korištenjem online dokaza. Međutim, u javnom domenu ima veoma malo informacija o softveru. Projekt Polaris analizira podatke uglavnom prikupljene preko Nacionalne telefonske linije za borbu protiv trgovine ljudima, dopunjene drugim (neodređenim) izvorima informacija.

Grupno djelovanje u svrhu otkrivanja žrtava navodi se kao građanska inicijativa omogućena tehnologijom, za koju se TraffickCam često smatra najboljim primjerom. Od ljudi se traži da slikaju hotelske sobe kako bi se takve slike mogle koristiti za identifikaciju lokacija žrtava. Međutim, nije jasno da li su takve inicijative efikasne. Štaviše, mogu otvoriti pitanja privatnosti, kao i povećati potencijalni rizik od osvete. Dok se savjeti korisnika smatraju veoma dragocjenim, inicijative za grupno djelovanje moraju biti pažljivo ispitane i uravnotežene u odnosu na rizik stvaranja virtuelnih (i nevirtuelnih) grupa osvetnika.

Općenito govoreći, organizacija ICAT (2019) identificirala je brojne načine kako tehnologija može igrati pozitivnu ulogu u borbi protiv trgovine ljudima. Oni uključuju: (a) pomaganje tokom istraga; (b) unapređenje krivičnog gonjenja; (c) podizanje svijesti; (d) pružanje usluga žrtvama; i (e) bacanje novog svjetla na strukturu i funkcioniranje mreža za trgovinu ljudima. Različiti izvori su ukazivali na značaj „**digitalnih otisaka**", što znači da online sadržaji i povezani uređaji predstavljaju izuzetno bogat izvor informacija (Myria 2017; Mitchell i Boyd 2014). Ono što je najvažnije, moguće je mapirati **kriminalne mreže** na osnovu stranica društvenih mreža (Myria 2017; također ICAT 2019 i TRACE 2015). Prikupljanje i analiza digitalnih dokaza mogu **smanjiti teret za žrtve** prilikom pružanja dokaza protiv trgovaca ljudima (kao i dokaza u njihovoj odbrani).

4. Obuka: šta je osigurano, šta je potrebno

4.1. Obuka za organe za provođenje zakona: šta je osigurano i šta je potrebno

Studija je prvo istražila obuke koje se trenutno pružaju organima za provođenje zakona u pogledu otkrivanja i istraživanja slučajeva trgovine ljudima posredstvom interneta i tehnologije. Zatim je izvršena „analiza potreba" kako bi se identificirale dodatne potrebe za obukama koje bi se mogle ponuditi kako bi se povećala efikasnost otkrivanja, vođenja istraga i identifikacije žrtava.

Općenito govoreći, različite države pružaju različite nivoe obuka za organe za provođenje zakona, u različitim formatima. Sve u svemu, većina država je prijavila da organizira obuke o trgovini ljudima. Međutim, publike za koje su takve obuke namijenjene variraju od države do

države, pri čemu neke zahtijevaju da svi policijski službenici koji bi mogli doći u kontakt s potencijalnom žrtvom prođu takvu obuku, dok drugi ograničavaju obuku na specijalizirane jedinice.

Koji su elementi obuka koje države smatraju ključnim u smislu trgovine ljudima posredstvom interneta i IKT-a? Postoji opća saglasnost o činjenici da službenici trebaju proći obuku o (a) načinu otkrivanja slučajeva trgovine ljudima i žrtava; (b) načinu prikupljanja, čuvanja i obrade **elektronskih dokaza**, uključujući metode izdvajanja informacija iz računara i drugih digitalnih medija; i (c) načinu korištenja relevantnih dijelova softvera, uključujući **analizu velikih količina podataka** i sistema za skeniranje mreže radi prikupljanja podataka (gdje to dozvoljava nacionalno zakonodavstvo). Nekoliko država smatra da je neophodna **obuka o OSINT-u**. Istražne tehnike koje uključuju **tajne istrage na internetu** također se smatraju ključnim.

Iako je većina država prijavila osiguravanje elemenata ovih obuka, one su također naglasile probleme, uključujući (a) potrebu da se obuka održi aktuelnom i, u nekim slučajevima, da se značajno unaprijede postojeći elementi; te (b) potrebu da se poveća udio osoblja koje prolazi obuku. Neke države su izrazile zabrinutost zbog ograničenih obuka koje se često pružaju kada je riječ o pitanjima povezanim s IKT-om i, još više, trgovinom ljudima posredstvom IKT-a. Predloženo je da se **osmisle i osiguraju intenzivni kursevi obuke o trgovini ljudima posredstvom IKT-a,** koji bi također obuhvatali i tehnička pitanja. Opet, različite države bi se našle u različitom položaju u odnosu na digitalne kompetencije svog osoblja za provođenje zakona, ali je jedan broj država ukazao na potrebu da se ponudi **dalja obuka o upotrebi IKT-a** kako bi se poboljšalo otkrivanje slučajeva trgovine ljudima.

Države su također istakle potrebu da se osigura i početna i kontinuirana obuka, uzimajući u obzir istražno okruženje koje se brzo mijenja. Ovo, s druge strane, zahtijeva resurse za pripremu modula obuke (uključujući istraživanje o novim razvojima u kontekstu trgovine ljudima posredstvom IKT-a) i njihovu realizaciju.

Nije neuobičajeno da države ugovornice imaju službenike koji pohađaju module obuke koje organiziraju međunarodne organizacije ili druge države. Razmjena informacija i znanja na međunarodnom nivou je svakako dobra praksa. Pored toga, za države s ograničenim budžetima i resursima koristi mogu biti značajne. Međutim, pošto su neki elementi obuke i dalje u velikoj mjeri specifični za kontekst, postoji potreba da sve države budu u poziciji da interno razvijaju znanje i da organiziraju obuke koje također uzimaju u obzir lokalne specifičnosti ove pojave (ograničen broj država trenutno ne organizira nikakve obuke o trgovini ljudima posredstvom IKT-a, uključujući o OSINT-u, već se oslanja samo na obuke koje pružaju vanjske organizacije).

Različite države imaju različite organizacijske strukture, posebno kada se odlučuje o tome gdje se nalazi znanje o IKT-u. Međutim, ključno je napomenuti značaj izbjegavanja uskih grla u svakodnevnim operacijama zbog neoptimalne raspodjele vještina. Naprimjer, važno je da **znanje nije tako strukturirano da se ne razmjenjuje**, jer to ometa efikasnost istraga. Predviđeno rješenje je razmišljanje o dvosmjernom sistemu obuke između službenika specijaliziranih za borbu protiv trgovine ljudima i službenika specijaliziranih za IKT. Druga strategija je širenje određenog stepena vještina u oblasti IKT-a među različitim jedinicama, uključujući i jedinice za borbu protiv trgovine ljudima. Gledajući u budućnost, **rizik od uskih grla** je posebno akutan. S obzirom na to da će se zločini posredstvom IKT-a, uključujući trgovinu ljudima, vjerovatno povećavati, postoji potreba da se ne oslanjamo previše na

centralizirane centre za borbu protiv visokotehnološkog (cyber) kriminala. U idealnom slučaju takve centre bi trebalo pozivati samo u slučajevima koje karakterizira veoma visok nivo tehnološke sofisticiranosti – što ne izgleda kao tipičan slučaj trgovine ljudima posredstvom IKT-a. Kako bi se izbjegla uska grla u sistemu, ključno je uključiti opća/osnovna **znanja o visokotehnološkom kriminalu u rutinske obuke** koje se pružaju za istražitelje, a ne da se ovo posmatra kao skup „specijaliziranih" vještina.

Na osnovu dokaza dobijenih od država ugovornica, možemo identificirati šest širokih oblasti koje se smatraju kritičnim za razvoj kapaciteta. One uključuju:

- prikupljanje i analizu informacija iz otvorenih izvora (OSINT);
- prikupljanje podataka s profila na društvenim mrežama i aplikacija za komunikaciju, kao i s mračne/TOR mreže;
- ispitivanje informacija koje se nalaze na uređajima za komunikaciju i čuvanje informacija, uključujući informacije koje su korisnici izbrisali, kao i znanje o šifriranju;
- sposobnost potkrepljivanja podataka dobijenih iz IKT izvora dodatnim dokazima stečenim tokom krivične istrage;
- identifikacija žrtava/potencijalnih žrtava u online okruženju;
- obuka o ekonomskom i finansijskom kriminalu s elementom posvećenim online transakcijama i potencijalno kriptovalutama.

4.1.1. Dizajniranje budućih obuka i dobrih praksi

Dokazi pribavljeni od država ugovornica ukazuju na niz konkretnih inicijativa koje bi se mogle usvojiti kako bi se ojačale odredbe o obukama u kontekstu trgovine ljudima posredstvom interneta i tehnologije. U nastavku su navedeni neki prijedlozi o dizajnu budućih modula obuke.

- Kreiranje studija slučaja i scenarija zasnovanih na trgovini ljudima koji će biti uključeni u **obuku o „digitalnoj istrazi"**. Takva obuka se može podijeliti na dva nivoa: nivo 1 bi se mogao organizirati za sve službenike na prvoj liniji, dok bi nivo 2 mogao uključivati napredne obuke koje se organiziraju za manji broj polaznika. Moguće je da bi barem dio ovih obuka bio organiziran u obliku učenja u manjim grupama kako bi se potakla razmjena ideja i diskusija o praksi.

- **Dodavanje elementa IKT-a u postojeće obuke o trgovini ljudima**. Iako je nekoliko država spomenulo organiziranje obuka o trgovini ljudima, samo nekolicina je izričito ukazala na uključivanje elemenata fokusiranih na IKT u ove obuke. Kako se sve više interakcija odvija na internetu, ključno je uključiti elemente IKT-a u „tradicionalne" obuke o trgovini ljudima. Tehnička obuka može uključivati elemente o najboljim praksama u istraživanju trgovine ljudima posredstvom IKT-a, kao i o nacionalnim i međunarodnim iskustvima.

- Organiziranje zajedničkih obuka koje uključuju više država i koje su osmišljene imajući u vidu aktuelne trendove. Naprimjer, ako postoje dokazi da se žrtve obično regrutiraju u državi A, a zatim eksploatiraju u državi B, moglo bi biti korisno organizirati zajedničku obuku koja uključuje službenike iz država A i B. Po ugledu na zajedničke istražne timove (ZIT), mogli bismo označiti takve aktivnosti kao **ZAO („zajedničke aktivnosti obuke")**.

- Izbor službenika bez policijskih ovlaštenja koji posjeduju tehničke vještine. Ti službenici mog integrirati specijalizirane jedinice (npr. jedinice za borbu protiv trgovine ljudima) da

interno razvijaju znanja o tehničkim pitanjima IKT-a i da ih šire unutar jedinice/organizacije.

- Organiziranje zajedničkih obuka koje **okupljaju specijalizirane istražitelje i tužioce** kako bi se obje grupe aktera upoznale s mogućnostima koje nude nove istražne metode, npr. korištenje cyber infiltracije ili tajnih operacija na internetu, kao i prikupljanje elektronskih dokaza (uključujući zapljenu virtuelne imovine). Takva obuka može obuhvatiti i tehničke i pravne aspekte u cilju poboljšanja upotrebe novih metoda orijentiranih na IKT među istražiteljima i tužiocima.

- **Razmjena znanja na međunarodnom nivou**, npr. kroz učešće u međunarodnoj/regionalnoj obuci fokusiranoj na specifične aspekte istrage trgovine ljudima posredstvom IKT-a (primjeri koje navode države ugovornice uključuju seminar „Međunarodna saradnja u oblasti visokotehnološkog kriminala i elektronskih dokaza" u organizaciji Vijeća Evrope i Zajedničkog projekta EU Cyber@East (održan 7–9. decembra 2020).

Države su navele niz konkretnih inicijativa kao primjere dobrih praksi, koje donosimo u nastavku teksta.

- U Austriji Zajednička operativna kancelarija za borbu protiv trgovine ljudima i krijumčarenja ljudi (sektor u okviru Kriminalističke obavještajne službe) organizira obuke i seminare o trgovini ljudima, prekograničnoj trgovini prostitucijom i identifikaciji žrtava. Posebna obuka je organizirana za Policiju Austrije, pravosudne organe, Saveznu kancelariju za imigraciju i azil (BFA), Savezni upravni sud (BVwG), nadležne organe u oblasti finansija, inspekcije rada i usluge pravnog savjetovanja o otkrivanju slučajeva trgovine ljudima na internetu, uključujući na društvenim medijima. Ono što je najvažnije, takva obuka je premašila granice organa za provođenje zakona i uključivala je inspekciju rada, savjetodavne službe i nadležne organe u oblasti finansija. Osim toga, policijski službenici specijalizirani za IKT prošli su posebnu obuku fokusiranu na trgovinu ljudima u svrhu seksualne eksploatacije. S druge strane, službenici specijalizirani za IKT pružali su obuku kolegama specijaliziranim za trgovinu ljudima/prekograničnu trgovinu prostitucijom u Kriminalističkoj obavještajnoj službi/CID. Ovo je dobar primjer dvosmjerne obuke o kojoj je ranije bilo riječi – i pruža obrazac koji bi se potencijalno mogao koristiti i na drugim mjestima.

- U Bugarskoj je 2020. godine organiziran niz specijaliziranih radionica za policijske službenike, tužioce i sudije gdje se diskutiralo o istraživanju i krivičnom gonjenju osoba uključenih u slučajeve trgovine ljudima pomoću podataka iz otvorenih izvora, uključujući online podatke.

- U okviru partnerskih sporazuma s Rumunijom i Bugarskom u oblasti trgovine ljudima, Norveška će organizirati dvije zajedničke aktivnosti obuke na temu obavještajnih podataka iz otvorenih izvora (OSINT) za učesnike iz Rumunije i Norveške. Cilj obuke je da se poboljša sposobnost istražitelja u Norveškoj, Bugarskoj i Rumuniji da identificiraju i istraže trgovinu ljudima posredstvom IKT-a.

- U Grčkoj obuke i obrazovne inicijative o visokotehnološkom kriminalu imaju dvosmjerni pristup:

- (a) skup univerzitetskih kurseva za poboljšanje razumijevanja visokotehnološkog kriminala među budućim generacijama naučnika i studenata prava, i (b) skup kraćih kurseva obuke za službenike za provođenje zakona, pravosudne organe i zaposlene u privatnom sektoru kako bi se poboljšalo njihovo razumijevanje visokotehnološkog kriminala i unaprijedili

njihovi svakodnevni odgovori.

- U Britaniji organi za provođenje zakona imaju formalne standardne operativne procedure (SOP) ili druge smjernice za proaktivno praćenje, otkrivanje, istraživanje i ometanje trgovine ljudima posredstvom IKT-a. Ovo uključuje: mapiranje online platformi na kojima je rizik od trgovine ljudima visok; vođenje tajnih operacija na internetu; korištenje specifičnih indikatora potencijalne trgovine ljudima na online platformama; analizu i upravljanje prijavama primljenim putem telefonskih linija za prijavu seksualnog zlostavljanja i eksploatacije djece na internetu; upotrebu specifičnih tehnoloških alata za borbu protiv trgovine ljudima. Pored toga, istražitelji prolaze obuku o tome kako da efikasno spoje informacije iz otvorenih izvora s različitim oblicima obavještajnih podataka.
- U Francuskoj obuka prvog nivoa za policijske službenike uključuje module o osnovama digitalne istrage; anonimnosti, mračnim mrežama i virtuelnim valutama; analizi okruženja za izvršenje krivičnih djela visokotehnološkog kriminala; istraživanju interneta i društvenih mreža (ovo obično prati specijalizacija na određenu temu, naprimjer prevara ili seksualno zlostavljanje djece); prvim osobama koje reagiraju na visokotehnološki kriminal (tj. očuvanju digitalnog mjesta zločina). Dalje specijalizirane obuke uključuju module o: istraživanju visokotehnološkog kriminala (prikupljanje, obrada i analiza dokaza s mobilnih telefona i računara); sudskim istražnim aktima u vezi s digitalnim tehnologijama, uključujući pravna pitanja, međunarodnu saradnju i istražne strategije; obuci za analitičare digitalnih tragova; prikupljanju telefonskih podataka; istragama pod pseudonimima. Trenutno je u fazi izrade jednosedmična obuka posvećena borbi protiv trgovine ljudima u svrhu radne eksploatacije (s ciljem da se organizira u prvoj polovini 2022. godine). Ova obuka će uključivati modul posvećen korištenju tehnoloških alata.

4.2. Obuka tužilaca i sudija

Prema dostavljenim dokazima, organiziranje obuka za tužioce i sudije u vezi s trgovinom ljudima posredstvom IKT-a prilično je neujednačeno u različitim državama ugovornicama. Nekoliko država je navelo da trenutno ne organizira nikakve obuke za pravosuđe o ovoj pojavi. Druge države organiziraju opće obuke o trgovini ljudima bez elemenata posebno fokusiranih na pitanja vezana za IKT. Druga grupa država navela je da organizira obuke o tome kako se koriste međunarodni pravni instrumenti u kontekstu visokotehnološkog kriminala, npr. Budimpeštanska konvencija i srodno nacionalno zakonodavstvo i/ili o tome kako se razvijaju predmeti visokotehnološkog kriminala. Na kraju, grupa država je u svoje obuke uključila elemente kriptovaluta i znanja o specifičnim tehnološkim alatima. U idealnom slučaju sve države bi trebale težiti **integriranju obuke o trgovini ljudima u vezi s IKT-om, upotrebi međunarodnih pravnih instrumenata u kontekstu visokotehnološkog kriminala**, kao i implikacijama upotrebe specifičnih tehnoloških alata prilikom istraživanja slučajeva trgovine ljudima (npr. sistemi za skeniranje mreže ili softver za dešifriranje informacija).

Čini se da je manji broj država integrirao studije slučaja u vezi s trgovinom ljudima u svoje obuke o visokotehnološkom kriminalu. Slično tome, manji broj država je naveo da organizira obuke koje uključuju elemente trgovine ljudima i IKT-a.

Države su u svojim odgovorima na upitnik navele niz konkretnih inicijativa kao primjere dobrih praksi, a navedene su u nastavku.

- U Republici Moldaviji tokom prve polovine 2021. godine Nacionalni institut za

pravosuđe je organizirao obuku za 110 polaznika koja je pokrivala aspekte istraga trgovine ljudima posredstvom IKT-a. Obuka je uključivala sesije o (a) „karakteristikama istraga i suđenja za krivična djela u vezi s trgovinom ljudima i tjelesnim elementima"; (b) „karakteristikama istraga i procesuiranju krivičnih djela u oblasti borbe protiv trgovine ljudima"; (c) „karakteristikama istraga i suđenja u predmetima koji se tiču prekograničnog, transnacionalnog i organiziranog kriminala".

- U Bugarskoj Tužilaštvo Vrhovnog suda održalo je seminare za istražitelje i tužioce o trgovini ljudima i upotrebi IKT-a u trgovini ljudima. Tužilaštvo smatra da su „posebno efikasne radionice koje vode stručnjaci iz oblasti IKT-a, koje predstavljaju praktične primjere korištenja softverskih programa, kao i mogućnosti i operativne alate za korištenje mobilnih aplikacija u svrhu otkrivanja teških krivičnih djela".
- U Švedskoj postoje tužioci specijalizirani za IKT, od kojih se neki bave predmetima trgovine ljudima. Tužilaštvo organizira internu obuku o vođenju istraga o krivičnim djelima u vezi s IKT-om (uključujući upotrebu kriptovaluta u kriminalnim aktivnostima). Brojni tužioci koji se bave predmetima trgovine ljudima prisustvovali su ovim obukama. Osim toga, Akademija za pravosudnu obuku, koja je dio švedske Nacionalne sudske uprave i odgovorna je za pravosudnu obuku sudija i drugog pravnog osoblja, organizira obuku o krivičnim djelima posredstvom IKT-a na različitim nivoima.
- Latvijski nadležni organi su uputili na međunarodnu obuku o trgovini ljudima i visokotehnološkom kriminalu koju je organiziralo poljsko Tužilaštvo za tužioce specijalizirane za organizirani kriminal (21–23. oktobra 2019. godine u Krakovu).

Na kraju, nekoliko država je istaklo značaj unapređenja obuka za sudije i tužioce u vezi s elektronskim dokazima.

POLJE | Obuke za NVO

NVO pružaju ključne obuke i stručnost na osnovu svog svakodnevnog iskustva u pomaganju i savjetovanju žrtava – uključujući policiju i ugrožene zajednice i pojedince. Međutim, NVO su izrazile potrebu da im organi za provođenje zakona i međunarodne organizacije organiziraju obuke o najnovijim dostignućima u tehnološkom okruženju i u oblasti trgovine ljudima, uključujući promjene u strategijama regrutiranja.

Također su istakli potrebu za obukama o najboljim praksama i razmjenom iskustava među državama. Ovo je naročito relevantno za dizajniranje i koordinaciju kampanja koje uključuju države porijekla i države odredišta.

Iako neke NVO imaju stručnjake za pitanja sigurnosti na internetu, generalno i dalje postoji nedostatak obuke o tehnologiji, uključujući i obuke o upotrebi posebnih alata za identifikaciju i pomoć žrtvama. Kako je istakla organizacija La Strada International, to je „zbog nedostatka resursa i kapaciteta" jer je „već teško prikupiti dovoljno sredstava za osnovne programe podrške".

5. Pravni instrumenti

Ovo poglavlje istražuje međunarodne pravne instrumente od značaja za borbu protiv trgovine ljudima posredstvom interneta i IKT-a. Pregled pravnih okvira specifičnih za državu koji se odnose na identifikaciju i uklanjanje sadržaja u vezi s trgovinom ljudima, kao i domaćih pravnih instrumenata koji su općenito relevantni za borbu protiv trgovine ljudima, dostupan je u Web-prilogu.

5.1. Međunarodni pravni instrumenti

Države ugovornice su identificirale određeni broj pravnih instrumenata koji su značajni za borbu protiv trgovine ljudima posredstvom IKT-a. Većina instrumenata je općeg karaktera i ima za cilj borbu protiv trgovine ljudima, bez obzira na modus operandi trgovaca ljudima. Najrelevantniji instrument usmjeren ka kriminalu posredstvom IKT-a je Budimpeštanska konvencija Vijeća Evrope (Konvencija o visokotehnološkom kriminalu), koju nekoliko država ugovornica navodi kao „važan" alat. S obzirom na njen značaj, primjena Konvencije o visokotehnološkom kriminalu u kontekstu trgovine ljudima razmatra se u posebnom odjeljku u nastavku. Dodatni instrumenti koje su identificirale države ugovornice su sljedeći:

- Konvencija UN-a protiv transnacionalnog organiziranog kriminala i njen Protokol za sprečavanje, suzbijanje i kažnjavanje trgovine ljudima, posebno trgovine ženama i djecom (2000);
- Evropska konvencija VE o ekstradiciji (ETS br. 024);
- Evropska konvencija VE o uzajamnom pružanju pomoći u krivičnim stvarima (ETS br. 030);
- Konvencija VE o borbi protiv trgovine ljudima (CETS br. 197);
- Direktiva 2011/36/EU Evropskog parlamenta i Vijeća od 5. aprila 2011. godine o sprečavanju i borbi protiv trgovine ljudima i zaštiti žrtava;
- Akt Vijeća od 29. maja 2000. godine kojim se u skladu s članom 34. Ugovora o Evropskoj uniji uspostavlja Konvencija o uzajamnom pružanju pomoći u krivičnim stvarima između država članica Evropske unije.

O povezanim pitanjima seksualnog zlostavljanja djece:

- Konvencija VE o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja (Lanzarot konvencija, CETS br. 201);
- Direktiva 2011/93/EU Evropskog parlamenta i Vijeća od 13. decembra 2011. godine o borbi protiv seksualnog zlostavljanja i seksualne eksploatacije djece i dječije pornografije;
- Odluka Vijeća Evropske unije od 29. maja 2000. godine o borbi protiv dječije pornografije na internetu 2000/375/PUP.

O radnoj eksploataciji:

- Međunarodna organizacija rada, Konvencija br. 189 i Preporuka br. 201 o dostojanstvenom radu domaćih radnika, 2011;
- Međunarodna organizacija rada, Protokol iz 2014. uz Konvenciju o prinudnom radu, 1930.

Pored toga, države ugovornice su identificirale niz međunarodnih agencija i programa koji su

od ključnog značaja za unapređenje međunarodne pravne saradnje, također u kontekstu trgovine ljudima posredstvom IKT-a. Oni uključuju:

- Interpol;
  - Projekt IWOL (blokiranje domena koji se odnose na seksualnu eksploataciju djece);
- Europol;
  - EMPACT (trgovina ljudima);
  - Dani zajedničkog djelovanja;
- Eurojust;
- Selec (Centar za provođenje zakona u jugoistočnoj Evropi).

Na kraju, niz specifičnih operativnih instrumenata proizlazi iz dokaza koje su dostavile države ugovornice. Ovaj skup uključuje sljedeće instrumente:

- zahtjevi za pravnu pomoć;
- evropski nalog za hapšenje;
- evropski nalog za istragu;
- zajednički istražni timovi;
- sistem EU Prüm (razmjena nacionalnih podataka o DNK, otiscima prstiju i registracijama vozila);
- EU evidencija imena putnika (PNR);
- Europol SIENA;
- službenici za vezu;
- Interpolov sistem za obavještenja.

5.1.1. Nedostaci postojećeg okvira

Općenito posmatrano, države ugovornice su izrazile pozitivan i podržavajući stav o dostupnim pravnim instrumentima koji omogućavaju saradnju među državama u borbi protiv trgovine ljudima. Konvencije VE o (a) uzajamnom pružanju pravne pomoći i (b) o visokotehnološkom kriminalu smatraju se „najčešće" korištenim instrumentima i, generalno, ocijenjene su kao „adekvatne". Ipak, države ugovornice su identificirale neke potencijalne nedostatke i oblasti u kojima bi se postojeće zakonodavstvo moglo poboljšati. Imajte na umu da ove praznine odražavaju – i dopunjuju – izazove vezane za istragu trgovine ljudima posredstvom IKT-a i krivično gonjenje osoba uključenih u ovakvu trgovinu, o čemu je već bilo riječi u Poglavlju 1 – i treba ih čitati zajedno s takvom analizom.

Glavni nedostaci koje su identificirale države ugovornice odnose se na sljedeće:

- odsustvo zajednički dogovorenog (standardiziranog) pravnog okruženja koje podržava razmjenu između pružalaca internetskih usluga i nadležnih organa kada se bave specifičnim istragama;
- odredbe koje omogućavaju blagovremeni odgovor privatnih kompanija na zahtjeve za dostavljanje podataka kako bi se izbjegla duga kašnjenja u dostavljanju takvih podataka. Međutim, takve odredbe trebaju uzeti u obzir da bi veoma kratki rokovi mogli kazniti manje pružaoce usluga u korist velikih pružalaca usluga jer ovi drugi mogu lakše priuštiti skupe automatizirane sisteme i/ili usluge na poziv (kao što su istakli švicarski nadležni organi);

- odredbe kojima se primoravaju privatne kompanije da otkriju informacije na direktan zahtjev/nalog druge države;
- odredbe kojima se provode zajednička pravila o čuvanju podataka;
- odredbe za olakšavanje prikupljanja svjedočenja žrtava i korištenje svjedočenja u drugoj državi. Ovo bi ublažilo poteškoće s kojima se države suočavaju u uvjeravanju žrtava da svjedoče na suđenjima zbog niza razloga, uključujući mobilnost žrtava, poteškoće u njihovom lociranju i stalnu ranjivost;
- odredbe u vezi sa šifriranjem (npr. pružaoci usluga nisu u obavezi da uklone šifriranje kada predaju materijale nadležnim organima);
- pitanja u vezi s transnacionalnim mjerama protiv web-lokacija na kojima se nalaze materijali koji se mogu povezati s olakšavanjem eksploatacije žrtava. Ovo je posebno složeno pitanje jer je usko isprepleteno s razlikama među državama ugovornicama u njihovom pristupu aktivnostima prostitucije – i različitim režimima usvojenim u različitim državama:
- odredbe koje uvode obavezu stalnog praćenja od strane kompanija u njihovom čitavom lancu snabdijevanja, ciljajući naprimjer na korištenje IKT-a u kontekstu zapošljavanja (naprimjer, francuski Zakon br. 399/2017 o obavezi stalnog praćenja i Zakon o modernom ropstvu Ujedinjenog Kraljevstva iz 2015. godine, kojim se uvodi obaveza transparentnosti u lancima snabdijevanja);
- upotreba terminologije koja ne dozvoljava uvijek da se zakonodavstvo razvija paralelno s promjenama u modusu operandi trgovaca ljudima;
- razlike u prenošenju krivičnog djela trgovine ljudima (prema Protokolu UN-a iz Palerma) u nacionalno zakonodavstvo. Ove razlike mogu predstavljati izazove za međunarodnu saradnju, naprimjer oko pitanja koja se odnose na nedostatak pristanka i prinudu žrtve;
- evropski nalog za hapšenje smatra se vrijednim sredstvom; međutim, neke relevantne države porijekla su često izvan pravosudnog okvira EU;
- evropskim nalozima za istragu (EIO) može nedostajati fleksibilnost, npr. može se javiti potreba za novim EIO ako istraga krene u novim pravcima, a oni mogu biti podložni dugim rokovima za odgovor;
- zajednički istražni timovi (ZIT) smatraju se „efikasnim" sredstvom; međutim, oni mogu biti (a) složeni za provođenje; i (b) zahtijevaju identičnu istragu u partnerskoj državi ili u više njih.

5.2. Budimpeštanska konvencija (o visokotehnološkom kriminalu) i borba protiv trgovine ljudima posredstvom IKT-a

Među državama ugovornicama postoji opća saglasnost o značaju Konvencije o visokotehnološkom kriminalu – pri čemu je mnoge države navode kao „veoma značajan alat". Nekoliko država ugovornica smatra Konvenciju o visokotehnološkom kriminalu ključnim **alatom za podršku** u borbi protiv trgovine ljudima posredstvom IKT-a.

Prema dostavljenim dokazima, države ugovornice smatraju odredbe koje se odnose na **procesno pravo** najvrednijim u kontekstu trgovine ljudima posredstvom IKT-a (poglavlje II, odjeljak 2. Konvencije), a ne mjere materijalnog krivičnog prava predviđene poglavljem II, odjeljak 1. Najvažnije je da oblast primjene odredbi procesnog prava nije zavisan od izvršenja krivičnog djela navedenog u tački 1. poglavlja II. Predmeti trgovine ljudima posredstvom IKT-a vjerovatno će potpasti ili pod „krivična djela počinjena pomoću računarskog sistema" ili, u

najmanju ruku, u djela koja zahtijevaju „prikupljanje dokaza u elektronskom obliku" (član 14, stav 2). Slično tome, član 23. navodi da se principi koji podržavaju međunarodnu saradnju u kontekstu Konvencije primjenjuju na „istrage ili postupke koji se tiču krivičnih djela u vezi s računarskim sistemima i podacima, ili u svrhu prikupljanja dokaza o krivičnom djelu u elektronskoj formi" (dodat kurziv). Države ugovornice su istakle **značaj da se procesne mjere ne ograniče samo na krivična djela koja su izričito navedena** (npr. ona u poglavlju II, odjeljak 1). Međutim, izgleda da se ne slažu baš sve države oko ovog šireg tumačenja oblasti primjene Konvencije.

Konvencija jasno ostvaruje svoj puni potencijal samo kada nije ograničena na krivična djela koja su izričito navedena u poglavlju II, odjeljak 1. Ovo je naročito tačno u kontekstu trgovine ljudima posredstvom IKT-a. Kao što su primijetili nadležni organi Finske, između ostalog, „odredbe materijalnog krivičnog prava iz Budimpeštanske konvencije [koje] pokrivaju krivična djela u vezi s računarom, kao što su nezakonit pristup, mijenjanje podataka, računarsko falsificiranje i kršenje autorskih prava i druga slična krivična djela, rijetko su relevantne ili uopće nisu relevantne u kontekstu trgovine ljudima". Naprotiv, nekoliko država ugovornica je navelo da su se oslanjale na odredbe Konvencije o čuvanju podataka u kontekstu istraga trgovine ljudima (posebno na članove 16–21).

Nekoliko država je ukazalo na korisnost odredbi navedenih u poglavlju III Konvencije (o međunarodnoj saradnji) kao pravne osnove za prikupljanje i razmjenu elektronskih dokaza među državama. Mehanizmi uzajamne pomoći predviđeni poglavljem III Konvencije (članovi 29–34) smatraju se „korisnim". Nekoliko država je izričito naznačilo da su se ranije oslanjale na njih. Članovi 29. i 31. se najčešće spominju; član 30. nije izričito spomenut u prijavama; ipak, mogao bi ponuditi koristan alat u kontekstu trgovine ljudima posredstvom IKT-a.

Uspostavljanje **mreže kontaktnih tačaka** dostupnih 24/7 (član 35) također se smatra važnom odredbom, posebno u kontekstu prikupljanja elektronskih dokaza. Ključno je, međutim, da kontaktne tačke budu lako dostupne iz svake države. Ovo govori o problemu **uskih grla unutar sistema**. Ključno je mjesto gdje se kontaktna tačka nalazi u sistemu krivičnog pravosuđa – i to može biti od velikog značaja. Primjenjuju se različiti modeli. U Republici Moldaviji, naprimjer, takva kontaktna tačka nalazi se pri Upravi za istrage visokotehnološkog kriminala; na Malti pri Policijskoj jedinici za visokotehnološki kriminal, a u Poljskoj pri Birou za borbu protiv visokotehnološkog kriminala Centralnog štaba nacionalne policije. U Francuskoj se nalazi pri Centralnom uredu za borbu protiv kriminala u oblasti informacijskih i komunikacijskih tehnologija (OCLCTIC), dok se u Latviji takva kontaktna tačka nalazi pri Odjeljenju za međunarodnu saradnju državne policije. Nadležni organi u Bosni i Hercegovini su izričito naveli svoje „veoma pozitivno iskustvo" uslijed činjenice da se kontaktna tačka dostupna 24/7 „ne nalazi u jedinici koja se bavi visokotehnološkim kriminalom". Gledajući u budućnost, vjerovatno je da će, sa sve centralnijom ulogom koju igraju IKT i elektronski dokazi, takve kontaktne tačke biti pod sve većim pritiskom – i brzo preopterećene ako ne budu imale adekvatno osoblje. Samostalne jedinice za podršku bi možda bile poželjnije od jedinica za visokotehnološki kriminal – idealno s osobljem koje posjeduje stručnost u različitim oblastima i vrstama kriminala, uključujući trgovinu ljudima posredstvom IKT-a. Međutim, bez obzira na izabrani model, država treba voditi računa o pitanju uskih grla.

5.2.1. Pogled u budućnost: kako se Konvencija o visokotehnološkom kriminalu može dalje primjenjivati u borbi protiv trgovine ljudima

Nekoliko država je istaklo značaj Drugog dodatnog protokola uz Konvenciju. U nekoliko prijava je navedeno da će Drugi dodatni protokol stvoriti vrijedne alate za organe za provođenje zakona – koji će se koristiti i u kontekstu trgovine ljudima posredstvom IKT-a – što će unaprijediti prekogranične krivične istrage i dalje unaprijediti saradnju u vezi s osiguravanjem elektronskih dokaza. Članovi koji su istaknuti kao posebno relevantni uključuju odredbe koje se odnose na zajedničke istrage, uključujući zajedničke istražne timove; ubrzano otkrivanje sačuvanih računarskih podataka; hitnu uzajamnu pomoć i direktno otkrivanje informacija o pretplatnicima.

Osim toga, države ugovornice su predložile sljedeće aktivnosti za poboljšanje borbe protiv trgovine ljudima posredstvom IKT-a kroz primjenu konvencija o visokotehnološkom kriminalu:

- potpuno usaglašavanje svih nacionalnih zakonodavstava s Konvencijom o visokotehnološkom kriminalu kako bi se iskoristio puni potencijal koji ova konvencija nudi;
- šira i poboljšana obuka o mogućnostima koje nudi Konvencija o visokotehnološkom kriminalu. Iz prijava proizlazi da trenutno ne koriste sve države ugovornice alate predviđene Konvencijom u njihovom punom potencijalu;
- više jasnoće u vezi s oblašću primjene odredbi procesnog prava koje su već uključene u Konvenciju i njene dodatne protokole jer se pojavio određeni stepen neslaganja među državama ugovornicama o tome u kojoj mjeri se postojeće odredbe mogu primijeniti na slučajeve trgovine ljudima. Dok neke države ugovornice smatraju da, sve dok pokriva elektronske dokaze, Konvencija o visokotehnološkom kriminalu može biti u potpunosti primijenjena, druge države su upozorile da primjena Konvencije i Protokola, uključujući Drugi dodatni protokol, zahtijeva „prikladne predmete" (u prijavama nije navedeno šta čini predmet „prikladnim");
- neke države ugovornice su izrazile stav da Drugi dodatni protokol treba uključiti odredbe koje jačaju razmjenu elektronskih dokaza, poboljšavaju modalitete uzajamne pravne pomoći, potiču saradnju s pružaocima internetskih usluga i poboljšavaju prekogranični pristup podacima;
- manji broj država ugovornica smatra da Konvenciju o visokotehnološkom kriminalu treba dopuniti ili izmijeniti kako bi izričito predviđala trgovinu ljudima u svojoj oblasti primjene. Bugarski nadležni organi su izrazili potrebu za izradom „kataloga krivičnih djela" na koja se mogu primijeniti alati sadržani u Konvenciji o visokotehnološkom kriminalu i dodatnim protokolima. Međutim, čini se da ovo gledište nije općeprihvaćeno među državama ugovornicama jer se čini da postoji opća preferencija za šire tumačenje oblasti primjene Konvencije zasnovano na (širokom) zahtjevu „prikupljanja dokaza u elektronskom obliku" (vidjeti također iznad);
- slovački nadležni organi su predložili provođenje procedure za ubrzanje pružanja UPP pružanjem mogućnosti da se zahtjev pošalje direktno subjektu koji se nalazi u stranoj državi pod uvjetom da se o tome obavijesti pravosudni organ te države.

POLJE | Izazovi koje su identificirale NVO

Općenito govoreći, NVO smatraju da su izazovi uglavnom posljedica provođenja postojećih odredbi, uključujući i nedostatak resursa koji su na raspolaganju organima za provođenje zakona i organizacijama za podršku, a ne po slovu važećih zakonskih odredbi.

Organizacija La Strada International primijetila je „**jasna ograničenja" koja su uvedena zakonodavstvom o zaštiti podataka (GDPR) i pravilima privatnosti**. Primjer je „zakon o e-privatnosti koji je predložila EU, a koji je spriječio tehnološke kompanije da skeniraju internet u potrazi za slučajevima seksualne eksploatacije djece na internetu" (sada privremeno suspendiran nakon protivljenja mnogih OCD). Organizacija Sustainable Rescue Foundation je ukazala na „jasan prijelaz s fizičkih dokaza na digitalne podatke" koji stvara potrebu za „digitalnom forenzikom kao prihvatljivim dokazom za policiju i tužioce" u svim državama. Ostali izazovi koje su prepoznali odnose se na GDPR u EU; ažuriranje propisa i sudske prakse tako da uzimaju u obzir visokotehnološki kriminal i internet; osmišljavanje zakonodavstva i operativnih pravila prilagođenih digitalnim istragama.

Fondacija Sustainable Rescue Foundation je također predložila da se zakonodavstvo protiv finansijskog kriminala razmotri kao rješenje za problem pretvaranja informacija u prihvatljive dokaze. Naprimjer, južnoafrička integrirana radna grupa za borbu protiv pranja novca, koja predstavlja partnerstvo između javnih subjekata i finansijskog sektora, može podnijeti zahtjev za izdavanje sudskog naloga kojim bi se odobrio pristup relevantnim informacijama koje se nalaze u posjedu finansijskih i drugih institucija. Putem izjave pod zakletvom, ove informacije (tj. finansijske analize finansijskih podataka dobijenih posredstvom suda) mogu zatim koristiti agencije za provođenje zakona.

6. Ljudska prava, etika i zaštita podataka

6.1. Dokazi prikupljeni od država ugovornica

Što se tiče **obrade i zaštite podataka**, sve države ugovornice su ukazale na usvajanje zakona o zaštiti podataka – koji su često usklađeni s Uredbom EU 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. godine (koja se također naziva Općom uredbom EU o zaštiti ličnih podataka: GDPR) i/ili Konvencijom VE o zaštiti lica u odnosu na obradu ličnih podataka (ETS br. 108, revidirano 2018. godine kao verzija 108+). Principi zaštite podataka slični su u svim državama ugovornicama. To uključuje zakonitost, ograničenje svrhe, minimiziranje i srazmjernost podataka, tačnost, ograničenje čuvanja, integritet i povjerljivost. Nije moguće izvršiti evaluaciju provođenja takvih principa na osnovu dokaza pruženih u odgovorima na upitnik.

Što se tiče **ljudskih prava** i **lične zaštite žrtava**, jedan broj država je ukazao na uvođenje mjera za sprečavanje počinilaca da stupe u kontakt sa žrtvama; ispitivanje svjedoka putem videokonferencije kako bi se spriječio kontakt s optuženima; a u nekim slučajevima i mogućnost da žrtve anonimno pruže dokaze na sudu kako bi se zaštitila njihova privatnost. Žrtve se mogu smjestiti u **skloništa** i može im se pružiti pomoć.

U Francuskoj korisnici platforme za prijavljivanje seksualnog i rodno zasnovanog nasilja moraju **dati saglasnost za prikupljanje ličnih podataka** kada se prvi put povežu s platformom. Ova saglasnost se obnavlja tokom razgovora. Međutim, nije obavezno da se navede identitet pojedinca da bi se pristupilo sobi za chat – na taj način se omogućavaju anonimni kontakti.

Što se tiče **podataka prikupljenih tokom policijskog rada**, uključujući istrage, države ugovornice su istakle da zakoni i propisi obično propisuju da su takve informacije podložne povjerljivosti i da se mogu dijeliti samo u veoma ograničenim okolnostima uz stroge procedure i ovlaštenja. Države ugovornice su navele da su pravila prema kojima policijske snage mogu registrirati podatke u određenim bazama podataka obično usklađena s Direktivom o policiji EU. Pojedinačne države mogu imati strože nacionalne zahtjeve. Kako su istakli norveški nadležni organi, posebne kategorije ličnih podataka, naprimjer o seksualnoj orijentaciji, vjeroispovijesti i političkim stavovima, mogu biti predmet dodatnih zahtjeva i „mogu se obrađivati samo kada je 'strogo neophodno' u prethodno utvrđene svrhe". Isti skup pravila i zaštitnih mjera najčešće pokriva sve istrage i obavještajni rad, uključujući trgovinu ljudima posredstvom IKT-a. Od ključnog je značaja da osoblje za provođenje zakona bude adekvatno obučeno o regulatornim i etičkim odredbama koje uređuju obradu ličnih podataka.

Rad policije također treba **postići ravnotežu između različitih potreba i prava**. Naprimjer, kako su primijetili finski nadležni organi, nalog kojim se ograničava pristup elektronskoj komunikaciji „može se izdati samo ako se koristi od zabrane pristupa informacijama mogu smatrati znatno većim od ograničenja slobode izražavanja i drugih osnovnih prava korisnika mreže" (član 185. Zakona o elektronskim komunikacijskim uslugama 917/2014). Pored toga, mora biti „tehnički proveden na takav način da zaštita povjerljivosti komunikacije ne bude ugrožena". Općenito govoreći, član 226c istog zakona propisuje da „mjere koje se odnose na uvjete korištenja platformi za dijeljenje videozapisa moraju biti srazmjerne prirodi predmetnog sadržaja i moraju uzeti u obzir, naprimjer, potencijalnu štetu i prava pružalaca usluga i korisnika". Finski nacionalni istražni biro je sam identificirao probleme

privatnosti u vezi s korištenjem eksternih tehničkih alata i prijavio ih je Odboru nacionalne policije.

Države ugovornice su navele da imaju uspostavljene **starosno osjetljive protokole** koji se odnose na različite skupove procedura i zaštitnih mjera koje se primjenjuju u zavisnosti od toga da li je žrtva dijete. Naprimjer, djeca su obično smještena u zasebnim centrima za podršku; koriste se različite tehnike i sobe za ispitivanje, često uz prisustvo psihologa. U nekim državama krivične postupke protiv djece vode isključivo policijski službenici posebno obučeni za rad s djecom i maloljetnicima.

6.2. Dokazi prikupljeni od nevladinih organizacija

NVO su naglasile značaj pravila – i svijest o pravilima – za zaštitu podataka, povjerljivosti, sigurnog čuvanja, kao i procedura oko pristanka.

Dokazi nekoliko nevladinih organizacija pokazuju da, u okviru standardne procedure, organizacije traže pristanak žrtve prije nego što podijele informacije s organima za provođenje zakona. Kao što je istakao FIZ (Švicarska), ova saglasnost se također odnosi na dijeljenje podataka o SIM kartici i akreditiva za društvene mreže. Organizacija La Strada International je navela da njeni članovi „ne prosljeđuju nikakve informacije policiji bez pristanka žrtve, osim u slučaju postojanja opasne situacije u kojoj je potrebna hitna reakcija". Problem nastaje kada žrtve oklijevaju da podnesu pritužbu policiji „zbog rizika koje to nosi, uključujući rizike da njihova situacija postane poznata drugima, pored rizika od odmazde". Organizacija La Strada International ocjenjuje da je to slučaj s „mnogim žrtvama trgovine ljudima".

Organizacija Different and Equal (Albanija) spomenula je upotrebu sigurnosnih protokola u svakoj komunikaciji s agencijama za provođenje zakona, uključujući šifriranje. Interni protokoli su uvedeni uzimajući u obzir potrebu da se sačuva povjerljivost žrtava i zaštite njihovi podaci. Slično tome, organizacija FIZ (Švicarska) naglasila je potrebu za zaštitom povjerljivosti podataka kao uvjeta za dobru saradnju s organima za provođenje zakona. Astra (Srbija) je istakla da je **povjerljivost žrtava** „ključan dio njihovog rada" i da odricanje od povjerljivosti „nije i ne smije biti uvjet za dobijanje podrške i pomoći". Organizacija KOK (Njemačka) istakla je da je „zaštita pojedinca jača od potrebe za prikupljanjem dokaza". Praksis (Grčka) tvrdi da, kada dijele informacije s organima za provođenje zakona u skladu s pravilima o zaštiti podataka (dijeljenje zasnovano na pristanku), njihova „primarna briga je uvijek neposredna i efikasna zaštita potencijalne žrtve".

Pitanja zaštite podataka i razmjene podataka mogu stvoriti **moralne dileme**. Kako je istakla organizacija La Strada International, dijeljenje podataka s organima za provođenje zakona i podnošenje pritužbi podržavaju istrage, koje zauzvrat kasnije potencijalno mogu spasiti i zaštititi više žrtava. Međutim, to može imati svoju cijenu za pojedinačnu žrtvu, koja bi mogla biti izložena rizicima i prijetnjama, uključujući socijalnu isključenost. Osim toga, mogu postojati problemi vezani za dugoročne efekte registracije žrtve i dijeljenja ličnih podataka, uključujući potencijalno krivično gonjenje i kažnjavanje od strane nadležnih organa (ovo se može pogoršati kada se žrtva nezakonito nalazi u državi u vrijeme registracije). I La Strada International i La Strada Moldova smatraju da pronalaženje prave ravnoteže između potrebe žrtava za povjerljivošću u pristupu uslugama i potrebe za prikupljanjem dokaza za pomoć u borbi protiv trgovine ljudima u širem smislu može biti „veoma izazovno".

Ovo je još akutnije kada je žrtva dijete: kako je primijetila La Strada Moldova, djeca se često

plaše da daju saglasnosti i podnesu zvaničnu pritužbu policiji, uključujući i zbog straha od reakcije svojih roditelja.

Prema navodima La Strada Internationala, pravila o zaštiti podataka „otežala su razmjenu podataka između nevladinih organizacija i drugih relevantnih aktera". Istovremeno, NVO su svjesne da bi „žrtvama trgovine ljudima ili rizičnim grupama moglo biti teško da znaju koji se podaci čuvaju i/ili da osiguraju da se podaci ispravljaju, blokiraju ili brišu i da koriste ovo pravo", uprkos postojanju protokola o zaštiti podataka.

Dalja pitanja proizlaze iz prikupljanja ličnih podataka na osnovu kojih se može izvršiti identifikacija putem **tehnika ekstrakcije podataka**. Sustainable Rescue Foundation (SRF) se osvrnuo na dva zasebna projekta koji se trenutno provode u Holandiji: RIVET (SRF) i Lovitura 10 Elenas (laboratorij Policije Holandije). Oba projekta se fokusiraju na trgovinu Rumunkama u Holandiji radi seksualne eksploatacije. SRF RIVET koristi ekstrakciju podataka usmjerenu na žrtvu na osnovu intervjua s 10 rumunskih seksualnih radnica i istražuje upotrebu tehnologije za otkrivanje, prikupljanje, čišćenje i analizu podataka radi izgradnje taksonomija modusa operandi. Lovitura 10 Elenas digitalno prati deset rumunskih seksualnih radnica kako bi se stekao uvid u način funkcioniranja kriminalnih mreža. Kako je istakao RSF, izazov je „osigurati [da] sve rumunske seksualne radnice koje učestvuju u oba projekta ostanu anonimne". Skloništa žele zaštititi anonimnost seksualnih radnika, a policija ne može dijeliti svoju operativnu bazu podataka. SFR je predložio korištenje protokola za poređenje podataka za multilateralno računanje (MPC) kao moguće rješenje. Ovaj pristup se sastoji od anonimiziranja podataka koji potiču iz različitih skupova podataka (npr. NVO i policije) na takav način da ih onda mogu dijeliti i čitati različiti sistemi kako bi provjerili, naprimjer, da li ima dupliranih imena.

Organizacija La Strada International je pozvala da se posveti više pažnje potencijalnim rizicima i šteti koju stvaraju prikupljanja podataka (u velikim razmjerama) i tehnološki alati, upozoravajući da je u ovom trenutku fokus samo „na pozitivnim aspektima i mogućnostima" takvih alata. Ista organizacija je također tvrdila da je „potrebna veća kontrola upotrebe podataka i njihovog sigurnog čuvanja, kao i da se osigura da se sva pravila zaštite podataka djelotvorno primjenjuju". Žrtve, rizične grupe i NVO trebaju imati „više mogućnosti […] da odbiju zahtjeve za pružanje podataka i da maksimalno smanje prikupljanje podataka".

NVO imaju tendenciju da imaju različite protokole na osnovu toga da li je žrtva dijete ili odrasla osoba (**starosno osjetljivi protokoli**).

6.3. Dodatni dokazi prikupljeni na osnovu analize okruženja

IKT mogu imati značajan utjecaj na **ljudska prava** pojedinaca, uključujući pravo na privatnost, slobodu izražavanja i zaštitu od diskriminacije. U literaturi su otvorena različita pitanja.

Na osnovu OSCE (2020), možemo navesti niz **etičkih pitanja** koja treba uzeti u obzir prilikom razvoja tehnologije za borbu protiv trgovine ljudima. To uključuje: (a) zaštitu privatnosti podataka; (b) protokole o saglasnosti koje potpisuju žrtve; (c) obuke za osobe koje rukuju osjetljivim podacima, posebno podacima o žrtvama; (d) sigurno čuvanje podataka; (e) sprečavanje upotrebe tehnologije za dobijanje osjetljivih podataka o ranjivim ljudima (opće prikupljanje podataka o ranjivim ili marginaliziranim populacijama, čime se stvara rizik od diskriminatornih praksi); i (f) korištenje tehnologije na način koji ne krši ljudska prava žrtava, kao ni ljudska prava šireg stanovništva. ICAT (2019) također naglašava pitanja vezana za

privatnost podataka, etiku, transparentnost, odgovornost i informirani pristanak. On naglašava potrebu da se osigura da se podaci sigurno čuvaju, da postoje protokoli o saglasnosti i da su podaci rodno i uzrasno osjetljivi. Osim toga, informacije koje objavljuju organi za provođenje zakona trebaju se procijeniti tako da žrtve i njihove porodice ne budu izložene riziku.

ICAT (2019) i drugi izvori su ukazali na osjetljivost u vezi s **dijeljenjem podataka**. Kada se podaci dijele između država i/ili relevantnih agencija, to treba uraditi u skladu s načelima privatnosti i povjerljivosti. Primjećuje se da bi potencijalni sukob mogao nastati između potrebe za povjerljivošću kada žrtve pristupaju uslugama i dobijaju podršku, s jedne strane, i potrebe za informacijama/dokazima za izgradnju jake istrage, s druge strane. Gerry i drugi (2016) naglasili su značaj ključnih pravnih principa – principa poštenog informiranja – u vezi s obradom ličnih podataka (ovo uključuje princip ograničenja svrhe). Predlaže se da takvi principi ostaju važni i u slučaju trgovine ljudima, a posebno u odnosu na žrtve.

Gerry i drugi (2016) su također upozorili na rizik koji donose široko rasprostranjeni **alati za praćenje** u borbi protiv trgovine ljudima. Iako takva tehnologija može ponuditi nove mogućnosti za intervenciju u situacijama trgovine ljudima, ona se također sastoji od **oblika nadzora koji potencijalno veoma zadire** u privatnost pojedinca. Kako navode, ova tehnologija „može otkriti mnoštvo informacija u vezi s njihovim privatnim životom, uključujući njihovu pripadnost određenoj vjeroispovijesti, razvoj ličnih odnosa i druženja s drugim pojedincima, kao i njihove svakodnevne navike", stavljajući tako ugrožene grupe u opasnost od diskriminacije i profiliranja. Opće praćenje čitavih rizičnih populacija, npr. grupe migranata, može imati ozbiljne posljedice po privatnost pojedinaca. Gerry i drugi (2016) naglašavaju potrebu da se razviju **mehanizmi za utvrđivanje da li se tehnologija praćenja koristi pretjerano ili zloupotrebljava**. Oni predlažu izbjegavanje sistema koji uključuju centralizirano čuvanje ličnih podataka žrtava ili potencijalnih žrtava. Općenito, alate za borbu protiv trgovine ljudima zasnovane na tehnologiji treba **razvijati i koristiti odgovorno i etički**. Takve zahtjeve treba uzeti u obzir u svim fazama, od razvoja do konačne upotrebe. Rješenja zasnovana na tehnologiji također treba procijeniti na osnovu njihovog nivoa zadiranja u privatnost ljudi. Neki naučnici, uključujući Milivojevića i druge (2020), upozorili su na potencijalne negativne posljedice široke upotrebe tehnika prepoznavanja lica za marginaliziranu populaciju, i općenitije za ono što definiraju kao „moralni imperativ zaštite i spašavanja". Iako priznaju potencijal tehnologije kao pomoćnog sredstva u borbi protiv trgovine ljudima, oni također naglašavaju značaj stavljanja **najboljih interesa žrtava** u centar svake akcije.

Nekoliko izvora, uključujući Milivojević i drugi (2020) i Gerry i drugi (2016), ističe značaj **da se žrtvama ne uskraćuje mogućnosti korištenja tehnologije**, jer pristup tehnologiji može biti njihov jedini način da komuniciraju s vanjskim svijetom i može poslužiti kao važan mehanizam suočavanja. Uklanjanje pristupa tehnologiji može obespraviti žrtve; promoviranje sigurnog pristupa tehnologiji treba umjesto toga imati prednost.

Na kraju, u literaturi se **rijetko uvažava rodno zasnovana osjetljivost**. Priznaje se da je vrsta eksploatacije rodno osjetljiva, pri čemu su žene češće eksploatirane za seksualne usluge, rad u kući i ličnu njegu, a muškarci češće u poljoprivredi, građevinarstvu i drugim zanimanjima koja zahtijevaju manuelni rad (npr. ulična prodaja, pranje automobila). Osim toga, čini se da je vrbovanje putem interneta više povezano sa ženskim žrtvama nego s muškim žrtvama; međutim dokazi također sugeriraju da bi druge ranjivosti mogle biti u igri u slučaju vrbovanja

putem interneta, naprimjer da je osoba u ustanovi za njegu (preliminarni dokazi iz Rumunije navedeni su u Di Nicola i drugi 2017).

Preporuke

Aktivnosti za poboljšanje otkrivanja slučajeva trgovine ljudima posredstvom tehnologije

1. Organi za provođenje zakona trebaju ulagati u razvoj kapaciteta u oblastima **nadgledanja interneta, cyber patrola, tajnih istraga na internetu (cyber infiltracija), upotrebe podataka iz otvorenih izvora (OSINT) od strane specijaliziranih službenika, analize društvenih mreža** i upotrebe **alata za automatsko pretraživanje** za analizu dokaza. Razvoj i upotreba takvih alata moraju biti u skladu s načelima vladavine prava. Države trebaju razmotriti prilagođavanje postojećeg zakonodavstva kako bi omogućile cyber patroliranje i tajne istrage na internetu (cyber infiltraciju) – uz pažljivo razmatranje etičkih implikacija. Nadležni organi također trebaju razmotriti ulaganje u alate za pomoć istražiteljima u rukovanju i obradi podataka u velikim razmjerama (mogućnost za obradu velikih količina podataka). Resursi bi se mogli udružiti na nadnacionalnom nivou za razvoj tehnoloških proizvoda, kao što su sistemi za skeniranje mreže, kao i za razmjenu stručnosti o njihovoj upotrebi.

2. Organi za provođenje zakona i inspekcije rada trebali bi provoditi **strože propise i češće kontrole na stranicama s oglasima za posao**. Ovo bi se moglo postići uz podršku

tehnoloških alata razvijenih u saradnji s privatnim kompanijama (npr. alati za validaciju oglasa za posao na internetu, alati za „struganje" stranica s oglasima za posao i upotreba markera trgovine ljudima). Inspekcije rada bi trebale **razviti digitalnu ekspertizu i povećati svoje prisustvo na internetu**.

3. Države/privatni pružaoci usluga/NVO moraju unaprijediti **mehanizme za povjerljivo prijavljivanje putem interneta** koji omogućavaju anonimno prijavljivanje slučajeva trgovine ljudima, kao i samoidentificiranje žrtava. Chat, uključujući chat-botove, i funkcije za razmjenu poruka mogu biti dragocjeni alati na internetu. Države bi trebale sarađivati s privatnim kompanijama koje nude online usluge kako bi **eliminirale mogućnosti za trgovce ljudima**, razvile **analitike sadržaja** za otkrivanje slučajeva trgovine ljudima i utvrdile lako dostupne mehanizme za klijente da prijave sumnjive aktivnosti/oglase. Tamo gdje je dozvoljeno nacionalnim zakonodavstvom, ovo bi se trebalo proširiti na kompanije koje nude usluge za odrasle na internetu. Kompanije trebaju sigurno čuvati online sadržaje i informacije (npr. IP adrese) povezane s prijavljenim aktivnostima/oglasima.

Aktivnosti za poboljšanje istraga o trgovini ljudima posredstvom tehnologije

4. Organi za provođenje zakona bi trebali razmotriti organiziranje obuka za službenike specijalizirane za IKT i trgovinu ljudima. Države bi također trebale razmotriti stvaranje **grupa za tehničku podršku** u kojima bi radili policijski službenici s policijskim ovlaštenjima ili ostali policijski službenici sa specijaliziranim sposobnostima u oblasti IKT-a, koje bi bile integrirane u jedinice za trgovinu ljudima. Osim toga, države trebaju preispitati strukturu interne **raspodjele digitalnih istražnih sposobnosti** kako bi predvidjele i izbjegle potencijalna **uska grla u istragama**. Kako će se zločini posredstvom IKT-a, uključujući trgovinu ljudima, vjerovatno stalno povećavati, nedostatak specijaliziranih službenika na lokalnom nivou i preveliko oslanjanje na pomoć (preopterećenih) centraliziranih jedinica za visokotehnološki kriminal će vjerovatno stvoriti uska grla.

5. Organi za provođenje zakona trebaju se pobrinuti da **svi službenici** posjeduju odgovarajući nivo stručnosti za prikupljanje i rukovanje **elektronskim dokazima**. Obuka o elektronskim dokazima treba biti sastavni dio nastavnih planova i programa obuke i neprekidno se ažurirati zbog brzog mijenjanja tehnološkog okruženja i ponašanja. Pošto je očuvanje elektronskih dokaza ključno za razvoj jakih istraga, **savjetnici i NVO na prvoj liniji odbrane** također trebaju biti upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem historije chata).

6. Države/međunarodne organizacije trebaju redovno vršiti **stratešku analizu** kako bi stekle uvid u novonastale trendove o modusu operandi počinilaca, kao i kako bi bile u toku s obrascima ponašanja korisnika tehnologije i tehnološkim okruženjem koje se brzo mijenja. Na osnovu ovih strateških dokaza, države tada mogu pokrenuti ciljane policijske operacije, uspostaviti sporazume o saradnji i osmisliti ciljane kampanje za podizanje svijesti. Znanje treba redovno širiti na nacionalnom i nadnacionalnom nivou.

7. Države trebaju povećati prekograničnu saradnju kroz **pojednostavljene procedure, razmjenu najboljih praksi i tehnologija** (npr. specijaliziranih softvera) i pojačano **širenje praktičnih informacija** o kontaktnim tačkama/namjenskim jedinicama koje služe kao „privilegirani kontakti" u slučaju trgovine ljudima, uključujući trgovinu ljudima posredstvom IKT-a. Treba poticati saradnju i podršku između država odredišta i država porijekla (npr. skupa tehnološka oprema može biti dostupna samo bogatijim državama odredišta).

Aktivnosti za poboljšanje krivičnog gonjenja u slučajevima trgovine ljudima posredstvom tehnologije

8. Tužiocima treba osigurati posebnu **obuku** o trgovini ljudima posredstvom tehnologije i rukovanju elektronskim dokazima, kao i izvođenju dokaza pred sudijom/porotom. Države trebaju poduzeti mjere kako bi osigurale da **tužioci budu upoznati s procedurama** za traženje elektronskih dokaza od privatnih kompanija, kao i za pribavljanje dokaza iz drugih država i saradnju s drugim državama kako u okviru pravnog okvira EU (preko zajedničkih istražnih timova i evropskih naloga za istragu) tako i van pravnog okvira EU.

Aktivnosti za unapređenje saradnje s privatnim kompanijama

9. Države bi trebale razvijati **procedure za razmjenu podataka** s kompanijama koje posjeduju relevantne podatke i razmotriti razvoj **protokola za saradnju** s privatnim kompanijama, uključujući kompanije za društvene mreže i ekonomiju honorarnih poslova, kao i platforme za iznajmljivanje kako bi se potaklo pravovremeno pružanje informacija. Takvi protokoli/procedure trebaju razjasniti zakonske uvjete pod kojima kompanije za IKT, ISP i pružaoci sadržaja funkcioniraju, odrediti kontaktne tačke unutar kompanija i razjasniti koje nacionalne agencije su odgovorne za konkretne akcije, npr. traženje dokaza ili uklanjanje sadržaja povezanih s trgovinom ljudima. Odbijanje da se podijele dokazi ili uklone sadržaji povezani s trgovinom ljudima treba biti blagovremeno, izričito i obrazloženo.

Aktivnosti za unapređenje međunarodne saradnje

10. Trebalo bi **uspostaviti lakši proces za zahtjeve za uzajamnu pravnu pomoći (UPP)**, a to se odnosi na jasnije procedure i povećanu upotrebu unaprijeđene mreže kontaktnih tačaka, uključujući kontaktne tačke u Evropskoj pravosudnoj mreži, te omogućiti da zahtjevi za uzajamnu pravnu pomoć budu jasno postavljeni i razmotreni na samom početku. Države trebaju osigurati da njihovo osoblje bude adekvatno obučeno za obradu zahtjeva za UPP, korištenje EIO i drugih međunarodnih alata. Države i međunarodne organizacije trebaju razviti **zajednički dogovorene i prihvaćene šablone** koji podržavaju procese saradnje u cilju olakšavanja komunikacije, smanjenja administrativnih opterećenja i smanjenja broja grešaka u zahtjevima. Države također trebaju razviti upotrebu **sigurnih oblika elektronske komunikacije** i promovirati njihovo usvajanje kako bi se olakšala međunarodna saradnja.

Aktivnosti za unapređenje obuka

11. Trebalo bi predvidjeti **zajedničke aktivnosti obuke (ZAO)** za države koje se sistematski bave zajedničkim slučajevima trgovine ljudima. Transnacionalna razmjena znanja može se podsticati kroz učešće u međunarodnim/regionalnim obukama koje su fokusirane na određene aspekte istraživanja trgovine ljudima posredstvom IKT-a. Takve obuke trebaju uključivati studije slučaja i scenarije o trgovini ljudima posredstvom IKT-a. Za tužioce i sudije također treba osigurati obuku o trgovini ljudima posredstvom IKT-a i o povezanim pravnim instrumentima.

12. NVO trebaju proći obuku o najnovijim dešavanjima u svijetu tehnologije i u oblasti trgovine ljudima, uključujući promjene u strategijama regrutiranja. NVO trebaju biti u poziciji da razmjenjuju iskustva o najboljim međunarodnim praksama.

Aktivnosti za unapređenje pravnih instrumenata

13. Nadležni organi bi trebali osmisliti **zajedničke procedure za brzu razmjenu digitalnih dokaza sa ISP** i **ponovo procijeniti trajanje obaveza čuvanja podataka** koje su nametnute ISP-u (trenutni periodi su previše kratki imajući u vidu trajanje policijskih istraga). Treba uložiti napore da se usvoji **zajednički okvir** u vezi s obavezama čuvanja podataka i razmjenom elektronskih dokaza.

14. Kako bi iskoristile puni potencijal koji nudi **Konvencija o visokotehnološkom kriminalu**, države trebaju (a) završiti usaglašavanje nacionalnog zakonodavstva s Konvencijom; (b) proširiti i unaprijediti obuke o mogućnostima koje nudi Konvencija pošto trenutno ne koriste sve države ugovornice u punom potencijalu sredstva koja su im dostupna; (c) provoditi aktivnosti za podizanje svijesti o širokom obimu procesnih ovlaštenja i alata za međunarodnu saradnju iz Konvencije, posebno u vezi s predmetima trgovine ljudima; i (d) brzo provoditi mjere iz Drugog dodatnog protokola.

15. Države trebaju pažljivo procijeniti pitanje gdje se njihova **kontaktna tačka** (prema Konvenciji o visokotehnološkom kriminalu) nalazi u okviru sistema krivičnog pravosuđa kako bi se izbjegla **uska grla**. Uz sve centralniju ulogu koju igraju IKT i elektronski dokazi, takve kontaktne tačke će biti pod sve većim pritiskom i brzo će biti preopterećene ako ne budu imale adekvatno osoblje. Države bi možda željele razmotriti popunjavanje takvih kontaktnih tačaka osobljem koje posjeduje stručnost u različitim oblastima borbe protiv kriminala, uključujući trgovinu ljudima posredstvom IKT-a.

16. Države van Evrope treba ohrabriti da **usvoje ključne međunarodne pravne instrumente**, kao što su Konvencija VE o visokotehnološkom kriminalu i Konvencija VE o uzajamnom pružanju pomoći u krivičnim stvarima, kako bi se ujednačila i poboljšala međunarodna saradnja.

17. Treba povećati **saradnju i sinergiju** između mehanizma za praćenje Konvencije o borbi protiv trgovine ljudima (GRETA i Komitet ugovornica) i T-CY-a, naprimjer u vidu razmjene mišljenja, kao i razvoja aktivnosti za izgradnju kapaciteta koje se fokusiraju na obje konvencije.

Aktivnosti za sprečavanje viktimizacije i ponovne viktimizacije

18. Privatne kompanije, u saradnji s nadležnim organima i nevladinim organizacijama, trebale bi povećati **društveno oglašavanje** na internetu kako bi spriječile viktimizaciju i poboljšale otkrivanje trgovine ljudima posredstvom tehnologije. Države trebaju povećati svoje napore da informiraju pojedince o njihovim radnim pravima na jeziku koji razumiju, u saradnji s nevladinim organizacijama i kompanijama koje pružaju usluge hostinga za oglase za posao. Utjecaj kampanja treba rutinski procjenjivati.

19. Države, NVO i privatne kompanije koje pružaju online i IKT usluge trebaju pokrenuti inicijative za **podizanje svijesti o rizicima vezanim za tehnologiju, uključujući to kako trgovci ljudima mogu iskoristiti tehnologiju** i kako mogu početi potencijalne situacije eksploatacije. Škole i prosvjetni radnici trebaju biti dio ovog napora jer su djeca i mladi odrasli izloženi povećanim rizicima. Države i NVO trebaju raditi s privatnim kompanijama koje nude usluge komunikacije i razmjene poruka kako bi u sistem ugradile informacije/upozorenja o **sigurnom korištenju privatnih kanala komunikacije**.

20. NVO trebaju ponuditi obuku o tehnikama zaštite podataka i sigurnijoj upotrebi tehnologije u okviru **programa zaštite i reintegracije žrtava**. Žrtvama ne treba uskratiti pristup

tehnologiji, što bi im moglo oduzeti moć.

Međusektorsko djelovanje

21. Države trebaju dodati tehnološku strategiju u svoje **nacionalne akcione planove** za borbu protiv trgovine ljudima.

Prilog 1 | Izgradnja baze dokaza o trgovini ljudima posredstvom interneta i IKT-a: Spisak izvora

Baza dokaza je izgrađena na osnovu širokog pozadinskog istraživanja koje pokriva različite izvore, uključujući sljedeće: (a) međunarodne organizacije; (b) akademske zajednice; (c) izabrane nacionalne izvjestioce; (d) NVO i humanitarne organizacije; (e) privatni sektor. Ukupno su 62 izvora identificirana kao relevantna za potrebe ovog rada. Iako razmatrani izvori obuhvataju period od 2003. do 2020. godine, većina je objavljena nakon 2015. godine, dok su 22 objavljena u posljednje tri godine. Svi razmatrani izvori su napisani na engleskom jeziku (s jednim izuzetkom: francuska verzija izvještaja koji je pripremila organizacija Myria, belgijski „Centre fédéral Migration").

Međunarodne i nacionalne organizacije

1. Council of Europe (2021). Protecting Women and Girls from Violence in the Digital Age.

2. Council of Europe (2019). Stepping up the Council of Europe action against trafficking in human beings in the digital age. Summary Report.

3. Council of Europe (2019). 9. opći izvještaj o aktivnostima GRETA.

4. Council of Europe (2016). Safeguarding Human Rights on the Net.

5. Council of Europe (2016). Study on Reduction Measure to Combat Trafficking in Human Beings for the Purpose of Labour Exploitation through Engagement of the Private Sector.

6. Council of Europe (2016). Emerging Good Practice by State Authorities, the Business Community and Civil Society in the Area of Reducing Demand for Human Trafficking for the Purpose of Labour Exploitation.

7. Council of Europe (2015). Comparative study of blocking, filtering and take-down of illegal Internet content.

8. Council of Europe (2007). Trafficking in human beings: Internet recruitment.

9. Council of Europe (2003). Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation.

10. ICAT (2019). Human Trafficking and Technology: Trends, Challenges and Opportunities. Inter-Agency Coordination Group Against Trafficking in Persons. Issue Brief 7.

11. OSCE (2020). Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools. OSCE and Tech Against Trafficking.

12. UN.GIFT (2008). Technology and Human Trafficking. The Vienna Forum to fight Human Trafficking: Background Paper.

13. UNODC (2019). Module 14: Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants. E4J Teaching Modules.

14. Myria (2017). En ligne_: Traite et trafic des êtres humains, Rapport annuel 2017.

15. Europol (2020). The challenges of countering human trafficking in the digital era.

16. Europol (2014). Trafficking in human beings and the Internet. Intelligence Notification.

Akademska zajednica

17. Ibanez M. and Gazan R. (2016). "Detecting Sex Trafficking Circuits in the U.S. Through Analysis of Online Escort Advertisements". IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM), 892–895.

18. Ibanez M. and Gazan R. (2016). "Virtual Indicators of Sex Trafficking to Identify Potential Victims in Online Advertisements", 818–824.

19. Ibanez M. and Suthers D. D. (2014). "Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources". 47th Hawaii International Conference on System Science, 1556–1565.

20. Volodko A., Cockbain E. and Kleinberg B. (2019). "'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers". Trends in Organized Crime, 27: 7–35.

21. Di Nicola A., Baratto G. and Martini E. (2017). Surf and Sound. The Role of the Internet in People Smuggling and Human Trafficking. eCrime Research Report 3.

22. Sykiotou A. P. (2017). Cyber trafficking: recruiting victims of human trafficking through the net. In "Essays in Honour of Nestor Courakis". A. N. Sakkoulas Publications.

23. Foot K.A., Toft A. and Cesare N. (2015). "Developments in Anti-Trafficking Efforts: 2008–2011". Journal of Human Trafficking, 1:2, 136-155.

24. Gerry F., Muraszkiewicz J. and Vavoula N. (2016). "The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns". Computer Law & Security Review, 32:2, 205-217.

25. Latonero M., Browyn W. and Dank M. (2015). Technology and Labor Trafficking in

a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study. California: University of Southern California, Annenberg Center on Communication Leadership & Policy.

26. Latonero M. (2011). The Role of Social Networking Sites and Online Classifieds. California: University of Southern California, Annenberg Center on Communication Leadership & Policy Research Series.

27. Latonero M. (2012). The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. University of Southern California, Annenberg Center on Communication Leadership & Policy.

28. Elliott J. and McCartan K. (2013). "The reality of trafficked people's access to technology". The Journal of Criminal Law, 77:3, pp. 255-273.

29. Hughes D. M. (2014). "Trafficking in human beings in the European Union: Gender, sexual exploitation, and digital communication technologies." Sage Open 4: 4.

30. Kunz R., Baughman M., Yarnell R. and Williamson C. (2018). Social Media and Sex Trafficking Process: From connection and recruitment, to sales. Ohio: University of Toledo.

31. Farley M., Franzblau K. and Kennedy M. A. (2013). Online prostitution and trafficking. Albany Law Review, 77:3, 101-157.

32. Barney D. (2018). Trafficking Technology: A look at different approaches to ending technology-facilitated human trafficking. Pepperdine Law Review, 45, 747-784.

33. Milivojevic S., Moore H. and Segrave M. (2020). Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology. Anti-trafficking review, (14), 16-32.

34. Raets S. and Janssens J. (2019). Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business. European Journal on Criminal Policy and Research, 1-24.

35. John G. (2018). Analyzing the Influence of Information and Communication Technology on the Scourge of Human Trafficking in Rwanda. Academic of Social Science Journal, 3:1, 1095-1102.

36. Maras M-H (2017). Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?, Journal of Internet Law, vol. 21, 17-21.

37. Stalans L. J. and Finn M. A. (2016). Understanding How the Internet Facilitates Crime and Deviance, Victims & Offenders, 11, 501-508.

38. Van Reisen M., Gerrima Z., Ghilazghy E., Kidane S., Rijken C. and Van Stam G. (2017). Tracing the emergence of ICT-enabled human trafficking for ransom. In Piotrowicz R., Rijken C., Baerbel, Uhl B. H. (eda), The Routledge Handbook on Human Trafficking. Routledge: London.

39. Raets S. and Janssens J. (2018). Trafficking & Technology: The role of digital communication technologies in the human trafficking business.

40. Dixon H. (2013). Human trafficking and the Internet (and other technologies, too). Judges' Journal, 52:1, 36-39.

41. Thakor M. and Boyd D. (2013). Networked trafficking: Reflections on technology and the anti-trafficking movement. Dialectical Anthropology, vol. 37, str. 277-290.

42. Michell K. J. and Boyd D. (2014). Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement. University of New Hampshire: Crime Against Children Research Centre.

43. Heil E. and Nichols A. (2014). Hot spot trafficking: A theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States. Contemporary Justice Review, 17(4), 421-433.

44. Andrews S., Brewster B., Day T. (2016) Organised Crime and Social Media: Detecting and Corroborating Weak Signals of Human Trafficking Online. U: Haemmerlé O., Stapleton G., Faron Zucker C. (eds) Graph-Based Representation and Reasoning. ICCS 2016. Lecture Notes in Computer Science, vol. 9717. Springer, Cham.

45. Mendel J. and Sharapov K. (2016). Human trafficking and online networks: Policy, analysis, and ignorance. Antipode, 48(3), 665-684.

46. TRACE (2017). Report on the role of current and emerging technologies in human trafficking. Deliverable 4.1, FP7/Security Research, koje finansira Evropska komisija.

47. Landman T., Trodd Z., Darnton H., Durgana D., Moote K., Jones P., Setter C., Bliss N., Powell S. and Cockayne J. (eds). Code 8.7: Conference Report 2019/02/19-20 New York. New York: United Nations University, 2019.

48. Kiss L., Fotheringhame D., Mak J., McAlpine A. and Zimmerman, C. (2020). The use of Bayesian networks for realist evaluation of complex interventions: evidence for prevention of human trafficking. Journal of Computational Social Science, 1-24.

49. Jackson B. and Lucas B. (2020). A COVID-19 Response to Modern Slavery using AI Research. 26 June, www.delta87.org.

50. Rende Taylor L. and Shih E. (2019). "Worker feedback technologies and combatting modern slavery in global supply chains: examining the effectiveness of remediation-

oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking", Journal of the British Academy, 7(s1), 131-165.

51. Musto J., Thakor M. and Gerasimov B. (2020), "Editorial: Between Hope and Hype: Critical evaluations of technology's role in anti-trafficking", Anti-Trafficking Review, 1-14, dostupno online na: https://doi.org/10.14197/atr.201220141.

52. Kougkoulos I., Cakir M. S., Kunz N., Boyd D. S., Trautrims A., Hatzinikolaou K. and Gold S. (2021). A multi-method approach to prioritize locations of labor exploitation for ground- based interventions. Production and Operations Management, online first.

NVO/humanitarne organizacije/privatni sektor

53. Fine Tune Project (2011). The Role of the Internet in Trafficking for Labour Exploitation. Final Report for the European Commission.

54. Thorn (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims.

55. Thorn (2018). Survivor Insights. The Role of Technology in Domestic Minor Sex Trafficking.

56. Chawki M. and Wahab M. (2005). Technology is a double-edged sword: Illegal human trafficking in the information age. Computer Crime Research Center.

57. Caliber (2008). Law Enforcement Response to Human Trafficking and the Implications for Victims: Current Practices and Lessons Learned. Final report prepared for U.S Department of Justice: National Institute of Justice.

58. Stop the Traffik (2019). Independent evaluation of Stop the Traffik's work and model.

Web-lokacije

59. Traffik Analysis Hub: https://traffikanalysis.org/ (IBM, Stop the Traffik i Clifford Chance).

60. The Counter Trafficking Data Collaborative: https://www.ctdatacollaborative.org/ (IOM, Polaris i Liberty Shared).

61. Alan Turing Institute, Data Science for Tackling Modern Slavery: https://www.turing.ac.uk/research/research-projects/data-science-tackling-modern- slavery

62. UN Delta 8.7. Alliance 8.7 Knowledge Problem: https://delta87.org/ (Globalna platforma za razmjenu znanja koja istražuje šta doprinosi eliminaciji prinudnog rada,

modernog ropstva, trgovine ljudima i dječijeg rada, Cilj 8.7 predviđen Ciljevima održivog razvoja UN-a).

Prilog 2. | Upitnik za državne aktere

Dio 1. Utjecaj IKT-a na trgovinu ljudima

1. Na osnovu dokaza do kojih se došlo u vašoj zemlji, možete li navesti primjere kako počinioci koriste IKT u kontekstu trgovine ljudima u svrhu seksualne eksploatacije? (Za svaki primjer navedite detalje o načinu rada trgovaca ljudima i o vrsti korištene tehnologije, npr. internet, određene web-lokacije, društveni mediji, aplikacije.)

2. Slično tome, možete li navesti primjere kako počinioci koriste IKT u kontekstu trgovine ljudima u svrhu radne eksploatacije? (Za svaki primjer navedite detalje o načinu rada trgovaca ljudima i o vrsti korištene tehnologije, npr. internet, određene web-lokacije, društveni mediji, aplikacije i privredni sektor u kojem se eksploatacija odvija.)

3. Koji su novi trendovi u vašoj državi u vezi s upotrebom IKT-a u trgovini ljudima (nove vrste tehnologije, novi modus operandi, nove vrste eksploatacije...)? Jeste li identificirali nove prakse na internetu koje mogu povećati rizik da neko postane žrtva trgovine ljudima (i u svrhu seksualne i u svrhu radne eksploatacije)?

4. Igra li mračna mreža bilo kakvu ulogu u trgovini ljudima u vašoj državi? Ako igra, možete li navesti neke detalje? (Pod mračnom mrežom se podrazumijevaju internetske stranice koje su dostupne samo preko anonimizirajućih pregledača kao što je Tor).

5. Da li se u vašoj državi IKT koristi za omogućavanje finansijskih tokova u kontekstu trgovine ljudima? Ako da, na koje načine? U kojoj mjeri se koriste kriptovalute ili kripto novčanici?

6. Općenito, na skali od 1 do 5, kako biste ocijenili utjecaj IKT-a na trgovinu ljudima u vašoj državi?

1	**2**	**3**	**4**	**5**
Veoma ograničen				Veoma značajan

Dio 2. Ključni izazovi s kojima se suočavaju države ugovornice prilikom otkrivanja i istraživanja trgovine ljudima posredstvom IKT-a te krivičnog gonjenja osoba umiješanih u trgovinu ljudima

Otkrivanje

7. Koje su strategije usvojene u vašoj državi za otkrivanje slučajeva trgovine ljudima na internetu?

8. Općenito govoreći, koji su izazovi u otkrivanju trgovine ljudima posredstvom IKT-a?

9. Možete li navesti neke primjere najboljih praksi u otkrivanju slučajeva trgovine ljudima posredstvom IKT-a?

10. Koju vrstu obuke pružate za istražitelje i druge aktere iz sistema krivičnog pravosuđa u pogledu identifikacije slučajeva trgovine ljudima posredstvom IKT-a? Koja dodatna obuka bi se mogla organizirati kako bi se povećala efikasnost strategija otkrivanja? Kako bi se mogla

ojačati online identifikacija žrtava?

Istrage

11. Kada je riječ o **istragama trgovine ljudima posredstvom IKT-a**, koliki problem predstavlja sljedeće:

	Obično nije problem	Mali problem	Veliki problem
Šifriranje podataka			
Nedostatak tehničkog znanja među organima za provođenje zakona			
Velika količina podataka dovodi do istraga za koje je potrebno mnogo vremena			
Brzina tehnoloških promjena (nove tehnologije se brzo pojavljuju itd.)			
Nedostatak tehničke opreme			
Nedostatak pomoći privatnog sektora			
Neodgovarajući zakonodavni instrumenti, uključujući instrumente za uzajamnu pravnu pomoć			

12. Za svaki problem koji smatrate „velikim" navedite nekoliko primjera i opišite korake, ako postoje, koji su već poduzeti kako biste ih prevladali/ublažili. Za svaki „veliki" problem, koja rješenja bi se mogla predvidjeti za njegovo prevladavanje?

13. Postoje li dodatni problemi koji nisu navedeni u tabeli? (Za svaki dodatni problem navedite detalje o problemu i rješenjima koja bi se mogla predvidjeti za njegovo prevladavanje.)

14. Koje su, po vašem mišljenju, najbolje strategije za vođenje djelotvornih istraga trgovine ljudima posredstvom IKT-a?

15. Koje obuke se trenutno organiziraju za organe za provođenje zakona u vezi s istragama trgovine ljudima posredstvom IKT-a? Koje dodatne potrebe za obukama za organe za provođenje zakona ste identificirali u vezi s trgovinom ljudima posredstvom IKT-a? Postoje li primjeri praksi pri provođenju obuka koje smatrate posebno uspješnim?

Krivično gonjenje

16. Kada je riječ o **krivičnom gonjenju osoba uključenih u trgovinu ljudima posredstvom IKT-a**, koliki problem predstavlja sljedeće:

	Obično nije problem	Mali problem	Veliki problem
Određivanje nadležnosti			
Ekstradicija osumnjičenih			
Pribavljanje dokaza iz drugih država			
Pomoć privatnog sektora			
Neodgovarajući zakonodavni instrumenti, uključujući instrumente za uzajamnu pravnu pomoć			
Nedovoljna obuka tužilaca			

17. Za svaki problem koji smatrate „velikim" navedite nekoliko primjera i opišite korake, ako postoje, koji su već poduzeti kako biste ih prevladali/ublažili. Za svaki „veliki" problem, koja rješenja bi se mogla predvidjeti za njegovo prevladavanje?

18. Postoje li dodatni problemi koji nisu navedeni u tabeli? (Za svaki dodatni problem navedite detalje o problemu i rješenjima koja bi se mogla predvidjeti za njegovo prevladavanje).

19. Koje obuke se trenutno organiziraju za tužioce i sudije u vezi s istragama trgovine ljudima posredstvom IKT-a? Koje dodatne potrebe za obukama za tužioce i sudije ste identificirali u vezi s trgovinom ljudima posredstvom IKT-a? Postoje li primjeri praksi pri provođenju obuka koje smatrate posebno uspješnim?

20. Postoje li u vašoj državi specijalizirane jedinice u okviru organa za provođenje zakona i pravosuđa čiji zadatak je vođenje predmeta trgovine ljudima s bitnom tehnološkom komponentom (npr. elektronski i online dokazi)? Ako je odgovor da, opišite njihove prakse.

Međunarodna saradnja

21. Koji izazovi se sreću tokom transnacionalnih istraga i pravosudne saradnje u kontekstu trgovine ljudima posredstvom IKT-a? Koje su najveće prepreke za djelotvornost, ako postoje, i kako se one prevladavaju?

22. Koji su primjeri dobrih praksi za unapređenje međunarodne saradnje?

Dio 3. Postojeći alati koji doprinose sprečavanju i borbi protiv trgovine ljudima posredstvom IKT-a

23. Možete li opisati najznačajnije nacionalne pravne instrumente koji se koriste u borbi protiv trgovine ljudima posredstvom IKT-a? Uspijeva li vaše zakonodavstvo pratiti korak s tehnološkim promjenama? Ako je odgovor da, kako se prilagođavate takvim promjenama? Ako je odgovor ne, kako se situacija može unaprijediti?

24. Možete li opisati najznačajnije međunarodne pravne instrumente koji se koriste u borbi

protiv trgovine ljudima posredstvom IKT-a? Smatrate li da su postojeći instrumenti adekvatni? Na koji način bi se mogli unaprijediti?

25. Postoje li određeni nedostaci u postojećem nacionalnom ili međunarodnom zakonodavstvu koji ometaju borbu protiv trgovine ljudima posredstvom IKT-a?

26. Imate li mehanizme usmjerene na sprečavanje upotrebe IKT-a u svrhu trgovine ljudima, uključujući na društvenim medijima i u vezi s oglasima za posao na internetu? Ako imate, opišite postojeće prakse i navedite koji državni organ je odgovoran za njihovo provođenje.

Dio 4. Korištenje tehnologije

27. Koji su tehnološki alati, ako postoje, trenutno dostupni u vašoj državi za identifikaciju žrtava trgovine ljudima? Koriste li se za identifikaciju žrtava vještačka inteligencija, tehnologija za prepoznavanje lica i/ili analiza velikih količina podataka? Imate li skup indikatora („znakova upozorenja") za identifikaciju žrtava?

28. Koje inicijative zasnovane na tehnologiji postoje u vašoj državi za pomoć žrtvama i širenje informacija među ugroženim zajednicama?

29. Koje inicijative zasnovane na tehnologiji postoje u vašoj državi za pomoć istragama i unapređenje krivičnog gonjenja?

Dio 5. Saradnja s privatnim kompanijama

30. Na koje načine kompanije za IKT, uključujući pružaoce usluga hostovanja interneta, društvenih medija i drugih online platformi, pomažu pri identifikaciji i uklanjanju internetskih sadržaja povezanih s trgovinom ljudima? Kako se vrši filtriranje? Jesu li aktuelni mehanizmi za filtriranje i uklanjanje djelotvorni? Ako nisu, kako bi se mogli poboljšati? Možete li navesti primjere dobrih praksi?

31. Postoje li zahtjevi u vašem pravnom okviru za filtriranje i uklanjanje internetskih sadržaja povezanih s trgovinom ljudima i koje sankcije su predviđene za nepoštovanje takvih zahtjeva? Postoji li kodeks ponašanja za pružaoce usluga/sadržaja? Je li pravni okvir djelotvoran? Ako nije, kako bi se mogao poboljšati?

32. Koje su prepreke s kojima se suočava vaša država pri radu s kompanijama za IKT i pružaocima internetskih usluga, uključujući pružaoce sadržaja i društvene medije, tokom borbe protiv trgovine ljudima? Kako se može razviti efikasno partnerstvo s kompanijama za IKT? Koji bi alati – pravni i operativni – mogli ojačati saradnju s kompanijama za IKT?

33. Na koje načine se kompanije za IKT bore protiv finansijskih transakcija povezanih s trgovinom ljudima? Kako bi se saradnja u ovom pogledu mogla ojačati?

34. Postoji li u vašoj državi nezavisno tijelo/regulator zadužen za praćenje internetskog sadržaja? Ako postoji, na kojoj osnovi se takve aktivnosti provode? Ako ne postoji, na koji način se vrši praćenje?

Dio 6. Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija)

35. Na koje načine, ako je to slučaj, vaša država koristi odredbe Konvencije VE o visokotehnološkom kriminalu (Budimpeštanske konvencije) za borbu protiv trgovine ljudima? Ako ne koristi, zašto je to tako?

36. Postoje li načini kako bi se Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija) i njeni dodatni protokoli mogli dodatno koristiti za borbu protiv trgovine ljudima?

Dio 7. Zaštita ljudskih prava

37. Koje mjere postoje za zaštitu ljudskih i građanskih prava pojedinaca, uključujući prava na zaštitu podataka i privatnosti, u kontekstu borbe protiv trgovine ljudima posredstvom IKT-a? Ako se koriste tehnološki alati, naprimjer detaljno pregledanje interneta, koji protokoli postoje kako bi se osiguralo da takvi alati štite osjetljive podatke, uključujući podatke o seksualnoj orijentaciji, vjeroispovijesti i političkim stavovima?

38. Imate li rodno osjetljive protokole povezane s upotrebom tehnologije u borbi protiv trgovine ljudima? Imate li starosno osjetljive protokole? Ako imate, možete li opisati ove protokole?

39. Kako se čuva povjerljivost podataka pri dijeljenju informacija s organima za provođenje zakona i trećim licima, uključujući privatne kompanije i humanitarne organizacije? Kako je uspostavljena ravnoteža između potrebe žrtava za povjerljivošću prilikom korištenja usluga i potrebe za prikupljanjem dokaza i informacija za borbu protiv trgovine ljudima?

Na kraju, postoji li još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT-a?

Dodatni materijali

Možete li navesti bilo koje relevantne materijale koji nisu povjerljive prirode, uključujući statističke podatke, saopćenja za medije, sažetke policijskih operacija, koji se odnose na trgovinu ljudima posredstvom IKT-a, uključujući sljedeće:

- upotreba IKT-a u trgovini ljudima;
- izazovi u otkrivanju trgovine ljudima posredstvom IKT-a, uključujući identifikaciju žrtava;
- izazovi koji se sreću tokom istraživanja slučajeva trgovine ljudima posredstvom IKT-a i krivičnog gonjenja osoba umiješanih u trgovinu ljudima;
- prekogranična saradnja u kontekstu trgovine ljudima posredstvom IKT-a;
- saradnja s kompanijama za IKT;
- alati za borbu protiv trgovine ljudima posredstvom IKT-a (pravni i/ili operativni alati);
- inicijative zasnovane na tehnologiji za borbu protiv trgovine ljudima;
- primjeri dobrih praksi.

Ako je vaš nacionalni izvjestilac istražio pitanje trgovine ljudima posredstvom IKT-a, podijelite s nama relevantne izvještaje/materijale.

Prilog 3. | Upitnik za NVO

Svrha ovog upitnika jeste da se shvati utjecaj tehnologije na trgovinu ljudima na osnovu dokaza prikupljenih tokom rada na terenu. Termin „tehnologija" ovdje podrazumijeva širok skup informacijskih i komunikacijskih tehnologija (IKT) koje korisnicima omogućavaju razmjenu digitalnih informacija. Primjeri tehnologija uključuju internet, online društvene medije i aplikacije za mobilne telefone.

Dio 1. Utjecaj tehnologije na trgovinu ljudima

1. Na osnovu dokaza do kojih se došlo u vašem radu, možete li navesti primjere kako počinioci koriste tehnologiju (IKT) u kontekstu trgovine ljudima u svrhu seksualne, radne ili druge vrste eksploatacije? (Za svaki primjer navedite detalje o vrsti eksploatacije i vrsti korištene tehnologije, npr. internet, određene web-lokacije, društveni mediji, aplikacije.)

2. Jeste li identificirali nove prakse na internetu koje mogu povećati rizik da neko postane žrtva trgovine ljudima?

3. Koji su izazovi u otkrivanju trgovine ljudima posredstvom tehnologije? Kako bi se mogla ojačati identifikacija žrtava?

4. Možete li navesti neke primjere dobrih praksi koje ste razvili za otkrivanje slučajeva trgovine ljudima posredstvom tehnologije i za identifikaciju žrtava?

5. Da li sarađujete s agencijama za provođenje zakona u borbi protiv trgovine ljudima posredstvom tehnologije? Koje su prepreke takvoj saradnji i kako bi se mogle prevladati?

6. Kakve obuke, ako postoje, organizirate za svoje osoblje i volontere u vezi s utjecajem tehnologije na trgovinu ljudima? Koja dodatna obuka bi bila korisna za povećanje efikasnosti strategija otkrivanja? Imate li tim u svojoj organizaciji koji je specijaliziran za trgovinu ljudima posredstvom tehnologije?

7. Postoje li određeni nedostaci u postojećem nacionalnom ili međunarodnom zakonodavstvu koji ometaju borbu protiv trgovine ljudima posredstvom tehnologije?

Dio 2. Korištenje tehnologije za borbu protiv trgovine ljudima

8. Koji su tehnološki alati, ako postoje, trenutno dostupni kao pomoćno sredstvo za identifikaciju žrtava trgovine ljudima (npr. određene aplikacije, analiza velikih količina podataka, skeniranje interneta)? Imate li skup indikatora („znakova upozorenja") za identifikaciju potencijalnih žrtava? Koju vrstu tehnoloških alata bi moglo biti korisno imati?

9. Koje su vam inicijative zasnovane na tehnologiji, ako postoje, na raspolaganju za pomoć žrtvama i širenje informacija među ugroženim zajednicama? Koje inicijative zasnovane na tehnologiji bi bilo korisno razviti?

10. Jeste li organizirali kampanje za podizanje svijesti usmjerene na korištenje tehnologije u trgovini ljudima? Ako jeste, možete li navesti neke od detalja o takvim kampanjama?

11. Imate li rodno osjetljive protokole povezane s upotrebom tehnologije u borbi protiv trgovine ljudima? Imate li starosno osjetljive protokole? Ako imate, možete li opisati ove

protokole?

12. Kako se čuva povjerljivost podataka pri dijeljenju informacija s organima za provođenje zakona? Kako je uspostavljena ravnoteža između potrebe žrtava za povjerljivošću prilikom korištenja usluga i potrebe za prikupljanjem dokaza za borbu protiv trgovine ljudima?

13. Na osnovu dokaza prikupljenih u vašem radu, kako biste ocijenili utjecaj tehnologije na trgovinu ljudima na skali od 1 do 5?

1	**2**	**3**	**4**	**5**
Veoma ograničen				Veoma značajan

Na kraju, postoji li još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT-a?

Dodatni materijali

Ako je to moguće, možete li podijeliti s nama bilo koje relevantne materijale koje ste izradili, uključujući statističke podatke, saopćenja za medije i izvještaje, a koji se odnose na trgovinu ljudima posredstvom tehnologije?

Prilog 4. | Upitnik za tehnološke kompanije

Svrha ovog upitnika jeste da se shvati utjecaj tehnologije na trgovinu ljudima na osnovu dokaza prikupljenih tokom rada na terenu. Termin „tehnologija" ovdje podrazumijeva širok skup informacijskih i komunikacijskih tehnologija (IKT) koje korisnicima omogućavaju razmjenu digitalnih informacija. Primjeri tehnologija uključuju internet, online društvene medije i aplikacije za mobilne telefone.

Dio 1. Utjecaj IKT-a na trgovinu ljudima

1. Na osnovu dokaza kojima raspolaže vaša kompanija/sektor, možete li opisati načine na koje počinioci zloupotrebljavaju IKT u kontekstu trgovine ljudima (u svrhu seksualne, radne ili druge vrste eksploatacije)?

2. Jeste li identificirali nove prakse na internetu koje mogu povećati rizik da neko postane žrtva trgovine ljudima?

3. Koji mehanizmi su razvijeni u vašoj kompaniji, ili generalno u vašem sektoru, za sprečavanje zloupotrebe IKT-a u svrhu trgovine ljudima?

Dio 2. Saradnja s agencijama za provođenje zakona i civilnim društvom

4. Na koje načine, ako je to slučaj, vaša kompanija sarađuje s agencijama za provođenje zakona kako bi se omogućile identifikacija žrtava i istrage u predmetima trgovine ljudima posredstvom IKT-a?

5. Koje su najvažnije prepreke koje se sreću tokom saradnje s agencijama za provođenje zakona u kontekstu trgovine ljudima posredstvom IKT-a?

6. Postoje li primjeri dobrih praksi za unapređenje saradnje s agencijama za provođenje zakona?

7. Koje pravne zahtjeve vaša kompanija mora poštovati u kontekstu borbe protiv trgovine ljudima?

8. Koji bi alati – pravni i operativni – mogli ojačati saradnju s agencijama za provođenje zakona?

9. Na koje načine, ako je to slučaj, vaša kompanija sarađuje s civilnim društvom kako bi se omogućile identifikacija žrtava i pomoć žrtvama trgovine ljudima?

Dio 3. Korištenje tehnologije

10. Koji su tehnološki alati, ako postoje, trenutno dostupni vašoj kompaniji za identifikaciju žrtava trgovine ljudima? Koriste li se za identifikaciju žrtava vještačka inteligencija, tehnologija za prepoznavanje lica i/ili analiza velikih količina podataka? Imate li skup indikatora („znakova upozorenja")?

11. Koje inicijative zasnovane na tehnologiji postoje u vašem sektoru za pomoć istragama i unapređenje krivičnog gonjenja?

12. Koje mjere postoje za zaštitu ljudskih i građanskih prava pojedinaca, uključujući prava na zaštitu podataka i privatnosti, u kontekstu borbe protiv trgovine ljudima posredstvom IKT-a? Ako se koriste tehnološki alati, naprimjer detaljno pregledanje interneta, koji protokoli postoje kako bi se osiguralo da takvi alati štite osjetljive podatke, uključujući podatke o seksualnoj orijentaciji, vjeroispovijesti i političkim stavovima? Imate li starosno osjetljive protokole?

13. Kakve obuke, ako postoje, organizirate za svoje osoblje u vezi s utjecajem tehnologije na trgovinu ljudima? Koja dodatna obuka bi mogla povećati efikasnost strategija za borbu protiv trgovine ljudima?

Na kraju, postoji li još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT-a?

Dodatni materijali

Ako je to moguće, podijelite s nama bilo koje relevantne materijale koji nisu povjerljive prirode, uključujući statističke podatke, saopćenja za medije i izvještaje, a koji se odnose na trgovinu ljudima posredstvom tehnologije.

www.coe.int

Vijeće Evrope je vodeća organizacija za ljudska prava u Evropi. Sastoji se od 46 država članica, uključujući sve članice Evropske unije. Sve države članice Vijeća Evrope potpisale su Evropsku konvenciju o ljudskim pravima, sporazum osmišljen da zaštiti ljudska prava, demokratiju i vladavinu prava. Evropski sud za ljudska prava nadgleda primjenu Konvencije u državama članicama.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE