Онлајн трговија со луѓе преку користење на технологија

Целосен извештај

ГРЕТА
Група на експерти за акција против трговија со луѓе

Превод кофинансиран од Европската Унија

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Онлајн трговија со луѓе преку користење на технологија

Целосен извештај

Извештајот е подготвен од
Д-р Паоло Кампања
Вонреден професор на Универзитетот во Кембриџ
Обединето Кралство

април 2022 година

Совет на Европа

Верзија на англиски јазик

Online and technology-facilitated trafficking in human beings

Овој превод е направен со финансиска поддршка на Европската Унија и на Советот на Европа. Наведената содржина е единствена одговорност на Советот на Европа и не значи дека секогаш ги одразува ставовите на Европската унија.

Француско издание:
La traite des êtres humains en ligne et facilitée par les technologies

Целата друга кореспонденција во врска со овој документ треба да биде упатена до Секретаријатот на Конвенцијата на Советот на Европа за акција против трговијата со луѓе trafficking@coe.int

Сите фотографии: Shutterstock

Оваа публикација не е лекторирана од уредувачката единица на СПДП со намера да се поправат печатните и граматичките грешки.

Отпечатено во Советот на Европа

Содржина

Кратенки употребени во текстот

ВИ: Вештачка интелигенција
ASW: Веб-страница со содржини за возрасни
CE: Совет на Европа
CID: Оддел за истражување на кривични дела
CSE: Детска сексуална експлоатација
CV: Работна биографија
EAW: Европски налог за апсење
EIO: Европски налог за истрага
EJN: Европска судска мрежа
ЕУ: Европска унија
БДП: Бруто домашен производ
GDPR: Генерална регулатива за заштита на податоци
ГРЕТА: Група на експерти на Советот на Европа за акција против трговијата со луѓе
HDD: Хард диск драјв
ЗИТ: Заеднички истражен тим
ИКТ: Информациско-комуникациска технологија
ISP: Давател на интернет услуги
МПП: Меѓусебна правна помош
НВО: Невладина организација
OSINT: Разузнавачки информации од отворени извори достапни на јавноста
ТЛ: Трговија со луѓе
TOR: The Onion Router
VOIP: Протокол за пренос на гласовни комуникации преку Интернет

Вовед

Интернетот и информациско-комуникациската технологија (ИКТ) воопшто, играат голема улога во осмислувањето на нашиот живот. Пандемијата со „Ковид-19" го откри степенот до кој интернетот и ИКТ сега се составен дел од различните активности и социјални интеракции и воедно ја забрзано ја истакна нивната релевантност. Состојбата со кривичните дела не е исклучок, а таа се однесува и на трговијата со луѓе (ТЛ).

Не постои сомнеж дека технологијата со себе носи предизвици – но, и можности – и за органите на прогонот и за невладините организации. Во исто време, базата на докази за онлајн ТЛ преку користење на технологија останува ограничена и непроменета. Во моментов, најдобрите докази кои ни се достапни се производ на прилично мал број на студии, кои обично се засновани на мал број интервјуа со полициски службеници и вработени во НВО - често спроведени во исклучително ограничен број земји - како и на неколку извештаи од меѓународните организации. Оваа студија оди подалеку од случајни докази, нудејќи анализа на онлајн ТЛ преку користење на технологија врз основа на систематски собрани докази од државите потписнички на Конвенцијата на Советот на Европа (СЕ) за акција против трговијата со луѓе.

Опфатот на оваа студија е прилично широк. Тој нуди проценка на степенот до кој технологијата влијае на ТЛ, како и истражување за начинот на делување на трговците со луѓе во контекст на онлајн ТЛ преку користење на технологија. Во фокусот на оваа студија е истражувањето на оперативните и правните предизвици со кои се соочуваат земјите-членки - и до одреден степен невладините организации - во откривањето, истрагата и гонењето на онлајн ТЛ преку користење на ИКТ, како и во идентификувањето на жртвите и подигањето на свеста кај ризичните групи. Од суштинско значење е тоа што студијата, исто така, ги истражува стратегиите, алатките и „добрите практики" усвоени од земјите-членки и НВО за надминување на ваквите предизвици и подобрување на нивниот одговор на онлајн ТЛ преку користење на технологија. Овој труд ги открива сличностите меѓу земјите, како и искуствата кои конкретно се однесуваат на одредена земјата. Конкретен фокус се става на обуката – земајќи предвид дека инвестициите во човечкиот капитал се еднакво важни како и инвестициите во технолошките алатки.

Студија е спроведена како дел од долгогодишниот интерес на Советот на Европа во врска со прашањето на технологијата и трговијата со луѓе. Покрај тоа што нуди *систематска проценка на тековната база на докази*, оваа студија, исто така, се стреми да им обезбеди алатка за спроведување идни проценки и следење на промените во технолошките и бихејвиоралните состојби на Групата експерти за акција против трговијата со луѓе на Советот на Европа (ГРЕТА) и на други заинтересирани страни.

Методологија

Доказите од оваа студија беа собрани преку иновативен прашалник кој вклучуваше отворени и затворени прашања. Прашалникот беше изработен во три верзии (претставени во Анексите): подолга верзија за земјите-членки (40 прашања) и две пократки верзии за НВО (14 прашања) и технолошките компании (11 прашања). Дизајнот на прашалникот е изработен со користење на информации добиени преку анализа на состојбата спроведена од октомври до декември 2020 година која опфаќа различни извори: меѓународни организации, академска заедница, НВО, како и приватен сектор (види Анекс А за деталите). Прашалникот е направен во консултација со членките на ГРЕТА и Секретаријатот на Советот на Европа во периодот јануари - март 2021 година. Одговори беа добиени од 40 земји-членки[1], 12 невладини организации[2] и 2 технолошки компании[3] од јуни до јули 2021 година (еден задоцнет одговор стигна до Секретаријатот на Советот на Европа во септември 2021 година). Потоа беа извршени анализи од јуни до септември 2021 година. Станува збор за прилично збиена временска рамка за студија со значително голем опфат на прашања, земји и ентитети. И покрај тоа што оваа студија нуди детална проценка на голема база на докази, таа во никој случај не претставува исцрпна студија која нема ограничувања. Во текстот, секогаш кога е релевантно тоа прашање се разгледува.

Оваа студија го следи Латонеро (2012: 9-10) во дефинирањето на технологијата како „информациско-комуникациски технологии, конкретно оние кои се состојат од дигитални и мрежни опкружувања. Технологиите кои им овозможуваат на корисниците да разменуваат дигитални информации преку мрежи ги вклучуваат Интернетот, онлајн социјалните мрежи и мобилните телефони".

Технологијата нема да исчезне - а со неа, се создаваат структурни промени во начинот на кој дејствуваат сторителите, на кој се отвораат нови можности и како постојните ранливости стануваат уште позагрозени. Според тоа, постои потреба земјите-членки да се приспособат и да ги снабдат органите на прогонот и системот на кривичната правда со способности кои се во чекор со ова опкружување кое (постојано) се менува. Со оваа цел, студијата нуди неколку препораки засновани врз докази.

[1] Албанија; Ерменија; Австрија; Азербејџан; Босна и Херцеговина; Белорусија; Белгија; Бугарија; Хрватска; Кипар; Данска; Естонија; Финска; Франција; Германија; Грција; Унгарија; Исланд; Ирска; Латвија; Литванија; Луксембург; Малта; Република Молдавија; Монако; Црна Гора; Холандија; Северна Македонија; Норвешка; Полска; Португалија; Романија; Сан Марино; Словачка; Словенија; Шпанија; Шведска; Швајцарија; Украина и Обединетото Кралство.

[2] Астра (Србија); Различни и еднакви (Албанија); ФИЗ (Швајцарија); Надеж сега (Данска); Језуитска служба за бегалци (Северна Македонија); КОК (Германија); Ла Страда (Република Молдавија); Ла Страда Интернешнл (ширум Европа); Центар за права на мигрантите (Ирска); Праксис (Грција); Швајцарска платформа за борба против трговијата со луѓе (Швајцарија); Фондација за одржливо спасување (Холандија).

[Astra (Serbia); Different and Equal (Albania); FIZ (Switzerland); Hope Now (Denmark); Jesuit Refugee Service (North Macedonia); KOK (Germany); La Strada (Republic of Moldova); La Strada International (Europe-wide); Migrant Rights Centre (Ireland); Praksis (Greece); Schweizer Plattform gegen Menschenhandel (Switzerland); Sustainable Rescue Foundation (The Netherlands).]

[3] Facebook и IBM.

Резиме на извештајот

Влијанието на технологијата врз трговијата со луѓе

Влијанието на технологијата врз трговијата со луѓе е од особена важност во текот на две фази од процесот на трговија со луѓе: **регрутирањето** (врбувањето) и **експлоатацијата**. Доказите доставени од земјите-членки укажуваат на „зголемена" релевантност на технологијата во контекст на ТЛ, при што мнозинството земји-членки сметаат дека влијанието на технологијата врз ТЛ е „многу важно" или „важно".

Земјите-членки забележаа зголемена релевантност на онлајн материјалите, рекламите и сајтовите/апликациите во потрагата по работни места, како и зголемена релевантност на онлајн социјализација и личните интеракции. За возврат, и едното и другото создаваат можности за сторителите кога станува збор за ТЛ и ги злоупотребуваат постојните пропусти. Технологијата го промени начинот на кој луѓето комуницираат, а тоа се рефлектира и во криминалното опкружување, вклучувајќи ја и ТЛ. Ова е структурна промена на која треба да се прилагодат органите на прогонот и казнените системи.

Технологијата може да игра улога во фазата на **регрутирање** преку олеснување на идентификацијата, локацијата и контактот со потенцијалните жртви. Различни механизми се во игра во зависност од видот на експлоатација.

Во контекст на регрутирање за **сексуална експлоатација**, неколку земји-членки идентификуваа случаи на огласи за работа со цел ТЛ и откриј докази за врбување преку платформи на социјалните медиуми, како и апликации за запознавање. Вообичаена стратегија е таканаречената **техника „љубовник"**: вид на онлајн врбување во кое трговецот со луѓе ги идентификува и контактира потенцијалните жртви преку онлајн платформа, се запознава со нивните хобија и интереси, како и со нивната лична и семејна ситуација. Трговецот со луѓе потоа нуди емпатија и поддршка на потенцијалната жртва во контекст на романтична врска – со намера да стекне доверба и последователно да воспостави контрола над жртвата.

Постојат многу докази од неколку земји за случаи на **уценување** на жртвите. Ова често се прави така што прво се собираат „компромитирачки" информации за жртвите - на пример, преку барање на голи слики или видеа - а потоа таквите информации се користат за тие да се принудат на проституција.

За време на **фазата на експлоатација**, технологијата може да ја олесни **продажбата** на сексуални услуги од страна на жртвите на ТЛ. Постојат многу докази од неколку земји за интернет-страници кои се користат за рекламирање сексуални услуги. Помеѓу ваквите реклами, има услуги што ги даваат жртви на ТЛ. Покрај тоа, иако преносот во живо [live-streaming] честопати е поврзан со сексуална злоупотреба на деца, неколку земји сугерираат дека таквиот пренос во живо може да вклучува и возрасни жртви на ТЛ.

Понатаму, технологијата може да се користи за **координирање на активностите**. Од суштинско значење е што технологијата овозможува **раздвојување** помеѓу местото каде што се врши сексуалната активност и местото каде што се одвива координацијата. Ова има важни импликации за кривичниот прогон.

Земјите обезбедија докази за технолошки алатки што ги користат трговците со луѓе за да ги **следат и контролираат** жртвите во фазата на експлоатација. Уцената и употребата на компромитирачки информации против жртвите, исто така, може да се користат за да се изврши контрола во оваа фаза.
Новите трендови во контекст на сексуалната експлоатација забележани од различни земји вклучуваат зголемена употреба на „веб камерите во живо" [live web cams] и апликациите за видео разговор „со припејд претплата" [pay-as-you-go apps] и зголемена употреба на апликациите за контрола на жртвите. Ваквите веб-камери и апликации за видео разговор може да се користат за пренос во живо на сексуални дејствија извршени од жртви на ТЛ. Неколку земји забележаа дека пандемијата со „Ковид-19" ги зголеми можностите за трговците со луѓе да воспостават онлајн контакти со ранливи поединци.

Во контекст на трговијата со луѓе за **трудова експлоатација**, доказите обезбедени од земјите-членки укажуваат дека ИКТ главно се користат за **регрутирање** жртви, особено преку **онлајн огласи за работа**. Ваквите огласи не се објавуваат само на доверливи веб-страници за работа, туку се објавуваат и циркулираат на социјалните мрежи во специјализирани групи за барање работа и групи за взаемна помош. Неколку земји ја истакнаа релевантноста на веб-страниците наменети за поттикнување размена на информации меѓу работниците мигранти како простор за врбување што е целта на трговците со луѓе.

Трендот што се појавува во контекст на трудовата експлоатација, пријавен од некои земји, вклучува пораст на случаите на регрутирање (врбување) преку Интернет и социјалните мрежи. Се верува дека ова е забрзано со избувнувањето на Ковид-19. Иако се чини дека технологијата не игра забележлива улога во фазата на експлоатација, земјите го истакнаа зголемувањето на можностите за искористување на жртвите на трговија со луѓе што ги нуди „економијата на тезги" [gig economy], особено платформите за обезбедување на услуги.

Нема докази за каква било релевантна улога на **темната мрежа [Dark Web]** во контекст на ТЛ со возрасни жртви (циркулирањето на материјали за сексуална експлоатација на деца е надвор од опсегот на оваа студија). Слично на тоа, се чини дека **криптовалутите** не се широко користени во контекст на ТЛ (напротив, тие се користат за купување на пренос во живо од сексуална злоупотреба на деца).

Слична слика даваат и доказите доставени од **НВО**. Тие забележаа употреба на интернетот и социјалните медиуми во сите фази на трговија со луѓе, а особено во врска со (а) регрутирањето; (б) експлоатацијата; и (в) вршењето контрола и притисок врз жртвите. Покрај тоа, трговците со луѓе можат да користат ИКТ, вклучително и социјални медиуми и шифрирани апликации, за да продолжат да контактираат со жртвите на ТЛ откако ќе ја напуштат ситуацијата на експлотацаија, честопати за да ги спречат да поднесуваат жалби и да бараат правда.

Новите трендови засновани на докази од НВО укажуваат на зголемување на експлоатацијата на децата преку **веб-камери и социјални медиуми**. Постојат претпоставки дека сторителите почнале да користат **онлајн игри** за да им пристапат на потенцијалните жртви.

На крај, достапната база на докази сугерира дека употребата на технологија ги надополнува, но не ги заменува личните, офлајн интеракции. Најдобро е доколку на технологијата и интеракциите во живо се гледа како на интегрирани активности.

Предизвици во откривањето, истражувањето и гонењето на ТЛ преку користење на технологијата

Предизвици за откривањето

Откривањето на случаи на онлајн трговија со луѓе преку користење на технологија останува голем предизвик. Земјите-членки истакнаа голем број предизвици:

- Континуирано растечкиот обем на онлајн активности/интеракции. Следењето на содржините на интернет бара премногу ресурси и подлежи на законски ограничувања (вклучувајќи ги законите за приватност и ограничувања за користење на веб-роботи во некои земји);
- Обемот на онлајн огласи (отворени и доверливи) и за сексуални и за несексуални услуги честопати е премногу голем за рачно да се пребарува;
- Потешкотии во идентификувањето и на сторителите и на жртвите бидејќи тие можат да користат прекари и псевдоними кога работат онлајн и може да користат софтвер за анонимизирање (на пр., VPN);
- Користење на шифрирана комуникација помеѓу трговците со луѓе и жртвите. Разговорите меѓу трговците со луѓе и жртвите се одвиваат во затворени групи;
- Однесување на интернет корисниците кое се карактеризира со брзи промени;
- Предизвиците во сортирањето на онлајн рекламите за да се идентификуваат оние поврзани со ТЛ и во контекст на сексуални и во контекст на несексуални услуги. Предупредувањата, односно црвените знаменца, во врска со рекламите поврзани и со сексуалната и со трудовата експлоатација сè уште се недоволно развиени или не се користат постојано;
- Непостоење на специјализирани единици во рамките на полицијата и/или недостаток на специјализирани истражители за ТЛ со напредни компјутерски вештини. Недостаток на службеници обучени да вршат тајни операции на интернет. Компјутерски-операциите може да бидат долги и да одземаат многу време;
- Процес кој одзема време како резултат на испраќањето на барања до компаниите сопственици на социјалните медиуми и недобивањето на одговор од страна на некои од нив;

- Кратки периоди на задржување податоци за IP адреси и потешкотии во обезбедувањето на пристап до нив.

Предизвици за истрагите

Шифрирањето на податоците се смета за најтешкиот предизвик со кој се соочуваат земјите-членки (оценка за сериозност од 80 од 100). По што следуваат големиот обем на податоци (71), брзината на технолошките промени (66), недостатокот на техничка опрема (63), несоодветните законодавни алатки (61), непостоењето на техничко знаење кај органите на прогонот (53) и отсуството на помош од приватниот сектор (46).

Протоколите за шифрирање на податоци вклучени во популарните апликации и онлајн услугите нашироко се сметаат за проблематични. Шифрирањето, исто така, ја ограничува можноста за следење на комуникациите. Неколку земји навестија дека постојат алатки за дешифрирање на некои видови уреди. Сепак, ова е опкружување кое постојано се развива и бара (големи) инвестиции и во обуката и во софтверот. Преземените чекори за надминување на ова прашање вклучуваат формирање на единици/центри за компјутерски криминал кои имаат задача да работат на технологијата за дешифрирање. Понатаму, треба да се размисли за здружување на ресурсите на наднационално ниво во развојот на технолошки производи, како што се софтверот за дешифрирање и веб-роботите (web-crawlers).

Електронските комуникации и ИКТ уредите генерираат **голем обем на податоци кој постојано расте** што, пак, претставува значителен товар за истражувачите. Овој товар влијае на способноста на истражувачите да ги извлечат и внимателно да ги испитаат податоците, што само по себе бара специјализирани софтвери, како и посебна обука за тоа како да се систематизираат и пребаруваат таквите обемни докази.

Постои широк консензус дека градењето на капацитет за ракување со масивни количини на **електронски докази** е од клучно значење. Сепак, таквиот капацитет треба постојано да се ажурира. Земјите забележаа дека предизвиците не произлегуваат само од зголемениот број на податоци генерирани од онлајн платформите и социјалните медиуми, туку и од променливите **модели на однесување** на нивните корисници.

Непостоењето на техничка опрема е означен како предизвик од неколку земји. Цената на специјализираниот софтвер и хардвер е висока и често бара постојани ажурирања и скапи договори за лиценцирање со цел да биде во чекор со брзината на технолошките промени. **Потребата да се биде во тек со технолошките промени** може да има значително влијание врз полициските буџети. Ова е предизвик што го истакнаа неколку земји без разлика на нивото на БДП (бруто домашниот производ).

Инвестициите во човечкиот капитал се исто толку важни како и оние во софтверот и хардверот, ако не и повеќе, особено затоа што се однесуваат на **недостатокот и потребата од развивање на техничко знаење меѓу органите на прогонот**. Доказите укажаа на потребата од развивање на знаење за (а) појавата на нови трендови и промени во употребата на технологијата; (б) појавата на нови апликации и услуги на технолошкиот пазар кој се карактеризира со брзи промени и (в) развојот на нови безбедносни протоколи и методи за шифрирање. Од суштинско значење е тоа што знаењето треба паметно да се дистрибуира во една организација. На пример, недостатокот од специјалисти на локално ниво може да создаде **кочници во истрагите**, доколку треба постојано да се бара помош од (зафатена) централизирана единица.

Неколку земји ја истакнаа потребата од **обезбедување дополнителна техничка обука за сите полициски службеници**, вклучително и познавање на технологијата и како таа функционира. Слично на тоа, треба да се обезбеди соодветна обука за откривање и ракување со **електронски докази** на што е можно поголем број на службеници и тоа треба да биде редовна тема во наставните програми за обука на полициските службеници. Во посложените случаи, можеби ќе треба да се формираат тимови со мултидисциплинарни групи на вештини (на пр., со здружување на истражители, финансиски специјалисти и специјалисти за компјутерски криминал).

Понатамошните предизвици вклучуваат прашања кои произлегуваат од несоодветните **обврски за задржување податоци** наметнати на давателите на интернет услуги (ISP) и примената на законите за приватност, на пример во врска со веб-роботите (web-crawlers).

Предизвици за кривичното гонење

Севкупно, предизвиците на кривичното гонење имаат пониски оценки од оние кои се однесуваат на истрагите, при што само „добивањето докази од други земји" има нешто повисока оценка од 50 (од 100). По што следува недостатокот на обука меѓу обвинителите (40); несоодветните законодавни алатки (38) и помошта од приватниот сектор (33). Екстрадицијата на осомничените (28) и определувањето на надлежност (16) се чини дека играат маргинална улога.

Соодветната **обука на обвинителите** се смета за клучна во гарантирањето на сеопфатноста на случаите преку користење на ИКТ, правилното собирање и искористување на електронските докази и соодветното презентирање на случаите пред судијата/поротата. Некои земји-членки забележаа случаи во кои обвинителите не беа запознаени со процедурите за барање електронски податоци од приватни компании или со оние за добивање докази од и воспоставување на соработка со други земји (на пр. преку заеднички истражен тим, ЗИТ или Европски истражен налог, ЕИО).

Некои земји-членки го покренаа прашањето за обработка на електронски материјали, особено во контекст на **обврските кои произлегуваат од GDPR** (Генерална регулатива за заштита на податоците на ЕУ). Загриженоста беше искажана и околу меѓународните регулативи за заштита на податоците што може да го попречат собирањето, складирањето и обработката на информациите добиени преку технолошките истражни техники (како што е веб-роботот/web-crawlers).

Забележани се предизвици околу IP адресите и електронските докази. IP адресите треба да се поврзат со корисничките имињата/псевдонимите и корисниците онаму каде што е возможно. Сепак, корисничките имињата може да се менуваат во секое време и честопати наизменично се користат од осомничените.

Дополнителниот предизвик се однесува на **изведување на докази** пред поротата (и судијата), бидејќи техничките докази во случаите преку користење на ИКТ може да бидат сложени и честопати треба да бидат објаснети од експерт. Развивањето на експертиза во институцијата меѓу службениците за тоа како ефективно и точно да се изведат електронски докази може да биде сè повредна.

Предизвици за меѓународната соработка

Долгото времетраење за добивање на повратни информации по обработката на **барањата за меѓусебна правна помош** (МПП) беше посочено од огромното мнозинство земји-членки како една од главните пречки на меѓународната соработка. Постапките за меѓусебна правна помош се сметаат за бавни, понекогаш непредвидливи, а има потреба и од меѓународно договорени шаблони. Ова прашање особено се влошува кога соработката се одвива надвор од правната рамка на ЕУ.

Соработка надвор од правната рамка на ЕУ се смета за процес кој одзема време и се карактеризира со поголема сложеност поради недостатокот на усогласеност меѓу различните правни системи, паралелно со елементите на непредвидливост и недоследност. Појасните оперативни процедури, подобрената редовна размена меѓу точките за контакт, јасното поставување по однос на барањата на МПП и дискусија од самиот почеток би помогнале да се поедностави процесот.

Технологијата им овозможува на криминалните мрежи да организираат и контролираат активности за експлоатација оддалеку - на пример, од друга земја - честопати знаејќи дека барањата за судска соработка нема да бидат навремено исполнети, ако бидат и воопшто исполнети. Ова создава потреба за подобрување, или во некои случаи воспоставување на договори со земјите на потекло на жртвите доколку тие се надвор од ЕУ.

Предизвиците во обработката на МПП може да произлезат и од **недостатокот на соодветно обучен персонал** за составување и процесирање на барањата, како и од употребата на застарена технологија.

Електронските докази може да ја отежнат идентификацијата на точната локација на податоците и земјата под чија надлежност и јурисдикција се таквите податоци, со што изготвувањето на барањето за МПП ќе биде предизвик.

Упатени се повици за заедничка правна рамка за **брза размена на дигитални докази**. Неколку земји изразија загриженост поради отсуството на хомогена регулатива за **задржување на податоците**, што ја попречува размената на електронски докази. Генерално, земјите-членки ја изразија потребата од посеопфатна рамка која го регулира задржувањето и преносот на електронски докази и заедничката правна рамка за замена на тековните ад-хок билатерални работни договори меѓу државите и приватните компании кои ги поседуваат податоците (види и во продолжение). Земјите-членки, исто така, ја истакнаа потребата од подобрување на размената на податоци за време на истрагите.

Предизвици за соработка со приватните компании

Неколку земји посочија дека давателите на интернет услуги (ISPs), поставувачите на содржини (hosts) и компаниите сопственици на социјални медиуми генерално биле кооперативни кога станувало збор за прашања поврзани со ТЛ и сексуална експлоатација на деца. Сепак, идентификувани се голем број предизвици. Вклучувајќи:

- **Добивање на навремен одговор** од некои даватели на интернет услуги и поставувачи на содржини. Комуницирањето со поставувачите на содржини преку писма испратени преку релевантни органи може да доведе до долги периоди на

чекање што носи ризик дека содржината може да биде избришана до моментот кога ќе се постапи по барањето;

- **Појаснување на законските барања** според кои работат ИКТ компаниите и давателите на интернет услуги. Некои земји изразија загриженост дека некои даватели на интернет услуги наметнуваат формалистички, „правно неоправдани" барања кога станува збор за органите на прогонот и соодветно не ги мотивираат и не ги објаснуваат одбивањата;
- **Непостоење на назначена контакт точка** во приватните компании. На големите компании кои работат во повеќе земји често им недостига персонал со соодветни јазични и правни вештини релевантни за секоја земја во која работат;
- **Непознавање** од страна на поставувачите на содржината и компаниите сопственици на социјалните медиуми за тоа која национална агенција/институција е одговорна за кои одлуки, на пр. отстранување на нелегална содржина. Имаше предлози да се воведе улогата на „доверлив означувач", односно да се идентификуваат конкретни агенции/институции кои имаат задача да се поврзат со меѓународните даватели на услуги за да ја отстранат содржината. Доверливиот означувач ќе има отворен канал за комуникација со компаниите и ќе изгради меѓусебна доверба.

Докази од НВО

Општо земено, доказите од невладините организации укажуваат на слични прашања со она дискутирано погоре. Поконкретно, НВО ги истакнаа следниве прашања:

- **Непостоењето на капацитет** меѓу органите на прогонот, што вклучува недостаток на обука, хардвер и софтвер и ограничена употреба на специјални истражни техники. Исто така, постои недостиг од специјализација кај некои полициски сили и судството во врска со ТЛ преку користење на технологија;
- **Брзото менување на технолошкото опкружување и начинот на делување на сторителите**. На професионалците им е тешко да останат во тек со ТЛ преку користење на технологија, што ја попречува нивната способност навремено да ги идентификуваат случаите. Знаењето за техничкото опкружување и практиките (*modus operandi*) честопати претставуваат паралелни процеси кои не се преклопуваат;
- Користење на приватни форуми, виртуелни простории за разговор [chat rooms] или шифрирани апликации за контакти помеѓу престапниците и жртвите. Ова го отежнува (а) откривањето на таквите контакти и (б) стекнувањето на докази што треба да се користат на суд. НВО предложија во виртуелните простории за разговор и апликациите да се вклучат информации/предупредувања за безбедно користење на приватните канали за комуникација;
- **Правилата за заштита на податоците и приватноста** може да ја попречат идентификацијата на жртвите, како и на трговците со луѓе. Правилата на GDPR ја ограничуваат употребата на технологијата за откривање на дигитални траги што ги оставаат и жртвите и сторителите;
- **Непостоењето на интердисциплинарна технолошка соработка** меѓу приватните компании, јавните агенции и невладините организации за целосно искористување на зголемениот број на податоци за ТЛ;
- **Непостоењето на технолошка стратегија** во националните акциски планови за борба против ТЛ;

- **Непостоењето на капацитет, ресурси и технички алатки** меѓу НВО за редовно откривање на онлајн експлоатацијата преку користење на технологијата;
- **Конфликтни цели** или различни пристапи помеѓу НВО и органите на прогонот.

Докази од технолошките компании

Како што е наведено погоре, само две компании дадоа одговори на прашалникот. Facebook наведе дека корисниците „ретко ја пријавуваат" содржината поврзана со трговија со луѓе. IBM наведе неколку пречки за соработка со органите на прогонот, вклучително и загриженост за законитоста на таквата соработка, особено во врска со приватноста на податоците и правната сложеност на повеќе надлежни јурисдикции. ИБМ, исто така, побара појаснување во врска со меѓународните правни дозволи за собирање и споделување податоци со органите на прогонот.

Стратегии и добри практики

Откривање на случаи на ТЛ преку користење на ИКТ

Земјите укажаа на спроведување на различни стратегии за откривање на случаи на онлајн ТЛ преку користење на ИКТ. Широко цитирана стратегија е **следењето на интернет**, вклучувајќи форуми и, во некои случаи, мрежи TOR (Dark Web). Ова е комбинирано со употребата на **разузнавачки податоци од отворени извори достапни на јавноста (OSINT)**, што значи собирање податоци од социјалните медиуми и други јавно достапни онлајн извори во врска со мрежата на контакти, условите за живеење и финансиската состојба на една личност.

Некои земји формираа **„компјутерски-патроли" со специјализирани службеници** задолжени да спроведуваат OSINT истраги на Интернет. Некои јурисдикции дозволуваат тајни онлајн истраги (компјутерски-инфилтрација).

Веб-скрејпинг алатки специјално развиени за извлекување информации од веб-страниците се користат од страна на некои агенции на органите на прогонот, особено во насока на идентификување на ризикот и ранливоста на веб-страниците со содржини за возрасни (ASW).

Поврзано со OSINT истрагите, се користат **техники за анализа на социјалните мрежи** за да се разбере и реконструира мрежата на контакти на сторителот и/или жртвата. **Поврзување на информациите** е клучно: информациите собрани од различни извори може да се систематизираат и да се користат **за откривање на криминалните мрежи**, т.е., релациите меѓу местата, сторителите и жртвите.

Меѓутоа, не сите земји-членки посочија дека користат „проактивни" стратегии. Неколку земји-членки посочија дека нивните истраги за ТЛ преку користење на ИКТ остануваат „реактивни".

Неколку земји имаат имплементирано **системи за корисниците на Интернет да можат да ги пријавуваат содржините и веб-страниците** за кои се сомневаат дека се поврзани со нелегални активности, вклучително и сексуална и трудова

експлоатација. Во некои земји, на пример, Франција, од давателите на пристап на интернет и од поставувачите на содржини на веб-страниците се бара да им помогнат на органите на прогонот во борбата против ширењето на материјали поврзани со конкретни прекршоци, вклучително и ТЛ. Од нив се бара да постават лесно достапен и видлив систем кој ќе му овозможи на секое лице да означи сомнителен материјал.

Некои земји пријавија употреба на **кампањи за подигање на свеста** за да се зголеми откривањето на случаи на ТЛ преку користење на ИКТ. Вклучувајќи и кампањи за подигање на свеста за клиентите кои користат веб-страници кои поставуваат огласи за сексуални услуги за да ги информираат за ризикот дека може да наидат на случаи на ТЛ (Белгија и Обединетото Кралство) и кампањи кои обезбедуваат информации за тоа како да се бараат безбедни можности за работа (Полска и Бугарија). Властите на некои земји ги користеа социјалните медиуми за да шират таргетирани информации, понекогаш преку создавање таргетирани реклами на Facebook поврзани со линијата за пријавување.

Истрага во случаите на ТЛ преку користење на ИКТ

Во некои земји, агенциите на органите на прогонот вршат **компјутерски-инфилтрација** во криминалните мрежи користејќи тајни техники, како и прикриени истраги. Неколку земји изразија потреба од зголемување на ваквите **тајни истраги**, па оттука произлезе и потребата од инвестирање во обука на специјализираните службеници. Постои широк консензус за важноста од набавувањето и пристапот до **специјализиран софтвер**, како и за важноста на масивните податоци (big data) и подобрувањето на способностите поврзани со големите податоци. Развојот на алатките за преземање информации од мобилните телефони заобиколувајќи ја лозинката и за дешифрирањето на разговорите преку апликациите за комуникација исто така се смета за клучно.

Инвестирањето во човечкиот капитал нашироко се смета за еднакво клучно како и инвестирањето во технолошката опрема. Инвестирањето во човечкиот капитал може да значи обезбедување на континуирана обука и развојни активности за службениците на органите на прогонот кои се засноваат на најдобрите локални и глобални практики. Исто така, неколку земји ја истакнаа важноста од вклучување на специјализирани истражни службеници со „дигитално знаење" во истрагите поврзани со ТЛ. Еден модел е заинтересиран за обезбедување на присуството на персонал специјално обучен за спроведување истраги на Интернет и на социјалните мрежи вградени во секоја единица специјализирана за борба против ТЛ. На овој начин ќе се создадат **групи за техничка поддршка** на истражителите. Таквите групи би можеле да бидат екипирани од полициски службеници или цивилни лица кои работат во полициските служби.

Понатаму, земјите-членки ја истакнаа вредноста на **меѓу-агенциската истражна работа** со вклучување и соработка на широк опсег на специјализирани агенции – како и споделувањето на знаењето во рамките на институциите. Слично на тоа, земјите ја истакнаа важноста од **унапредување на преку-граничната соработка** преку, на пример, меѓусебната размена на службеници со земјите на потекло на жртвите. На оперативно ниво, земјите истакнаа дека истрагата може да биде олеснета со **олеснување на меѓу-државното чување на доказите и пристапот до нив**.

При спроведување на истраги, на земјите им беше предложено да не се потпираат претерано на **пропишаната листа на индикатори**, на пр. идентификување на високоризични онлајн огласи, туку и да ја земат предвид и слоевитоста на

информациите од различна природа, вклучително и разузнавачките податоци, информациите од отворени извори и полициските досиеја. Нагласена беше и **важноста на анализата на мрежите и поврзаните податоци**.

Иако одзема многу време, **стратешката анализа** која генерира знаење за новите трендови и ажурираните информации за *начинот на делување* на сторителите (вклучувајќи ја технологијата и веб-страниците што ги користат сторителите) се смета за многу важна.

Технологијата може и да се користи за да **се олесни собирањето докази од жртвите** и за време на истрагата и гонењето на случаите на ТЛ, како и за да се намали товарот на жртвите.

Поттикнување на меѓународната соработка

Земјите-членки ги идентификуваа следниве добри принципи за поттикнување на меѓународната соработка:

- Искористување на ресурсите достапни во рамките на агенциите како што се Европол и Европравда, и формирање ЗИТ за оние земји кои се дел од Судската рамка на ЕУ;
- Воспоставување контакт со други заинтересирани страни во раната фаза на истрагата;
- Постигнување на многу добро разбирање на правниот контекст и можностите за соработка со други земји;
- Организирање на координативни состаноци за размена на информации и докази што е можно побрзо и поекспресно и за дефинирање на заедничка стратегија од *самиот почеток*;
- Постигнување на заедничко разбирање за стандардизираните пристапи и обезбедување на транснационална интероперабилност на органите на прогонот преку транснационални сесии за обука.

Соработката со власти кои не припаѓаат на полицијата, а која е често занемарена, може да биде исто толку релевантна како и полициската соработка, особено во контекст на ТЛ за трудова експлоатација (на пр. меѓу трудовите инспекторати).

Идентификација и помош на жртвите

Софтверот за распознавање на лица се чини дека е широко користен во случаите на сексуална експлоатација на деца (CSE). Со исклучок на CSE, неговата употреба е поограничена. Неколку земји укажаа на употребата на технолошки алатки за идентификување на жртвите на ТЛ кои користат масивни податоци (најчесто веб-роботи, но исто така и алатки за распознавање на лица под построги услови).

Неколку земји се потпираат на индикатори за идентификација на случаи на ТЛ („**црвени знаменца**"); сепак, ова се „општи" показатели за ТЛ и не се однесуваат конкретно на ТЛ преку користење на ИКТ. Иако постои јасна потреба за развивање на показатели кои конкретно ќе се однесуваат на ТЛ преку користење на ИКТ, властите исто така предупредија од прекумерното потпирање на „црвените знаменца". Дури и во случаите

во кои индикаторите се развиени конкретно за идентификација на жртвите на веб-страниците со содржини за возрасни (ASWs), како во Обединетото Кралство, индикаторите покажуваат некои јасни ограничувања и најдобро се користат заедно со **анализата на социјалните мрежи и човечката проценка** на доказите.

Технолошките алатки може да бидат многу вредни во намалувањето на обемот на податоците и справувањето со големите количини на информации; сепак, тие треба да се користат од добро обучени оператори кои имаат познавање од одредена тема/прашање (на пр. ТЛ). Користењето на вештачка интелигенција и технолошки алатки за идентификација на жртвите не е без предизвици, вклучувајќи ја и грижата за етичноста и потенцијалот од дискриминација (на пример, профилирање врз основа на дискриминаторски критериуми; види во продолжение).

Во однос на иницијативите кои се потпираат на технологијата за помош на жртвите и ширењето на информации до ризичните заедници, земјите идентификуваа примери на (1) онлајн механизми и линии за самопријавување, вклучително и дигитална помош преку функцијата за разговор (chat); (2) онлајн кампањи за подигање на свеста, често насочени кон одредени ризични групи (на пр., барателите на работа); (3) целно развиени апликации и онлајн алатки; и (4) официјални материјали достапни онлајн и преведени на неколку јазици. Добра практика е да се работи со приватни компании за продуцирање на **социјално рекламирање** (на пример, развиени во соработка и спонзорирани од страна на социјалните медиуми). Сепак, онлајн кампањите не треба да ги заменат директните, лични контакти со ранливите поединци.

Докази од невладини организации

Невладините организации ја истакнаа важноста од поседувањето на **соодветни и ажурирани информации** до кои лесно може да се пристапи на интернет од страна на жртвите на трговија со луѓе и оние кои се ранливи на експлоатација и злоупотреба. Ваквите онлајн платформи треба да **овозможат и самоидентификација** на жртвите. Ова треба да биде придружено со **кампањи за подигање на свеста**.

Невладините организации дополнително ја истакнаа важноста од градење на знаење за ризиците поврзани со ИКТ, и поопшто ТЛ со поддршка на технологијата, исто така меѓу организациите кои им помагаат на жртвите, вклучително и услугите за советување. Бидејќи **чувањето на електронските докази** е клучно за градењето на силни истраги, од огромно значење е советниците и лицата кои непосредно работат со жртвите на ТЛ од НВО да се запознаат со стратегиите за чување на дигиталните докази (на пример, со зачувување на историите од разговорите [chats]).

Доказите од невладините организации потврдуваат дека „**црвените знаменца**" за случаите на ТЛ преку користење на технологијата не се широко користени. Невладините организации известуваат дека користат стандардни индикатори, но тие бараат **ревидирање на таквите индикатори** за да се земат предвид специфичностите на ИКТ преку користење на технологијата.

Невладините организации идентификуваа примери на **иницијативи со користење на технологија** кои ги развија со цел (а) да го поттикнат онлајн самоизвестувањето; (б) воспостават контакт со ризично население, на пр., да се прекине изолацијата и да се оснажат жртвите; (в) да се подигне свеста кај ранливите и ризичните групи и да се

побара помош, преку апликации и веб-страници направени за таа намена; и (г) да произведува онлајн кампањи за подигање на свеста.

Општо земено, невладините организации сè повеќе ја користат технологијата, но нивното севкупно ниво сè уште останува „ограничено". Постои широк консензус дека може да се направи повеќе за да се искористи технологијата, особено во однос на начинот на кој технологијата се користи за ширење на информациите; да им се пристапи на потенцијалните жртви и да се комуницира со нив; како и да се овозможи добивање на совети и пријави.

Невладините организации, исто така, покренаа некои **критични прашања** поврзани со иницијативите и технолошките алатки, вклучително и потребата од периоди за тестирање на нови алатки и — од суштинско значење — докази за нивната ефикасност (која сè уште е многу ограничена). Тие повикаа на **зголемена евалуација и проценка на влијанието** на развиените технолошки алатки. Дополнително, честопати не постои долгорочна финансиска стратегија за промовирање и искористување на произведените алатки, вклучително и ресурсите за нивно ажурирање. НВО-оата, исто така, нагласија дека, генерално, сè уште постои ограничена достапност на технолошките алатки кои **практичарите *можат* да ги користат** (за да одговараат на потребите на НВО, алатките треба да бидат „евтини и лесни за употреба").

Дополнителни докази од анализата на состојбата

Други прашања покренати во достапната база на докази вклучуваат:

- Потребата да се делува врз основа на информациите добиени со помош на технологијата (во случајот што го дискутираа Ренде Тејлор и Ших (2019), беше откриено дека тешко се постапува по известувањата од работниците добиени преку апликациите за експлоатација во синџирите на експлоатација);
- На технологијата не треба да се гледа како на замена за теренското знаење;
- Групирањето на изворите за откривање на жртви може да покрене прашања за приватноста, како и за потенцијалниот ризик од освета. Додека советите од клиентите се сметаат за многу важни, иницијативите за групирање на изворите треба внимателно да се проверат и да се избалансираат против ризикот од создавање виртуелни (и невиртуелни) групи на осветници;
- Потребата да се подобри собирањето и анализата на дигиталните докази за да се намали оптоварувањето на жртвите (на пр. кога од нив се бара да се обезбедат докази против трговците со луѓе или во корист на нивната одбрана).

Обука: што е обезбедено, што е потребно

Огромното мнозинство земји пријавија дека спроведуваат обука за ТЛ. Сепак, нивоата и форматите на обука што им се обезбедуваат на **органите на прогонот** се различни во различните земји. Некои земји бараат од сите полициски службеници кои би можеле да дојдат во контакт со потенцијална жртва да поминат таква обука, додека други ја ограничуваат обуката на специјализираните единици.

Постои консензус околу фактот дека полициски службениците треба да добијат обука за (а) како да ги откријат случаите и жртвите на ТЛ; (б) како да соберат, складираат и обработуваат електронски докази, вклучувајќи методи за извлекување информации од компјутерите и другите дигитални медиуми; и (в) како да ги користат релевантните софтвери, вклучувајќи „**Анализа на масивни податоци**" и веб-роботи (онаму каде што тоа е дозволено со домашното законодавство). **Обуката за OSINT** се смета за суштинска од неколку земји. Истражните техники кои вклучуваат **тајни онлајн истраги**, исто така, се сметаат за сè поважни.

Додека повеќето земји пријавија обезбедување на елементи од гореспоменатата обука, тие исто така истакнаа определени прашања, вклучително за (а) потребата од постојано ажурирање на обуката и, во некои случаи, значително подобрување на тековните обезбедени обуки; и (б) зголемување на процентот на персонал кој ја добива обуката. Некои земји изразија загриженост во врска со ограничената обука што често се обезбедува во врска со прашања поврзани со ИКТ и, што е уште поважно, ТЛ преку користење на ИКТ.

Во иднина, **ризикот од кочници во системот** е особено акутен. Земајќи предвид дека злосторствата преку користење на ИКТ, вклучително и ТЛ, веројатно постојано ќе се зголемуваат, потребно е да не се потпираме премногу на централизираните оддели за компјутерски криминал. Од клучно значење е да се вклучи општото/основно „**компјутерско" знаење во рутинската обука** обезбедена од страна на инспекторите наместо да се гледа на ова како на збир на „специјализирани" вештини со цел да се избегнат таквите кочници.

Шест широки области се истакнуваат како критични за градење капацитети: собирање и анализа на информации од отворени извори (OSINT); собирање податоци од профили на социјалните мрежи и апликациите за комуникација, како и Darknet/TOR мрежата; испитување на податоците во уредите за чување на комуникации и податоци, вклучувајќи ги и податоците избришани од корисниците, како и познавања од областа на шифрирањето; способност за поткрепување на податоците добиени од ИКТ изворите со дополнителни докази собрани во текот на кривичната истрага; идентификација на жртвите/потенцијалните жртви во онлајн опкружувањето; обука за економски и финансиски криминал со елемент посветен на онлајн трансакциите и потенцијално криптовалутите.

Обезбедувањето на **обука за обвинителите и судиите** во врска со ТЛ преку користење на ИКТ е прилично нерамномерно меѓу земјите-членки. Неколку земји посочија дека во моментов не му обезбедуваат никаква обука за овој феномен на судството. Други земји обезбедуваат општа обука за ТЛ без некој елемент конкретно фокусиран на прашања поврзани со ИКТ.

НВО-оата ја изразија потребата од добивање на обука од домашните органи на прогонот и меѓународните организации за најновите случувања во технолошкото опкружување и во областа на трговијата со луѓе, вклучително и промените во стратегиите за регрутирање/врбување. Тие, исто така, ја истакнаа потребата од обука во врска со најдобрите меѓународни практики и споделување на искуства меѓу земјите.

Правни инструменти

Недостатоците во постојната меѓународна рамка

Генерално, земјите-членки го изразија нивното позитивно мислење за достапните правни инструменти кои овозможуваат соработка меѓу земјите во борбата против ТЛ. Конвенциите на СЕ за меѓусебна правна помош и за компјутерски криминал се сметаат за „најчесто" користени инструменти и генерално, се оценуваат како „соодветни". Сепак, земјите-членки идентификуваа некои потенцијални недостатоци и области во кои сегашното законодавство може да се подобри. Главните идентификувани недостатоци се однесуваат на:

- Непостоењето на заеднички договорено (стандардизирано) правно опкружување кое ја поткрепува размената помеѓу давателите на интернет услуги и властите кога станува збор за конкретни истраги;
- Одредби кои овозможуваат понавремен одговор од приватните компании на барањата за податоци;
- Одредби за принудување на приватните компании да откриваат информации на директно барање/налог од друга држава членка;
- Одредби за спроведување на споделени правила за задржување на податоци;
- Одредби за олеснување на собирањето на сведоштвата на жртвите и нивната употреба во друга земја;
- Прашања во врска со транснационалните мерки против веб-страниците кои поставуваат материјали што може да се поврзат со олеснување на експлоатацијата на жртвите;
- Одредби со кои се воведува „должност на будност" од страна на компаниите на целиот нивен синџир на снабдување;
- Употреба на терминологија која не секогаш дозволува законодавството да се развива паралелно со промените во начинот на делување *(modus operandi)* на трговците со луѓе;

- Разлики во транспонирањето на кривичното делото за трговија со луѓе (според Протоколот од Палермо на ООН) во домашните законодавства.

Конвенцијата за компјутерски криминал (Конвенцијата од Будимпешта) и борбата против ТЛ преку користење на ИКТ

Конвенцијата на СЕ за компјутерски криминал (Конвенсијата од Будимпешта) е најрелевантниот инструмент насочен кон криминалот преку користење на ИКТ што го наведуваат земјите-членки.

Земјите-членки ги сметаат одредбите поврзани со **процесното право** за најзначајни во контекст на ТЛ преку користење на ИКТ (Поглавје II, Дел 2 од Конвенцијата). Понатаму, тие ја истакнаа **важноста на неограничувачките процедурални мерки само за кривичните дела кои се експлицитно наведени** (на пр., оние во Поглавје II, Дел 1) Конвенцијата јасно го постигнува својот целосен потенцијал само кога не е ограничена на кривичните дела експлицитно наведени во Поглавје II, Дел 1. Ова е особено точно во контекст на ТЛ преку користење на ИКТ.

Неколку земји ја посочија корисноста на одредбите вклучени во Поглавје III од Конвенцијата за меѓународна соработка како правна основа за **собирање и споделување електронски докази** меѓу земјите. Конвенцијата воспоставува мрежа на контакт точки. Иако ова е важна алатка, во иднина, веројатно е дека - со сè поцентралната улога што ја играат ИКТ и електронските докази - таквите контакт точки ќе бидат под зголемен притисок - и брзо ќе бидат преоптоварени ако не се екипирани со соодветен персонал. Ова зборува за прашањето на **кочници** во системот, каде што контакт точката која се наоѓа во казнениот систем е клучна и може да предизвика многу последици.

Во иднина, следните чекори може да дозволат **Конвенцијата за компјутерски криминал дополнително да се користи** за борба против ТЛ:

- Имплементација на Вториот дополнителен протокол на Конвенцијата, кој беше усвоен во ноември 2021 година и ќе биде отворен за потпишување на 12 мај 2022 година;
- Завршување на хармонизацијата на националното законодавство со Конвенцијата за компјутерски криминал за да се искористи нејзиниот целосен потенцијал;
- Проширена и подобрена обука за можностите што ги нуди Конвенцијата за компјутерски криминал, бидејќи не сите земји-членки моментално го користат целосниот потенцијал на алатките што им се достапни;
- Поголема свесност за опсегот на процедуралните одредби вклучени во Конвенцијата, бидејќи доказите сугерираат одреден степен на несогласување меѓу испитаните земји за степенот до кој сегашните одредби може да се применат во случаите на трговија со луѓе;
- Спроведување на постапка за забрзување на обезбедувањето МПП преку давање можност за испраќање барање директно до субјектот кој се наоѓа во странската јурисдикција, под услов да е известен судскиот орган на таа земја;
- Градење синергија помеѓу ГРЕТА и Комитетот на конвенција за компјутерски криминал (ТС-Y) за континуирана проценка на употребата на Конвенцијата за компјутерски криминал во контекст на ТЛ.

Предизвици идентификувани од невладините организации

Невладините организации забележаа „јасни ограничувања" поврзани со **заштитата на податоците (GDPR) и правилата за приватност**. Понатаму, тие бараат законодавство што дозволува **дигитална форензика** како прифатлив доказ во сите јурисдикции. Дополнителните предизвици се однесуваат на ажурирањето на регулативите кои треба да го земат предвид компјутерскиот криминал и интернетот, како и да осмислат законодавство и оперативни правила за дигиталните истраги.

Домашни правни рамки поврзани со отстранувањето на содржини поврзани со ТЛ

Огромното мнозинство на земји имаат законски мерки за регулирање на идентификацијата, филтрирањето и отстранувањето на содржините на интернет поврзани со ТЛ. Мерките често не се однесуваат конкретно на ТЛ, туку поопшто на „нелегалната содржина"(исклучок се материјалите за сексуална експлоатација на деца). Во некои земји, процедурите за отстранување на содржината поврзана со ТЛ бараат судски налог. Некои од овие земји ги сметаат овие постапки за „премногу ригидни" или неефикасни и се залагаат за поефикасни средства. Конечно, некои земји нагласија дека давателите на услуги лоцирани во странство можат лесно да ги заобиколат националните законодавства за правната одговорност на давателите на услуги за поставување на содржини.

Човекови права, етика и заштита на податоците

Докази од земјите-членки

Сите земји-членки го истакнаа усвојувањето на домашното законодавство со кое се регулира **обработката и заштитата на податоците**. Во однос на **личната заштита на жртвите**, голем број земји забележаа воведување мерки за спречување на престапниците да стапат во контакт со жртвите; испрашување на сведоци преку видео-конференциска врска за да се спречи контакт со обвинетите; а во некои случаи и можноста жртвите анонимно да дадат докази пред суд за да го заштитат својот идентитет.

Земјите-членки посочија дека имаат воспоставено **протоколи во однос на возраста** во форма на различен збир на процедури и заштитни мерки кои вообичаено се применуваат во зависност од тоа дали жртвата е дете (под 18 години). Што се однесува до **родово-сензитивните протоколи**, сите земји за кои се достапни овие информации посочија дека немаат воспоставено такви протоколи, единствениот исклучок е Австрија, која посочи посебен систем за поддршка врз основа на родот на жртвата.

Докази од невладини организации

Како стандардна процедура, невладините организации бараат согласност од жртвата пред да споделат информации со органите на прогонот. Предизвиците се јавуваат кога жртвите не сакаат да поднесат пријава до полицијата поради различни причини, вклучувајќи го и ризикот од одмазда, социјална исклученост или можноста за депортација на жртвата. Невладините организации проценуваат дека ова е случај за „многу жртви на трговијата со луѓе". Прашањата кои се однесуваат на заштитата на податоците и споделувањето на податоците може да создадат **морални дилеми**. Додека споделувањето на податоците со органите на прогонот и поднесувањето пријави

е во насока на *поддршка* на истрагите, што има потенцијал да спаси и заштити повеќе жртви, тоа носи последици за самата жртва, која може да биде изложена на ризици и закани.

Невладините организации повикаа на поголемо внимание во однос на **потенцијалните ризици и штети генерирани од собирањето на податоци од големи размери и технолошките алатки**. Тие, исто така, повикаа на понатамошно размислување и дополнителни контролни мерки во врска со употребата на податоците и нивното безбедно складирање - и во врска со гарантирањето на самото почитување на правилата за заштита на податоците.

На крај, постојат многу ограничени докази за **родово-сензитивни протоколи** изработени од НВО-а. Вообичаено се воспоставуваат **протоколи за возраста** врз основа на тоа дали жртвата е малолетна или возрасна.

Дополнителни докази од анализата на состојбата

ИКТ може да има значително влијание врз **човековите права** на поединците, вклучувајќи ги правата на приватност, слобода на изразување и ослободеност од дискриминација. Политиките кои предвидуваат исклучителна употреба на технологијата за борба против трговијата со луѓе треба да бидат изработени на начин на кој ќе се земат предвид човековите права.

Утврдени се клучните прашања кои се однесуваат на **приватноста на податоците, етиката, транспарентноста, отчетноста и информираната согласност**. ОБСЕ (2020) идентификуваше голем број етички прашања поврзани со развојот на технологијата за борба против трговијата со луѓе, вклучувајќи: (а) заштита на приватноста на податоците; (б) протоколи за согласност потпишани од жртвите; (в) обука за лица кои ракуваат со сензитивни податоци, особено со податоци за жртвите; (г) безбедно складирање на податоци; (д) спречување на употребата на технологија за добивање сензитивни податоци за ранливите луѓе (на пример, целосно собирање на податоци за ранливите или маргинализираните популации, што создава ризик од дискриминаторски практики); и (ѓ) користење на технологијата на начин на кој не се нарушуваат човековите права на жртвите, како и оние на општата популација. ICAT (2019) и другите извори укажаа на чувствителноста околу споделувањето на податоците. Кога податоците се споделуваат меѓу земјите и/или релевантните агенции, потребно е тоа да се прави во согласност со принципите на приватност и доверливост.

Гери и др. (2016) предупредија за ризикот од широко распространетите **алатки за следење** во борбата против трговијата со луѓе. Иако таквата технологија може да понуди нови можности за интервенирање во ситуациите на трговија со луѓе, таа исто е **форма на надзор што е потенцијално многу инвазивна** за приватноста на една личност.

На крај, неколку извори, вклучително и Миливојевиќ и др. (2020) и Гери и др. (2016), ја истакнаа важноста од **неисклучувањето на жртвите од технологијата**, бидејќи пристапот до технологијата може да биде нивниот единствен начин на комуникација со надворешниот свет и може да послужи како важен механизам за справување и надминување на состојбата. Отстранувањето на пристапот до технологијата може да ги

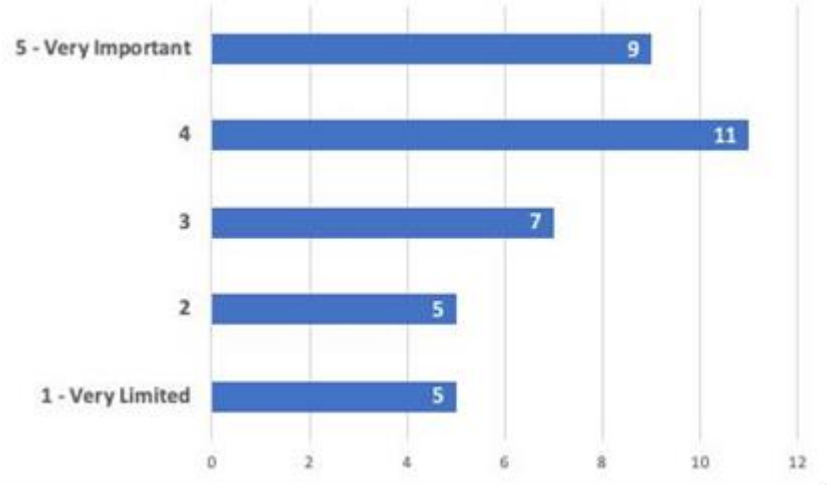
обесхрабри жртвите. Наместо тоа, треба да се фаворизира промовирањето на безбеден пристап до технологијата. Генерално, во центарот на секоја акција треба да биде ставен најдобриот интерес на жртвата.

1. Влијанието на технологијата врз трговијата со луѓе

1.1. Докази од земјите-членки

Доказите поднесени од земјите-членки ја потврдуваат зголемената релевантност на технологијата во контекст на ТЛ, а особено во однос на регрутирањето и експлоатацијата. Технологијата и онлајн активностите стануваат сè порелевантни во животот на луѓето – и тоа се огледува во контекст на ТЛ. Мнозинството земји-членки сметаат дека влијанието на технологијата врз ТЛ е или „многу важно" или „важно" (Слика 1).[4]

Слика 1. Влијание на технологијата врз ТЛ: Земји-членки



5-многу важно 1-многу ограничено
Забелешка: N = 37

Помеѓу земјите кои пријавиле ограничено влијание, некои пријавиле и многу ограничен број или непостоење на случаи на ТЛ (т.е., со ниско ниво на технолошко влијание, ниско ниво на ТЛ во целост). За други земји, употребата на технологијата севкупно е (сè уште) прилично ограничена (т.е. ниско ниво на употреба на технологија, незабележително влијание на технологијата). Во последниот случај, сликата може да се промени земајќи предвид дека технологијата е пошироко прифатена. Навистина, некои земји-членки укажаа на зголемената релевантност на онлајн материјалите, огласите и сајтовите/апликациите во потрагата по работни места, како и **зголемената релевантност** на онлајн социјализацијата и личните интеракции. За возврат, и двете **создаваат можности** за сторителите на трговија со луѓе и ги **загрозуваат постојните ранливости**.

[4] Три земји не додадоа одговор на ова прашање.

1.1.1. Трговија со луѓе за сексуална експлоатација

Во контекст на **врбувањето за сексуална експлоатација**, неколку земји-членки идентификуваа случаи на огласи за вработување кои нудат сомнително високи плати, често во услужните сектори, што се покажа како средство за регрутирање поединци за експлоатација. Неколку земји укажаа на присуството на измамнички или целосно лажни огласи за работа, често објавувани на широко достапни веб-страници и наведени покрај легитимните огласи. Дополнително, постојат докази за регрутирање преку платформите на социјалните медиуми од страна на поединци кои нудат работа, на пример, во угостителството (на пр., келнери) и земјоделството. Сторителите обично ветуваат (непостоечка) добро платена работа во странство, а потоа го принудуваат лицето да врши сексуални услуги во земјата на дестинација.

Според Националниот извештај за состојбата на ТЛ за 2019 година на германските власти, 11% од идентификуваните жртви биле контактирани или регрутирани преку интернет (N = 47). Од тие 47 жртви, 31 биле контактирани преку широко користена платформа на социјалните медиуми и 13 преку рекламни портали (три жртви биле регрутирани користејќи „друг" метод базиран на интернет). Бугарската национална комисија за борба против трговијата со луѓе истакна дека потенцијалните жртви кои се контактираат преку платформите на социјалните медиуми се „главно млади девојки и жени". Врз основа на податоците од полицијата, Холандските власти објавија дека платформите на социјалните медиуми се користат за регрутирање малолетни жртви. Според доказите од Австрија, регрутирањето има тенденција да се одвива во земјата на потекло на жртвите.

Кога им пристапуваат на потенцијалните жртви на интернет, сторителите може да усвојат прилично софистициран модус операнди, често заснован на лажни профили кои покажуваат висок животен стандард и значително богатство. Како што соопштија бугарските власти, „голем број истраги откриле дека пред да им пристапат на нивните потенцијални жртви и да започнат со регрутирање, сторителите внимателно ги испитуваат нивните фотографии [со цел] да ги истражат нивните животни услови, социјалниот статус и околината, семејните односи и статусот на лицето, како на пример дали се во брак, дали се разведени или верени. [...] Само по такво внимателно испитување сторителите контактираат со своите жртви, применувајќи извонредни психолошки вештини за убедување и мотивирање на жртвите да се вклучат во одредени однесувања". Доказите за таквиот начин на работа се огромни и доаѓаат од неколку земји, вклучувајќи ги Австрија, Босна Херцеговина, Бугарија, Белгија, Хрватска, Унгарија, Република Молдавија, Холандија, Полска, Португалија, Словачка, Шведска и Украина. Ваквиот модус операнди често е дел од таканаречената техника „љубовник", односно глумење романтична врска за да се принуди жртвата на проституција. Како што оценија романските власти, меѓу другото, „техниката љубовник продолжува да биде најчесто користената алатка". Се состои во контактирање на лицето преку онлајн платформа, запознавање со нивните хобија и интереси, нивната семејна ситуација и лични околности (како и ранливости). По што, „трговецот со луѓе ѝ пристапува на жртвата со емпатија, со голема подготвеност да ѝ помогне и да ја разбере, како и финансиски да ја поддржи. Честопати, жртвата е манипулирана преку ветувања за сериозна врска, понекогаш со понуди за брак, во обид да се стекне нејзината доверба, а потоа психички да се контролира" (доказ од Романија). Според доказите од Белгија, жртвите регрутирани преку платформите на социјалните медиуми имаат тенденција да покажат модели на семејна нестабилност, предвремено напуштање на школскиот систем, ниска самодоверба и генерално демонстрираат психосоцијална ранливост.

Доказите од Франција сугерираат дека мрежите за трговија со луѓе од различни националности, вклучително и јужноамерикански, источноевропски, како и француски државјани вклучени во т.н. трговија со луѓе *de cité* („подведување во сиромашни населби“) ги користат социјалните мрежи за регрутирање на жртвите. Мрежите за ТЛ кои вклучуваат поединци од африканските земји се чини дека се исклучок од ова правило. Голем број земји обезбедија докази за регрутирање извршено на апликации за запознавање (вклучувајќи ги Обединетото Кралство, Норвешка, Финска, Австрија, Украина и Белорусија).

Постои значителен број на докази од неколку земји за случаи на **уцени**. Ова често се прави прво со собирање „компромитирачки“ информации за жртвите, на пример со барање голи слики или видеа, а потоа искористување на овие докази за присилување на лицето на проституција. Сторителите најпрво ќе воспостават врска со жртвата, ќе ја стекнат нивната доверба и потоа ќе побараат „компромитирачки“ информации. Докази за таквото однесување се пријавени од страна на неколку држави, вклучувајќи ги Босна и Херцеговина, Бугарија, Хрватска, Холандија, Финска, Литванија и Шведска.

Некои земји дадоа примери на жртви регрутирани преку интернет меѓу поединци кои сакаат да дадат сексуални услуги; сепак, откако ќе се регрутираат, тие потоа се предмет на експлоатирачко работно време и многу лоши услови за сместување и се соочуваат со можности за заработка кои се драстично различни од оние што се рекламираат (докази од Унгарија и Полска). Доказите од Полска, исто така, укажуваат на случаи на жени кои рекламираат сексуални услуги кои се цел на трговците со луѓе, кои се заплашени и принудени да го делат својот профит (механизам сличен на изнуда).

Има многу докази од неколку земји за интернет-страници кои се користат за **рекламирање сексуални услуги**. Вгнездени во таквите реклами, има и огласи поврзани со услугите што ги даваат жртвите на трговија со луѓе. Како што забележаа британските власти, веб-страниците со содржини за возрасни (ASW) „продолжуваат да бидат најзастапениот начин на кој се **овозможува сексуална експлоатација** поврзана со трговијата со луѓе во Обединетото Кралство“. ASW се „привлечни за сторителите, бидејќи степенот на верификација на корисникот е низок, а обезбедуваат пристап до голема потенцијална база на клиенти“ (поднесок од британските власти). Според доказите од Финска, „ИКТ платформите, особено сајтовите за рекламирање базирани на форуми, се главниот *начин на работа* во однос на маркетингот и контактирањето со клиентите во контекст на ТЛ“. Француските власти известуваат дека интернет користеле 65% од идентификуваните жртви на сексуална експлоатација во 2019 година; што е зголемување од 49% во претходната година. Едно клучно прашање нагласено во поднесокот од страна на британските власти - и рефлектирано од други - е дека „рекламите што ги создаваат трговците со луѓе добиваат легитимитет со начинот на кој изгледаат споредени со рекламите што ги создаваат самосталните сексуални работници“. Според финските власти, „жртвите на ТЛ и сексуалните работници кои не се жртви ги користат истите страници“. Честопати претставува голем предизвик за властите да ги сортираат рекламите поврзани со ТЛ од оние објавени од независните сексуални работници (види, исто така, Поглавје 2).

Технологијата може да се користи за **координирање на активностите за време на фазата на експлоатација**, како и за воспоставување контакт со потенцијалните клиенти (вклучувајќи преговарање за цените, одредување локации и склучување договори). Од суштинско значење е тоа што **технологијата овозможува раздвојување** помеѓу местото каде што се врши сексуалната активност и местото каде што се одвива координацијата. Тоа има важни импликации за спроведување на законот.

На пример, властите на Босна и Херцеговина презентираа докази за синџир кој искористувал босански жени кои вршат сексуални услуги во Германија и Австрија - таквите услуги биле координирани и управувани од сторители со седиште во Босна и Херцеговина. Ова вклучува активности како што се уредување на онлајн профилите на жртвите и закажување состаноци со клиенти. Доказите од Франција укажуваат на присуство на платформи за одговарање на повиците и организирање на состаноци од далечина од Кипар (за мрежите на руски јазик) и Кина (за мрежите на кинески јазик). Во голем број случаи разгледани од шведската полиција во 2019 година, имало „сомнежи дека активностите за проституирање биле организирани од криминални мрежи со седиште во земјите на потекло на жените или преку поврзаност со агенција во трета земја". Истиот извештај, исто така, идентификуваше слики на различни жени поврзани со исти или многу слични адреси на е-пошта и/или на исти мобилни телефонски броеви. Властите тоа го посочија како индикатори кои активираат црвено знаменце. Шведските власти наидоа и на случаи на неписмени Нигеријки и Романки кои имале профил на веб-страници со содржина за возрасни. Тоа сугерираше дека таквите профили биле напишани и менаџирани од некој друг - уште едно потенцијално црвено знаменце.

Земјите обезбедија докази за технолошките алатки што ги користат трговците со луѓе за да ги **следат и контролираат** жртвите во фазата на експлоатација. Во случајот пријавен од словенечките власти, трговците со луѓе бараа од жртвите да се пријават онлајн за секоја дадена услуга. Од жртвите исто така се бараше да известуваат за други жртви за да можат трговците со луѓе да имаат целосна контрола врз нивните активности. Во други случаи, беа користени конкретни апликации за следење на локацијата на жртвата.

На крајот, покрај двете „главни" области за регрутирање/врбување и експлоатација, постојат докази дека технологијата се користи за да се помогне во логистиката на трговијата со луѓе, вклучително и купувањето авионски билети, како и, во некои случаи, добивањето на лажни патни и други документи (докази од Кипар). Апликациите и веб-страниците може да се користат и за резервирање имоти во кои се вршат сексуални услуги (докази од Франција, Естонија, Обединетото Кралство и Шпанија). Додека се дел од ТЛ, ваквите активности се помошни на двете основни активности на регрутирање и експлоатација.

Како **трендови во зародиш** во контекст на сексуалната експлоатација, постои зголемување на **преносот во живо** на сексуалните чинови извршени од жртвите на трговија со луѓе. Иако преносот во живо често е поврзан со сексуална злоупотреба на деца, неколку земји сугерираат дека таквиот пренос во живо може да вклучува и возрасни жртви на ТЛ. Кипарските власти забележаа проширување на веб-камерите во живо. Според шпанските власти, трговците со луѓе „сè повеќе" користат веб-страници за пренос во живо (video streaming) за да продаваат услуги обезбедени од жртвите на трговија со луѓе. Слично на тоа, ирските власти го истакнаа брзиот раст на таканаречените апликации за видео разговор „со припејд претплата" [pay-as-you-go], како што се Escortfans и Onlyfans, кои ги заменуваат традиционалните платформи на веб-страници, обезбедувајќи можност за гледање на ескортите во приватни или јавни видео простории за разговор (chatrooms). Ирските власти истакнаа дека „природата на овие апликации и веб-страници прави речиси невозможно да се знае дали некој доброволно ги користи платформите или е експлоатиран" (сличен тренд е забележан во Финска). Овој пазарен сегмент, наводно, „забрзано е проширен" од избувнувањето на Ковид-19. Како што забележаа холандските власти, бројот на платформи „се очекува уште повеќе да се зголеми во (блиска) иднина". Овој тренд се прелева и на страниците

и апликациите за запознавање, веб-страниците за рекламирање на сексуални услуги, како и социјалните медиуми кои примарно не се фокусираат на сексуални услуги, но можат да се користат за таа цел.

Кипарските власти, исто така, забележаа зголемување на употребата на апликации за контрола на жртвите, на пр. употреба на автоматизирани пораки испратени до мобилниот телефон на трговецот со луѓе секогаш кога жртвата ќе изврши одредена акција (на пр., кога ќе ја отвори влезната врата). Швајцарските власти на сличен начин укажаа на откривање апликации со услуги за лоцирање на телефоните на жртвите, веројатно преземени без нивно знаење. Сличен тренд на користење технологија за контрола на жртвите е идентификуван и во Австрија. Дополнително, грчките власти пријавија зголемување на регрутирањето деца мигранти за сексуална експлоатација преку мобилни технологии.

Неколку земји пријавија **зголемување на онлајн интеракциите** поради пандемијата со Ковид-19, со што се зголемуваат можностите за трговците со луѓе да воспостават контакт со ранливите поединци. Романските власти забележаа зголемување на бројот на жртви регрутирани онлајн во последниве години, а особено по мерките за јавно здравје како резултат на Ковид-19. Сепак, додаваат тие, во Романија повеќето жртви продолжуваат да се регрутираат преку директен контакт од пријатели, партнери и роднини. Во Франција, властите забележаа промена од проституирање на улица во „подискретен" систем кој се потпира на огласите на интернет по усвојувањето на Законот од 13 април 2016 година кој го забранува купувањето сексуални услуги. Тие понатаму забележаа забрзување на овој процес по пандемијата со Ковид-19. Според шведското обвинителство, користењето на интернет во врска со трговијата со луѓе за сексуални цели е толку распространето што сега „речиси и да не постои случај на трговија со луѓе во кој интернетот не е вклучен" како дел од *начинот на делување* на трговците со луѓе. Белгиските власти очекуваат да забележат зголемување на случаите на ранливи деца или младинци регрутирани преку ИКТ за целите на сексуална експлоатација - бидејќи луѓето од овие возрасни групи сè повеќе комуницираат онлајн или преку ИКТ (во технолошкото опкружување кое постојано се менува и кое претставува предизвик за самата навигација на истражителите).

1.1.2. Трговија со луѓе за трудова експлоатација

Доказите обезбедени од земјите-членки укажуваат дека, во контекст на трговијата со луѓе за трудова експлоатација, ИКТ главно се користат за **регрутирање** жртви. Според германските власти, интернетот и социјалните медиуми играат „сè поважна улога во врска со воспоставувањето контакти и регрутирањето во полето на ТЛ и трудовата експлоатација". Овој став го делат шпанските власти, според кои онлајн регрутирањето за трудова експлоатација „станува сè повообичаено". Овој процес веројатно е забрзан од Ковид-19 и како резултат на растот на онлајн просторите кои ги заменуваат интеракциите и состаноците лице в лице. Како што истакнаа ирските власти, „оваа зголемена употреба на социјалните медиуми за регрутирање на работници мигранти создава се поголем предизвик за властите кои се борат против погрешното и експлоатирачко онлајн регрутирање". Според француските власти, додека „традиционалните форми на регрутирање (огласи во рубриките за вработување во весници, класифицирани огласи, летоци, по препорака, итн.) сè уште се чини дека преовладуваат, употребата на онлајн огласите расте". Ова е поврзано со сè поголемото зголемување на употребата на ИКТ од страна на барателите на работа.

Докази за **лажни огласи за работа кои наведуваат на погрешен заклучок** во контекст на регрутирање за трудова експлоатација се обезбедени од неколку земји, вклучувајќи ги Австрија, Хрватска, Кипар, Естонија, Финска, Франција, Грција, Латвија, Литванија, Република Молдавија, Норвешка, Полска, Португалија, Романија, Шведска и Швајцарија. Бугарските власти го истакнаа присуството на различни веб-страници за наоѓање работа на огласи во кои „работодавачот" ветува големи плати, бесплатен превоз, бесплатно сместување и бонуси за работни места за кои не се потребни високи вештини или течно познавање на локалниот јазик. Ваквите реклами често се дел од *начинот на делување* на трговците со луѓе кои сакаат да регрутираат работници кои потоа ќе се вработат во експлоатирачки услови. Ова се повторува во доказите обезбедени од германските власти според кои „некои сторители првично нудат вработување на различни интернет портали. Работните места треба да бидат добро платени, а работното време наводно регулирано". Меѓутоа, откако пристигнале во Германија, работниците „ниту добиле официјален договор за работа, ниту биле платени како што им било ветено. Честопати воопшто не добивале плата или добивале само мал дел од ветената плата". Слични огласи се идентификувани и во Шпанија, каде што според властите „многу жртви на трговијата со луѓе со цел трудова експлоатација се регрутираат преку рекламни страници на интернет", според властите.

Има докази од Обединетото Кралство за лажни огласи за вработување циркулирани на социјалните мрежи кои промовираат можности за работа за високо платена работна сила/градежници во Лондон – но, во реалноста, како што истакнаа властите, „честопати тоа не е случај и таква работа не постои". Што се однесува до содржината на огласите, британските власти забележаа дека „поголемиот дел од рекламите за регрутирање кои се пријавени како користени од на трговија со луѓе се засноваат на нејасни ветувања за добра работа, платата и услови, без да се наведе видот на работа или платата. Меѓутоа, во мал број на евидентирани случаи, рекламирањето за регрутирање ги содржи овие детали. Кај трудовата експлоатација повеќе од сексуалната, вообичаено е да се опишува секторот на работа, иако редовно се пријавува дека лицата се измамени". Сторителите може навистина да се потрудат за со цел да создадат една претпоставка за легитимноста зад која можат да ја сокријат својата вистинска природа: „Сторителите кои поседуваат бизниси во кои се случува експлоатација, исто така, користат интернет-овозможувачи кои ги рефлектираат (mirror) легитимните оператори на истиот пазар, користејќи златна книга/именик за да ги отсликаат тие што даваат такви услуги и го пресликуваат нивното работно време и понудените услуги" (доказ од Обединетото Кралство). Има докази од повеќе земји кои укажуваат дека огласите обично се стават на „добро познати веб страници за огласи„ во земјата на потекло (доказ од Литванија) и во земјата на експлоатација (доказ од Франција и Грција). Друг modus operandi, акцентиран од страна на Британските власти, укажува дека престапниците употребуваат "Интернет платформа да се идентификуваат улогите или слободните работни места каде да се стават жртвите и да се отворат банкарски сметки за добивање плата" (така наречен модел "без работодавец").

Различни јурисдикции може да ја толкуваат ТЛ за трудова експлоатација на различни начини, а границите помеѓу ТЛ, злоупотребата на трудот и неусогласеноста со прописите може да бидат нејасни и може да варираат од земја до земја (концептуално, тие може да се стават на континуум на сериозност почнувајќи од непочитување на прописите за ситуации во кои се одземаат пасошите и строго се ограничува слободата на движење). На пример, британските власти забележаа дека некои огласи отворено упатуваат на нивоа на плата под националната минимална плата; сепак, „голема е веројатноста дека овие [огласи] се однесуваат на злоупотреба на трудот и неусогласеност со регулативите, наместо на ТЛ". Трговците со луѓе може да „избегнат

да се обврзат на каква било плата, со што ја избегнуваат можноста да го привлечат вниманието на органите на прогонот и регулаторните агенции". Уште еднаш, тоа ги покажува разликите со кои властите се соочуваат во идентификување и отстранување на таквите огласи.

Огласите не се објавуваат само на доверливи веб-страници за работа, туку се објавуваат и циркулираат на социјалните мрежи, на пример во **специјализирани групи за барање работа и групи за взаемна помош** (на пр., „Бугари кои живеат во странство" или „Nguoi tim viec", виетнамски за „луѓе кои бараат работа"). Неколку земји ја истакнаа релевантноста на страниците наменети за поттикнување на размена на информации меѓу работниците мигранти како простор за регрутирање кој е цел на трговците со луѓе - простор кој често е слабо регулиран, бидејќи таквите страници може да ги водат поединци или здруженија со незначителни ресурси. Во некои случаи, таквите огласи може да се циркулираат преку групи за барање работа создадени во апликациите за испраќање на пораки како што е Telegram.

Огласите може да содржат многу погрешни информации за работните услови и надоместоците, а честопати може да се контактира со „работодавачот" или „агенцијата" само преку шифрирани апликации како што се Viber или WhatsApp. Ваквите објави може да допрат до широка публика по многу мала цена или бесплатно. Во социјален експеримент, бугарска невладина организација објави оглас за работа на страница на Facebook во која се нуди работа во Данска за „берење зелена икра" (игра на зборови што потекнува од бугарскиот идиом „да се испрати некого по зелена икра", што значи да се испрати некого во лов на духови), со исклучително високи надоместоци за час. За помалку од една недела, повеќе од 150 апликанти ги доставија своите биографии. Како што беше забележано во неколку поднесоци, нивото на технички вештини потребни за користење на онлајн ресурсите и социјалните медиуми за целите на трговија со луѓе е релативно скромно и слично со вештините кои повеќето корисници на мрежите нормално би ги поседувале (случајно, тоа е далеку од софистицираните хакери и компјутерски криминалци).

Според доказите од Бугарија, огласите често се поврзани со работни места во земјоделството (сезонски работници), на градилиштата, во фабриките и угостителскиот сектор. Други сектори кои се сметаат за изложени на ризик се домашните услуги и услугите за нега. Германските власти го идентификуваа онлајн огласувањето во следните сектори како огласување каде постои ризик: сезонски земјоделски работи, услуги за чистење, етнички ресторани, градежништво, прехранбена индустрија, транспорт и нега (салони за нокти и масажа). Португалските власти пријавија неколку случаи поврзани со лажни огласи за работни места кои наведуваат на погрешен заклучок во секторите земјоделство и градежништво. Шведските власти ги истакнаа услугите за чистење, градежништвото, ресторaните и салоните за нокти. Во продолжение, кипарските власти ги истакнаа понудите за лажни образовни можности на приватни универзитети и колеџи.

Како **тренд во зародиш** во контекст на трудовата експлоатација, бугарските власти пријавија пораст на случаите на регрутирање преку интернет и социјалните мрежи. Се верува дека ова е забрзано со избувнувањето на Ковид-19 и поврзаните мерки за јавно здравје. Слично зголемување на огласите на социјалните мрежи, меѓу другото, забележаа и кипарските, германските и француските власти. Во Франција, властите почнаа да забележуваат употреба на групи за самопомош во заедницата за регрутирање и контрола на жртвите и за трансфер на средства. На крајот, Франција и Обединетото Кралство го истакнаа зголемувањето на можностите за искористување на жртвите

поврзани со „економијата на тезги" (gig economy), бидејќи документите за идентификација не се проверуваат редовно и поединците можат да работат на туѓа сметка. На пример, трето лице може да ги добие сите плати на својата банкарска сметка и само дел да му пренесе на работникот. Според британските власти, „овој *начин на работа* е идентификуван како олеснување на злоупотребата на трудот и незаконското работење, но нивото на контрола што имателот на сметката го има врз финансиите на работникот обезбедува ризик за ТЛ". Овој став го делат француските власти, кои истакнаа дека „иако во моментов формално не е откриен ниту еден случај на трговија со луѓе, се вели дека некои самовработени работници организираат форми на експлоатација со подзакуп на нивната банкарска сметка на нерегуларни мигранти, при што мигрантите работат без надоместок или со многу низок надоместок". На крајот, белгиските власти забележаа дека е можно да се добијат фалсификувани документи на групи кои ги рекламираат нивните услуги на шифрирани апликации за комуникација; таквите документи потоа може да се искористат за олеснување на трудовата експлоатација (пр. фалсификувани документи за идентификација и возачки дозволи, лажни работни договори и лажни работни дозволи).

1.1.3. Dark Web и криптовалутите

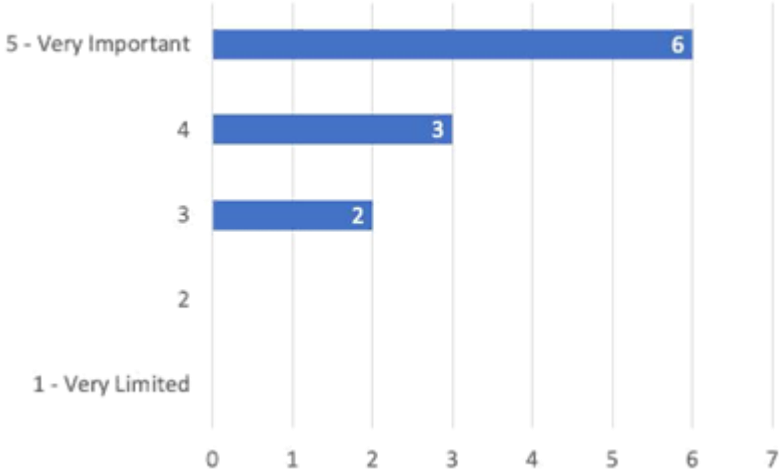
Генерално, земјите-членки не пријавија докази за значителна употреба на Dark Web во контекст на ТЛ. Добиените ограничени докази се однесуваат само на ширењето на материјали за сексуална злоупотреба на деца. Постојат некои докази од Франција за трговците со луѓе кои купуваат податоци за кредитни картички на Dark Web, а потоа ги користат за резервирање соби во хотели и изнајмување апартмани - сепак, оваа активност се чини дека е прилично ограничена и споредна. Норвешките и француските власти забележаа дека сексуалната злоупотреба со пренос во живо (streaming) може да се случи на Dark Web, но не е јасно од обезбедените докази дали овие преноси во живо главно вклучуваат деца или вклучуваат и возрасни жртви. Генерално, многу е веројатно дека Dark Web игра многу ограничена улога во моментот, бидејќи и за време на регрутирањето и за време на експлоатацијата, трговците со луѓе се обидуваат да допрат до најголемата можна публика – а, тоа не е баш компатибилно со Dark Web во неговото сегашно поставување и нивоа на употреба. За регрутирање се претпочитаат платформи со голем број корисници (навистина, една од клучните предности на технологијата е способноста да се допре до големи групи на поединци за релативно мала сума). Слично на тоа, онлајн рекламирањето на сексуалните услуги бара контакт со голема публика - нешто што не е можно во потаинствениот Dark Web.

Се чини дека криптовалутите не се широко користени во контекст на ТЛ (напротив, постојат докази за нивна употреба за купување пренос во живо на сексуална злоупотреба на деца на Dark Web). Трансферите на пари сè уште се вршат преку користење на традиционални методи, на пр. преку компании како што се Western Union или MoneyGram, или, во некои случаи, преку користење на поединци (т.н. „мазги"). Во некои случаи, се искористат и неформалните системи за трансфер на пари, како што е Хавала. Некои земји почнаа да откриваат трансфери на пари преку апликации за испраќање на пораки (на пример, WeChat). Веројатно е дека производите поврзани со финансиската технологија, на пр. трансферите кои се потпираат на апликации, би можеле да играат сè поголема улога во иднина - бидејќи ќе развијат поголем отпечаток во поширокото општество (слично со крипто-валутите, штом - и доколку - постигнат поголема циркулација). На крајот, постојат докази за употребата на картички и ваучери кои не носат лични информации (како што се PaySafe картичките) за плаќање на онлајн услуги, на пр. рекламен простор на веб-страниците со содржини за возрасни.

1.2. Докази од невладини организации

Три од четири невладини организации консултирани за оваа студија сметаат дека влијанието на технологијата врз ТЛ е или „многу важно" или „важно", при што ниту една НВО не укажува на „ограничено" или „многу ограничено" влијание (Слика 2).[5]

Слика 2. Влијание на технологијата врз ТЛ: НВО



5-Многу важно 1-Многу ограничено

Забелешка: N = 11

Севкупно, квалитативните докази доставени од невладините организации кои директно обезбедуваат помош на жртвите на трговија со луѓе даваат слична слика за земјите-членки. НВО ја идентификуваа употребата на Интернетот и социјалните медиуми во сите фази на трговијата со луѓе, а особено во однос на (а) регрутирањето/врбувањето; (б) експлоатацијата; и (в) вршењето контрола и притисок врз жртвите. Тоа е широко споделен став во рамките на невладините организации дека влијанието на технологијата врз ТЛ се зголеми за време на пандемијата со Ковид-19. Сепак, пандемијата можеби само го забрза постоечкиот тренд. Како што е наведено од КОК – германска мрежа од 37 невладини организации кои водат специјализирани советодавни услуги за жртвите на трговија со луѓе – „веќе неколку години, советувалиштата известуваат за сè поголема улога на интернетот и социјалните медиуми во трговијата со луѓе".

Членовите на Ла Страда Интернешнал, европска платформа на НВО-а која обединува 30 организации за борба против трговијата со луѓе во 23 европски земји, пријавија случаи на ТЛ регрутирани преку различни онлајн платформи, вклучително и социјални медиуми и веб-страници за запознавање за сексуална и за трудова експлоатација. Овие случаи се однесуваа на регрутирање на возрасни и на деца. Според податоците од ЦКМ, холандска невладина организација, онлајн контактите играат особено важна улога кога жртвите и сторителите не се познаваат: во речиси 80% од овие случаи, првиот контакт се остварува онлајн, на пр. преку социјалните медиуми или апликациите за запознавање (докази обезбедени од Ла Страда Интернешнал). Ова е особено изразено кај малолетните жртви. Врз основа на интервјуа со жртви на трговија со луѓе, албанската невладина организација „Различни и еднакви" забележа дека социјалните медиуми „станаа главно средство" преку кое сторителите регрутираат жртви. Ова е случај особено за „девојките [регрутирани] за сексуална експлоатација". Во Швајцарија, ФИЗ,

[5] Една невладина организација не даде одговор на ова прашање.

исто така, забележа нов тренд на регрутирање на ТЛ преку различни платформи на социјални медиуми, како и апликации за запознавање. Генерално, постои широк консензус за фактот дека употребата - и важноста - на технологијата во случаите на ТЛ е во пораст - и дека таквата нагорна траекторија е забрзана во последните години.

1.2.1. Трговија за сексуална експлоатација

Стратегиите и механизмите што го поткрепуваат регрутирањето преку социјалните медиуми пријавени од невладините организации се во согласност со доказите веќе дискутирани во Дел 1.1.1 погоре. Има докази за таканаречената стратегија „љубовник", односно воспоставување лична/романтична врска преку социјалните мрежи за последователна експлоатација на жртвата. За таа цел се поставени лажни профили на социјалните мрежи. Жртвите најчесто се малолетни или млади. Ла Страда Молдавија истакна дека се особено ранливи децата од руралните области, од социјално ранливите семејства или со лоша финансиска состојба.

Механизмите слични на оние што беа дискутирани претходно во овој извештај беа истакнати од невладините организации во однос на фазата на експлоатација. Тие вклучуваат употреба на веб-страници за рекламирање сексуални услуги. КОК (Германија) забележа дека е потешко за полицијата и советодавните служби да им пристапат на поединци кои рекламираат сексуални услуги преку интернет наспроти оние што ги обезбедуваат истите услуги во регистрирани установи - со што ја прави идентификацијата на случаите на ТЛ да биде поголем предизвик.

Исто така, во случајот на сексуална експлоатација, сместувањето може да се резервира онлајн преку специјализирани страници (докази од Франција преку Ла Страда Интернешнал).

1.2.2. Трговија за трудова експлоатација

Во однос на регрутирањето за трудова експлоатација, невладините организации дадоа дополнителни докази за механизмите кои веќе беа дискутирани во Дел 1.2.2 погоре, особено за употребата на лажни огласи за работа преку интернет. На пример, во Албанија, невладината организација „Различни и еднакви" забележа онлајн огласи за работа поврзани со експлоататорски практики насочени кон мажи и жени. Во Србија, невладината организација „Астра" изрази загриженост дека дури и агенциите кои се официјално регистрирани во Управата за деловен регистар и со редовна лиценца може да рекламираат незаконски работни места. Забележаа и „голем број" „неовластени" реклами, т.е., реклами на поединци за кои се тврди дека се претставници на агенции, како и реклами поврзани со експлоататорски практики. Повеќето од онлајн рекламите, сметаат тие, „не подлежат на каква било форма на контрола или надзор". Германските и швајцарските невладини организации откриja и докази за онлајн регрутирање за работни места кои или не постојат или се предмет на експлоататорски услови. Ова е во контекст на „пролиферацијата на онлајн регрутирање за работни места" истакната од страна на Центарот за права на мигрантите во Ирска.

Нема докази во поднесоците на НВО дека технологијата игра клучна улога во фазата на експлоатација во контекст на трудовата експлоатација. Сепак, беше означено дека работните места од економијата на тезги (gig economy), особено онлајн платформите за

храна и други испораки, може да бидат подложни на злоупотреба од трговците со луѓе. Како што е забележано од француската невладина организација „Comite Contre l'Esclavage Moderne" (CCEM, француска членка на Ла Страда Интернешнал), иако досега не се идентификувани случаи на ТЛ во овој контекст, процедурите што моментално се спроведуваат од платформите за онлајн испорака може да им дозволат на трговците со луѓе да вработуваат жртви користејќи туѓ идентитет.

1.2.3. Контрола и притисок врз жртвите

Невладините организации забележаа дека технологијата се користи за да се изврши **контрола врз жртвите**, особено во контекст на сексуална експлоатација. Имаше случаи во кои трговците со луѓе се потпираа на видео надзор, мобилни телефони, апликации и софтвер за следење на локациите (доказ од Ла Страда Интернешнал). Сторителите исто така можат да користат ИКТ за да упатуваат закани кон семејството и пријателите, на пр. преку социјалните медиуми, доколку жртвата одлучи да избега од нивната состојба (докази од КОК, Германија). Слични докази собра и невладината организација „Астре" во Швајцарија.

Во продолжение, жртвите може да бидат предмет на **уцена** користејќи социјални медиуми и други онлајн платформи. Ова често се поврзува со заканата да се обелоденат „компромитирачки" информации, вклучувајќи слики и други лични информации (КОК известува за случај на жена вклучена во трговијата со луѓе која ја уценувала нејзината жртва со закана дека ќе го објави нејзиниот статус на заразена со СИДА на Fb).

Клучно е тоа што невладините организации истакнаа дека трговците со луѓе можат да користат ИКТ, вклучително и социјални медиуми и шифрирани апликации, за да го **продолжат контактот** со жртвата на ТЛ дури и откако лицето ќе ја напушти ситуација на експлоатација - често за да ги спречат да поднесуваат жалби и да бараат правда. Во Холандија, ЦКМ откри дека тоа е случај со приближно една третина од жртвите што ги интервјуирале (докази обезбедени од Ла Страда Интернешнал).

1.2.4. Нови трендови

КОК и Ла Страда Молдавија забележаа зголемување на експлоатацијата на децата **преку веб-камери и социјални медиуми**. Според Ла Страда Молдавија, сторителите стапуваат во контакт со деца на социјалните мрежи или **онлајн игрите**, се спријателуваат со нив или симулираат романтична врска. Понекогаш сторителите може да се претставуваат како претставници на агенции за модели. Потоа од детето се бара да сподели интимни фотографии кои потоа се користат за уцена. Тогаш, сторителите бараат од своите жртви да произведуваат и споделуваат повеќе сексуално експлицитни содржини, како и да произведуваат пренос во живо (streaming) на сексуални чинови. Во некои случаи, жртвите се под притисок да регрутираат други деца или да се сретнат офлајн за сексуални односи (КОК забележа слични шеми).

Генерално, Ла Страда Интернешнал и КОК укажаа на зголемената ранливост создадена од **откривањето на големи количини лични информации** на социјалните медиуми и другите онлајн платформи, како и зголемената отвореност со која поединците би

можеле да воспостават интимни контакти со странци на онлајн платформите.[6] Ова е поизразено кај помладите генерации. Иако технологијата може да донесе значителни можности и предности - вклучително и збогатување на размената - таа исто така може да ја загрози ранливоста. На пример, споделувањето сексуално експлицитни слики (секстирање) може да носи ризици поврзани со ТЛ, како и ризици од уцена, генерално. Иако сè уште недостасуваат статистички податоци, истражувањето нарачано од Ла Страда Молдавија во 2020 година со репрезентативен примерок на деца на возраст од 9-17 години дава интересни контекстуални сознанија. Оваа истражување покажа дека 13% од децата во Република Молдавија сметаат дека споделувањето интимни фотографии на интернет е нормално помеѓу луѓето кои се сакаат.[7]; 35% комуницирале со непознати онлајн и 20% се сретнале офлајн со луѓе кои првпат ги запознале на интернет (2% од вторите тврделе дека биле вознемирени од она што се случило на тој состанок).

1.3. Дополнителни докази од анализата на состојбата

Иако технологијата може да влијае на трговијата со луѓе (ТЛ) во сите нејзини фази, нејзината улога е од особена важност во однос на две фази од процесот: регрутирање и експлоатација (Латонеро 2012; Ди Никола и др. 2017 меѓу други автори).

Технологијата може да игра улога во фазата на **регрутирање/врбување** преку олеснување на идентификацијата, локацијата и контактот на потенцијалните жртви. Главната промена што ја донесе технологијата е проширување на досегот на трговците со луѓе во нивната потрага по жртви, истовремено намалувајќи ги „оперативните трошоци" за идентификација и контакт со потенцијалните жртви (Раетс и Јансенс 2018). Сепак, бидејќи последователните интеракции во живо сè уште играат клучна улога, трговците со луѓе сè уште се соочуваат со ограничувања во обемот на нивните операции. Земено предвид дека во игра се различните механизми во зависност од видот на експлоатација, од клучно значење е да се оддели регрутирањето за целите на сексуална експлоатација од регрутирањето за целите на трудовата експлоатација.[8]

Во однос на регрутирањето жртви за **сексуална експлоатација**, технологијата може да помогне при регрутирањето на два начина:

а. Може да го олесни создавањето и ширењето на **онлајн огласите за работа** кои промовираат можности за работа, најчесто во странство, во голем број сектори кои се движат од администрација, чистење или грижа за деца (Европол 2014) до забава, модели, услуги за придружба (ескорти) и сексуална индустрија (CoE 2007; UN.GIFT 2008; Ди Никола и др. 2017).

[6] Исто така, треба да се забележи дека социјалните медиуми и ИКТ генерално, исто така, можат да им помогнат на ГО да идентификуваат и воспостават контакт со потенцијалните жртви на трговија со луѓе (повеќе за оваа точка во Поглавје 3).

[7] Само 1% од испитаниците експлицитно изјавиле дека споделиле интимни (сексуално експлицитни) фотографии и видеа. Овој резултат, сепак, треба да се толкува со претпазливост, поради ефектот на социјална пожелност.

[8] Нема докази дека технологијата се користи при регрутирање за други видови на експлоатација, вклучително и присилно питачење.

б. Може да ја олесни идентификацијата и контактот со потенцијалните жртви, честопати ранливи поединци, преку социјалните медиуми и други апликации за личен контакт (види, на пр., Ди Никола и др. 2017).

Ова може да се смета за специфичен тип на **онлајн груминг**. Пристапот кој се потпира на технологија често се користи во моделот на регрутирање „дечко". Специфичните веб-страници и апликации кои што се користат може да се променат во зависност од однесувањето и преференциите на интернет во конкретните земји. Некои извори укажаа на нова практика на стекнување „компромитирачки информации" за време на регрутирањето, а потоа уценување на жртвите за да добијат контрола (практика слична на „изнуда"; Европол 2020 година).

Во однос на регрутирањето за **трудова експлоатација**, технологијата главно помага при регрутирањето преку ширење на онлајн огласи за работа. Специфични сектори се идентификувани како особено изложени на ризик: жените се со поголема веројатност да бидат регрутирани во однос на лична нега, чистење на домови, фризерски и козметички салони и чување деца, додека мажите се со поголема веројатност да бидат регрутирани во однос на земјоделство, градежништво, транспорт и собирање и испораката на торби од добротворни цели (Европол 2014; Ди Никола и др. 2017; види исто така *Fine Tune Project* 2011 и Совет на Европа 2007). Идентификуваните дополнителни сектори вклучуваат: угостителство, преработка на храна и пакување (*Fine Tune Project* 2011). Рекламите може да се објавуваат на легитимни, широко достапни веб-страници, на ад-хок веб-страници и/или циркулираат преку социјалните медиуми.

Додека одредени извори се чини дека ја нагласуваат физичката поделба помеѓу трговците со луѓе и жртвите постигната благодарение на технологијата (ОБСЕ 2020), реалноста е посложена. Постојат силни докази кои сугерираат дека употребата на технологија ги надополнува наместо да ги замени личните, офлајн интеракции. На технологијата и интеракциите во живо најдобро би било да се гледа како на интегрирани активности. Многу е веројатно дека степенот на влијанието на технологијата зависи од фактори кои се специфични за одредени ризични популации во одредени земји, вклучувајќи: (а) користење на интернет и општо земено социјалните медиуми; (б) користење на интернет и социјални медиуми при барање работа; и (в) технолошка писменост на одредени ризични групи.

Истражувањата сугерираат дека жртвите вообичаено - но не секогаш - се регрутираат во нивната земја на потекло, а потоа се експлоатираат во странство. Овој наод беше веќе нагласен во Советот на Европа (2007), а последователните докази, иако се ограничени, даваат дополнителна поддршка. Импликацијата е дека веројатно ќе бидат потребни билатерални и мултилатерални акции за справување со таквите појави.

Преминувајќи во **фазата на експлоатација**, технологијата може да игра улога во однос на сексуалната експлоатација. Меѓутоа, во овој преглед речиси и да не е пронајден доказ за забележливата улога на технологијата во трудовата експлоатација (Ди Никола и др. 2017; Раетс и Јансенс 2018 меѓу другите).

Во случајот на **сексуална експлоатација**, технологијата може да влезе во игра на два различни начини:

а. Може да ја олесни **контролата** на трговците со луѓе врз жртвите преку користење GPS или други мобилни апликации, со што ќе се ограничи потребата трговците со луѓе да бидат физички блиски. Уцената и употребата на компромитирачки информации

против жртвите, исто така, се споменуваат како можни стратегии за вршење контрола (Раетс и Јансенс 2018). Кај ретки докази, се чини дека уцената на жртвите е идентификувана во релативно мал дел од случаите анализирани во Холандија (8,8% од случаите, без датум; извор: ОБСЕ 2020).

б. Може да ја олесни **продажбата** на сексуални услуги обезбедени од жртвите на трговија со луѓе преку онлајн реклами насочени кон крајните клиенти. Ваквите огласи често се објавуваат на специјализирани веб-страници или ад-хок веб-страници. Севкупно, влијанието на технологијата на **транспортната** фаза се смета за ограничено, бидејќи жртвите често патуваат доброволно и почнуваат да се соочуваат со принуда само кога стигнуваат до одредишната земја (фаза на експлоатација; докази од органите на прогонот од Бугарија, Романија и Италија презентирани во Ди Никола и др. 2017). Употребата на технологијата во оваа фаза е претежно поврзана со мобилните телефони и апликациите кои се користат за организирање патување и координирање на времето и местото на состаноците, како и користењето на интернет за купување билети и правење аранжмани за патување. Иако постои можност трговците со луѓе да го користат Dark Web за да купат фалсификувани билети, како и компромитирани детали за кредитни картички кои потоа се користат за купување (лажни) патни документи, непосредната проценка на повеќе извори, и академски и јавно достапни документи за спроведување на законот, сугерира дека употребата на Dark Web сè уште се чини многу ограничена.

2. Предизвици во откривањето, истражувањето и гонењето на ТЛ со поддршка на технологијата

Ова поглавје ги истражува предизвиците што се јавуваат како последица на употребата на технологијата во контекст на трговијата со луѓе (ТЛ). Не се разгледуваат пошироките предизвици со кои се соочуваат земјите-членки кои не се директно поврзани со употребата на технологијата. Поглавјето најпрво ги истражува предизвиците поврзани со истрагата, проследено со оние поврзани со обвинителството и меѓународната соработка врз основа на докази обезбедени од земјите-членки. Ова е надополнето со доказите собрани од НВО-а, како и прегледот на тековната литература.

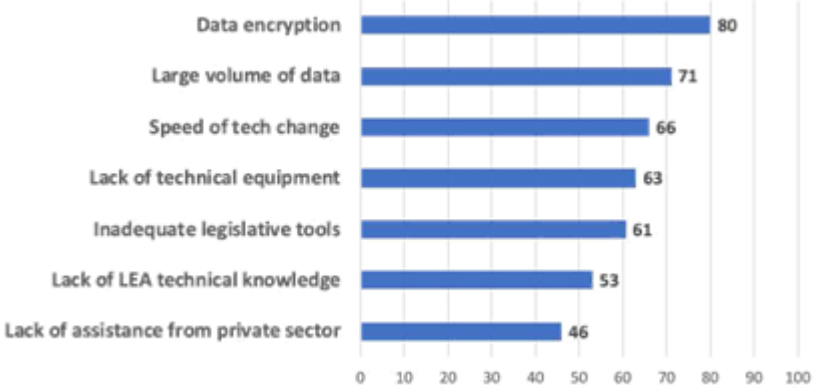
2.1. Предизвици за истрагата

На земјите-членки им беше претставен список со седум потенцијални предизвици за истрагите идентификувани врз основа на преглед на тековната база на знаење, како и претходните работни активности спроведени од ГРЕТА, Групата на експерти на Совет на Европа за акција против трговијата со луѓе и Советот на Европа, вклучително и работилницата од 2019 година за „Засилување на акцијата на Советот на Европа против трговијата со луѓе во дигиталната ера“[9]. Слика 3 го прикажува **резултатот на сериозност** за секој од седумте предизвици[10].

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

[10] За секој предизвик, од земјите-членки беше побарано да ја оценат неговата сериозност користејќи скала од три точки („Нормално не е проблем“, „Мал проблем“ и „Голем проблем“). Ваквите

Слика 3. Резултати за сериозност на предизвиците за истрагите



шифрирање на податоци / голем обем на податоци / брзина на промени на технологијата / недостаток на техничка опрема / несоодветни законодавни алатки / недостаток на техничко знаење кај органите на прогонот / отсуство на помош од приватниот сектор

Забелешка: опсег на резултати = [0, 100]

Шифрирањето на податоците се смета за најтежок предизвик (оценка од 80). На спротивниот крај од рангирањето, недобивањето на помош од компаниите од приватниот сектор се смета за најмалку сериозен предизвик. Сите предизвици освен помошта од компаниите од приватниот сектор имаат оценки повисоки од 50, што значи дека нивното севкупно влијание се смета за повеќе од само „минорен" проблем.

Овие предизвици се оценуваат последователно во следните делови: шифрирање на податоци (2.1.1), голем обем на податоци што треба да се обработуваат (2.1.2), недостаток на техничка опрема (2.1.3), недостаток на техничко знаење кај органите на прогонот (2.1.4) и брзина на технолошките промени (2.1.5). Предизвиците поврзани со помошта од приватниот сектор се дискутирани во Дел 4 во ова поглавје, додека предизвиците кои произлегуваат од законодавните алатки се дискутирани во Поглавје 5. Треба да се истакне дека, иако се дискутираат одделно, некои од предизвиците се испреплетени. На пример, шифрирањето на податоците (и дешифрирањето) бараат континуирани инвестиции во технологијата, како и во градењето експертиза меѓу персоналот на органите на прогонот. Исто така, од земјите членки беше побарано да наведат со какви идни предизвици би се соочувале, покрај седумте веќе идентификувани. Таквите дополнителни предизвици се разгледувани во Дел 2.1.6 во продолжение.

2.1.1. Шифрирање на податоците

Шифрирањето на податоците се смета за главен предизвик со кој се соочуваат властите кога спроведуваат истраги за ТЛ преку користење на ИКТ. Додека влијанието на TOR/Darkweb или шифрираните телефонски мрежи како Encrochat се сметаат за маргинални, земјите укажаа на предизвиците што ги поставуваат протоколите за шифрирање вклучени во широко користените апликации и онлајн услуги (како што се WhatsApp и Telegram). Шифрирањето на податоците може да го „оневозможи враќањето

информации потоа беа трансформирани во резултат со доделување вредност од 0, 1 и 2 на, соодветно, „не е проблем", „мало" и „големо". Резултатите потоа беа пресликани во опсегот [0, 100].

на податоците за време на форензичката истрага" (албанските власти). Властите на Босна и Херцеговина истакнаа дека „се повеќе истраги водат до шифрирани HHD, заклучени телефонски уреди, мемориски стикови и шифрирани податоци". Според исландските власти, повеќето проблеми со кои се соочува полицијата доаѓаат од „анонимни и шифрирани сметки и апликации за е-пошта, како што се Proton-mail или [добивање] информации за претплатникот, на пример". Мониторингот и надзорот се исто така ограничени, ако не и невозможни - дури и со законски налог и спротивно на сите други видови на комуникации. Австриските власти ја истакнаа неможноста да се стави под надзор интернет телефонијата за гласовна комуникација преку интернет (VOIP), додека француските власти ја истакнаа „неможноста за следење на инстант пораките (Whatsapp, Messenger, Tik Tok, Wechat, Snapchat)", создавајќи на тој начин „главна пречка за истрагите (потешкотии во идентификацијата на сторителите и жртвите, воспоставувањето на врски меѓу луѓето, собирањето на докази за принуда и подреденост)"[11]. Белгиските власти понатаму забележаа дека истражните активности извршени во затворени шифрирани канали бараат употреба на информатори и тајни агенти - и тоа може да биде проблематично во одредени јурисдикции (вклучувајќи ја и Белгија). Ирските власти изразија став дека „шифрирањето станува посилно" - и тоа го повторија неколку земји-членки. Разновидноста на шифрираните технологии достапни за поширокатa јавност расте, има сè повеќе и повеќе апликации за инстант пораки чија цел е да го максимизираат шифрирањето и да го минимизираат количеството на генерирани податоци од корисникот (на пр. Threema или Signal).

Како што беше посочено во швајцарскиот поднесок, влијанието на шифрирањето варира во зависност од тоа дали истражителите имаат пристап до физичкиот уред или не. Ако уредот е физички во рацете на истражителите, тогаш „шифрирањето на податоците е помал проблем, а податоците може да се дешифрираат од специјализираните полициски служби" (слична поента беше наведена и од Луксембург). Сепак, службениците со овие технички вештини се ретки и овие служби веројатно ќе бидат преоптоварени, со што би се одолговлечила истрагата. Ако органите на прогонот немаат пристап до физичката поддршка, тогаш „истрагите се потешки" (швајцарски поднесок). Во некои земји, на пример во Обединетото Кралство, полициските сили имаат овластување да побараат од некое лице да им ја предаде лозинката или PIN-от за мобилниот телефон. Сепак, како што се истакнува во британското доставување докази, проблемите остануваат: „дури и при апсење и одземање на такви уреди, може да има бариери за пристап до важни комуникации", особено до уреди со високо ниво на безбедносни карактеристики. Ова го повторија белгиските власти, истакнувајќи дека постојат потешкотии во дешифрирањето на најсофистицираните алгоритми (на тој начин тие повикаа на повеќе инвестиции во нови алатки за дешифрирање).

Неколку земји навестија дека постојат алатки за дешифрирање на барем некои видови алгоритми. Јасно е дека ова технологија постојано се развива и бара (големи) инвестиции и во обуката и во софтверот. Преземените чекори за надминување на ова прашање вклучуваат формирање на единици/центри за компјутерски криминал кои имаат задача да работат на технологијата за дешифрирање. Ова е случајот со Норвешка, на пример. Слично, Франција моментално работи на развој на уред за пробивање на лозинка „на централно ниво".

Словенечките власти го покренаа прашањето за трошоците поврзани со дешифрирањето на електронските податоци. Ваквите трошоци се генерираат од потребата да се ангажира специјализиран високо обучен персонал, како и од

[11] Ова се повторува во доставувањето докази од страна на грчките власти.

купувањето на специјализиран софтвер што можат да го заобиколи шифрирањето. Понатаму, паралелно со развивањето на протоколите за шифрирање, постои потреба од постојано ажурирање на софтверот кој често доаѓа со скапи уплати за лиценца.

Понатаму, би било корисно и да се разгледа можност за споделување ресурси на наднационално ниво во развојот на технолошки производи, како што е софтверот за дешифрирање и веб-роботите како што е предложено, на пример, од шведските власти. Севкупно, од доставените докази произлегува дека може да се направи повеќе во **поттикнувањето на размената на знаење и здружувањето на технолошкиот развој** кај различните земји. Поблиската и соодветно финансираната техничка соработка се покажа како многу успешна, на пример во инфилтрацијата на шифрираната мрежа за пораки Encrochat што ја користат истакнатите организирани криминални групи низ Европа (ова доведе до повеќе истраги од висок профил и судења во Франција, Холандија, Обединетото Кралство и Шведска, меѓу другите земји).

Во некои случаи, како што истакнаа француските власти, шифрирањето може да се надмине преку користење на алтернативни истражни техники, на пример преку „технички надзор на телефонските линии на жртвите [што] останува ефективно средство додека се чека технологија што ќе овозможи заобиколување на шифрирањето".

2.1.2. Голем обем на податоци

Електронските комуникации и ИКТ уредите генерираат непрестајно растечки обем на податоци, што, пак, може да предизвика значителен притисок врз истражителите. Како што истакнаа неколку земји, големиот обем на генерирани податоци има влијание врз способноста за нивно извлекување, за што е потребна моќна техничка опрема. Поедначков предизвик е анализата и внимателното испитување на големите количини на информации. Паметните телефони имаат уште поголем капацитет за складирање. Доказите генерирани од корисниците може да се најдат во повеќе форми: (долги) разговори (chats), но и слики, филмски снимки и гласовни пораки за кои може да бидат потребни „недели" за да се анализираат (докази од Швајцарија). Овој предизвик е особено заострен во случаите кога „не може да се изврши пребарување на специфични клучни зборови и [истражителите] треба да ги прочешлаат сите податоци" (докази од Швајцарија). Според швајцарските авторитети, „искуството и праксата покажаа дека количината на податоци е значително зголемена со модерните социјални медиуми, и потенцијално генерира многу долги истражни активности [...] со кои истражителот може да биде зафатен со месеци и кои може да претставуваат кочници во поглед на ресурсите".
Големиот обем на податоци често бара специјализиран софтвер како и специфична обука за тоа како да се систематизираат и пребаруваат податоците во толку обемен корпус на докази. Според британските власти: „Интернет пазарите и социјалните мрежи генерираат огромно количество податоци [кои] потешко може да се анализираат, а скапо е да се лиценцираат или развијат алатки кои можат ефикасно да ги анализираат овие информации". Француските власти поедначков ја нагласија потребата од развивање на алатки кои може да им помогнат на истражителите во ракувањето со големите податоци, на пример преку користење на алгоритми на вештачка интелигенција (ВИ) (ова беше истакнато и од шпанските власти). Според норвешките власти, обемот на електронски податоци ги прави „истрагите покомплексни со појавата

на потребата од повеќе истражни методи кои се потпираат на технологијата".[12] Меѓутоа, таквите методи често „водат до голем обем на податоци [од кои] само мал дел […] се корисни за истрагата".

Постои широк консензус околу фактот дека градењето капацитет за ракување со голем број електронски докази е од клучно значење. Сепак, таквиот капацитет треба постојано да се ажурира за да се држи чекор „со постојаното менување на интернет-овозможувачите поради брзината на технолошките промени" (британски коментар). Сличен беше и коментарот на холандските власти, кои го истакнаа растечкиот број на податоци генерирани од онлајн платформите и социјалните медиуми, како и предизвикот што го предизвикува **менувањето на моделите на однесување** на нивните корисници, поради што „тешко може да се открие каде да се пребарува". Достапноста на дигиталните алатки се смета за прв (неопходен) чекор; сепак, постојаното прилагодување на технолошката и бихејвиоралната дигитална средина е предизвик, но и неопходен иден чекор.

Тоа што го прави проблемот уште поголем е што честопати треба да се обработат и анализираат големи количини на податоци во кратка временска рамка. На пример, кога осомничениот е приведен, полициските службениците се под временски притисок да прегледаат голем број електронски докази многу брзо – како што истакнаа словенечките власти. Ограниченото време кое често им е достапно на истражителите за преглед на материјалот бара „**подобра технологија за пребарување и сортирање на информациите**" (докази од Обединетото Кралство). Покрај тоа, неколку земји-членки истакнаа дека електронските податоци собрани во контекст на истрагите за трговија со луѓе честопати се на јазик што вообичаено не го зборуваат истражителите, а тоа бара долги и скапи преводи (ова прашање е особено присутно меѓу земјите на дестинација).

2.1.3. Недостаток на техничка опрема

Неколку земји го истакнаа недостатокот на техничка опрема како главен предизвик за истрагите. Ова вклучува често недоволен број уреди способни да извршуваат специјализирани задачи, како што е пробивањето на шифрата, како и потешкотии во следењето на новитетите кои се појавуваат во однос на софтверот и хардверот. Како што веќе беше дискутирано погоре, цената на специјализираниот софтвер и хардвер е висока и често бара постојани ажурирања и скапи договори за лиценцирање со цел да биде во чекор со брзината на технолошките промени. Ова може да има значително влијание врз полициските буџети. На земјите со помала куповна моќ им е тешко да бидат во чекор со барањата во однос на техничката опрема. Да не беше поддршката од меѓународните партнери и донаторите од приватниот сектор, некои земји веќе би биле исфрлени од меѓународниот пазар за специјализирани технички алатки (оваа точка е експлицитно наведена од албанските власти, но тоа произлегува и од поднесоците од другите земји). Сепак, ова во никој случај не е прашање ограничено на земји со помалку ресурси. Германија, Белгија, Шведска, Франција и Обединетото Кралство, меѓу другите, изразија сериозна загриженост за цената на специјализираната софтверска и хардверска опрема.

Повеќето случаи на ТЛ се од меѓународна природа често вклучуваат жртви од помалку богати земји кои се експлоатирани во побогатите нации. Ова генерира потреба од меѓународна соработка меѓу земјите за конкретни случаи. Самото тоа, исто така, се

[12] Португалските власти имаа слична поента.

преточува во често занемарената потреба од унапредени програми преку користење на технологијата поддржани од земјите на дестинација во корист на земјите на изворот (т.е. земјите на потекло на жртвите) - како дополнение на постоечките мултилатерални програми, како што се оние што ги спроведува Европската унија кои веќе обезбедуваат финансиска поддршка за надградба на технолошката опрема.

2.1.4. Недостаток на техничко знаење кај органите на прогонот

Самата техничка опрема има ограничена употреба доколку нема соодветна обука на располагање на органите на прогонот. Поопшто, инвестициите во човечкиот капитал, т.е., во обуката и техничкото знаење меѓу полициските службеници, се исто толку важни како и оние во софтверот и хардверот - ако не и повеќе. Потребата да се обезбеди таква обука и дополнително техничко знаење на полициските службеници беше нашироко споменувана од земјите-членки. Според зборовите на белгиските власти, „императив" е да се намали „**дигиталниот јаз меѓу сторителите и полициските сили**". Земјите-членки идентификуваа различни потреби за знаење. Прво, постои потреба да се развие знаење за појавата на нови трендови и промени во употребата на технологијата и од сторителите и од жртвите. Второ, земјите ја истакнаа важноста од развивање на знаење за појавата на нови апликации и услуги на технолошкиот пазар кој се карактеризира со брзи промени. Трето, постои потреба да се биде во тек со развојот на нови безбедносни протоколи и методи за шифрирање. Од суштинско значење е тоа што знаењето треба паметно да се дистрибуира во една организација. На пример, недостатокот на специјализирани службеници на локално ниво може да создаде **кочници во истрагите**, доколку треба постојано да се бара помош од (зафатената) централизирана единица. Ова е клучно прашање на кое земјите треба да посветат соодветно внимание – и тоа беше потврдено во поднесокот од неколку земји-членки, вклучително и Албанија, Белгија, Исланд, Франција, Португалија, Словачка и Словенија (видете Поглавје 4 за поисцрпни дискусии во врска со обуката).

Неколку земји ја истакнаа потребата од **обезбедување дополнителна техничка обука за „општите" полициски службеници**. Покрај обуката на специјализираните службеници со техничко знаење на напредно ниво поврзано со специфичниот софтвер или техники за дешифрирање, постои потреба да се обезбеди основен пакет за дигитални вештини и техничко знаење за сите службеници. Од клучно значење е полициски службениците кои први интервенираат на местото на злосторството да поседуваат такво знаење. Како што забележаа албанските власти, грешките направени од службениците кои први се појавуваат на местото на настанот „може да бидат фатални при собирањето електронски докази, [кои] потоа стануваат невалидни кога станува збор за понатамошната анализа". На најголемиот број службеници треба да им се обезбеди соодветна обука за стекнување и ракување со **електронски докази**. Исто така, развивањето експертиза во овој домен треба да биде редовна тема во наставните програми за обука на полициските службеници.

Дополнително, иако основното ниво на техничко знаење би било вистинска предност за сите истражители, може да има посложени случаи во кои можеби ќе треба да се формираат тимови со мултидисциплинарни вештини (на пр., со здружување на истражители, специјалисти за финансиски и компјутерски криминал). Земјите можеби ќе сакаат да размислат за воведување – или подобрување – на одредби што ќе го олеснат брзото формирање на таквите тимови, секогаш кога е потребно, или дури и да ги направат интердисциплинарните тимови како еден вид на поструктурна карактеристика на модерната полициска работа. Ова може да се прошири на

меѓународните заеднички истражни тимов, на пр. со вклучување на експерти за технологија и комуникација во таквите тимови (точка што ја истакнаа бугарските власти).

Швајцарските власти забележуваат дека „да се држи чекор со технолошкиот напредок е голем предизвик за органите на прогонот", а денешните истражители потребно е да се специјализирани и за трговијата со луѓе и за ИКТ, вклучително и за користењето на социјалните медиуми и техничките вештини. Француските власти ја истакнаа потребата од обучување на повеќе кадри кога станува збор за новите технологии, како и за финансиските истраги. Бугарските власти објавија пример во кој беа употребени комбинирани истражни техники на интернет и офлајн во соработка со француските власти. Поаѓајќи од откривањето на порнографски слики на деца, истражителите успеале прво да ја идентификуваат IP адресата, а потоа физички да ја лоцираат во хотел. Додека го чешлале хотелот, наишле на голем број жени принудени да нудат сексуални услуги и добиле збир на Facebook називи на други жртви, кои потоа биле идентификувани преку нивните Facebook профили. На крајот, биле идентификувани 60 жртви на трговија со луѓе за сексуална експлоатација, едно дете жртва присилувано да произведува порнографски материјал и 18 престапници. Овој случај укажува на потребата истражните службеници да бидат добро упатени во истражните техники, и онлајн и офлајн, бидејќи е сè поверојатно дека и двете ќе треба да се користат за време на истрагите за трговија со луѓе. Ова, се разбира, бара континуирана обука.

2.1.5. Брзина на технолошки промени

Брзото темпо на технолошките промени е меѓусекторско прашање кое има влијание врз сите предизвици дискутирани погоре: шифрирање, обука на полициските службеници, технолошка опрема и собирање електронски докази. За повеќе детали ве молиме погледнете ја горенаведената дискусијата.

2.1.6. Дополнителни предизвици за истрагите

Голем број земји го означија прашањето поврзано со (несоодветните) **обврски за задржување податоци** која ја имаат давателите на интернет услуги (ISP) и нивното влијание врз истрагите. Во Бугарија, на пример, сегашното законодавство бара од давателите на интернет услуги да ги складираат таквите податоци шест месеци - должина што се смета за несоодветна за водење цврсти истраги. Должината на периодите на задржување на податоците беше спомената и од холандските и малтешките власти. Норвешките власти забележаа дека, според домашното законодавство, на давателите на интернет услуги не им е дозволено да складираат информации за IP адреси повеќе од 21 ден и од нив не се бара да ги складираат информациите на врската помеѓу претплатникот и IP адресата. Бугарските и романските власти повикаа на усогласување на националните регулативи во врска со складирањето на податоците за интернет сообраќајот, како и за истражните практики поврзани со кршењето на законот преку користење на ИКТ.

Забраната за тројанци (т.е. шпионски софтвери) се смета за дополнителен предизвик за истрагите преку користење на ИКТ, бидејќи на органите на прогонот не им е дозволено да влегуваат во домови и други простории со цел да инсталираат шпионски софтвер на уредите што ги користат поединци кои се под истрага. Властите тврдат дека таквите

алатки ќе им овозможат на органите на прогонот да ги ублажат прашањата поврзани со шифрирањето, како и потешкотиите во прислушувањето на разговорите со VOIP. Белгиските власти повикаа на промени во правната рамка за да се олесни истрагата преку користење на нови технологии. Тие ја истакнаа потребата од поедноставување на процедурите и правните алатки земајќи го предвид *начинот на делување* на сторителите.

Бугарските власти покренаа прашање поврзано со електронските докази, конкретно потребата да се воведат меѓународни барања за давателите на интернет услуги да имплементираат соодветни безбедносни протоколи за спречување на какво било **манипулирање со податоците** и за време на складирањето и за преносот до органите на прогонот.

Холандските власти покренаа прашање поврзано со примената на **законите за заштита на приватност**, на пример во контекст на користење на веб-робот.*

Шпанските власти ја истакнаа потребата од зголемување на бројната состојба на персоналот специјализиран за трговија со луѓе со напредни компјутерски вештини. Белгиските власти имаа сличен коментар.

Молдавските власти ги истакнаа потешкотиите во задржувањето на квалификувани практичари бидејќи службениците со искуство често ги напуштаат специјализираните единици за да се приклучат на други делови од судството или приватниот сектор и ја истакнаа важноста од редовни прегледи на мотивацијата за привлекување и задржување на таленти.

Австриските власти го истакнаа проблемот со казните предвидени за ТЛ во нивниот домашен Кривичен законик, кои се движат меѓу шест месеци и 10 години затвор. Иако оваа казна е доволна за следење на пораките со налог од суд, не ги овластува полициските сили да користат визуелен и акустичен надзор (т.е. аудио надзор на приватни разговори и приватни простории).

Британските власти истакнаа предизвик околу IP адресите и електронските докази. IP адресите се почетна точка во истрагата и, откако ќе се добијат, органите на прогонот треба да ги усогласат тие IP адреси со различни називи и кориснички имиња. Сепак, називите може да се менуваат во секое време и често се користат од осомничените наизменично. Во таков случај, од клучно значење е органите на прогонот да го проверат континуитетот на IP адресите со корисничките имиња. Дополнително , во виртуелните простории за разговор (chatrooms), некои корисници може да се видат на екранот -- и нивниот идентитет е докажан - но може да има и други кои ги немаат вклучени нивните веб-камери. Некои осомничени може да споделуваат уреди со други, на пример, ако се во живеалишта во кој живеат повеќе различни луѓе или семејства, што, пак, може да создаде предизвик во нивната идентификација.

Британските власти, исто така, го покренаа прашањето за справување со неискористениот електронски материјал, особено во контекст на обврските за GDPR. На иста линија, холандските власти сметаат дека меѓународните регулативи за заштита на податоците „го попречуваат собирањето, складирањето и обработката на информациите добиени преку технолошки истражни техники (како што е индексирање на веб)", со што „се спречува оптималната употреба на [таквите] техники".

ЗУМ (ZOOM) | Предизвици во откривањето на случаи на ТЛ преку користење на ИКТ

Истрагите и гонењето зависат од самото откривање на случаите. Во продолжение се претставени предизвиците *идентификувани* од страна на земјите поврзани со откривањето на ТЛ преку користење на ИКТ:

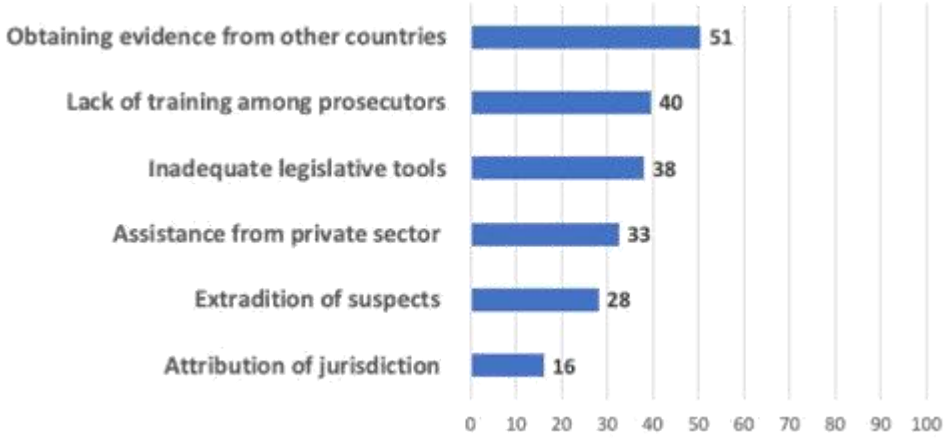
- Интернетот е огромен простор за следење, а обемот на онлајн активности/интеракции постојано расте. Ресурсите на интернет опфаќаат многу широк и разновиден спектар од онлајн-рекламни сајтови и веб-страници за возрасни до платформи за социјални медиуми, простории за разговор (chatrooms) и потенцијално Темната мрежа (Dark Web). Патролирањето и контролата на таквиот простор бара многу ресурси и подлежи на законски ограничувања (закони за приватност и ограничувања за користење на веб-роботи во некои земји).
- Рачното пребарување на онлајн веб-страниците е исклучителен предизвик, додека големите количини на неструктурирани податоци го отежнуваат пребарувањето на Интернетот (доколку тоа воопшто е дозволено со домашните закони). Обемот на онлајн огласите (отворени и класифицирани) и за сексуални и за несексуални услуги често е преголем за да може рачно да се пребаруваат.
- Потешкотиите во идентификувањето и на сторителите и на жртвите бидејќи тие можат да користат прекари и псевдоними кога работат онлајн. Софтверот за анонимизирање (на пример, VPN) и употребата на шифрирана комуникација помеѓу трговците со луѓе и жртвите дополнително ја попречува идентификацијата. Разговорите меѓу трговците со луѓе и жртвите се одвиваат во затворени групи (на пр. Facebook, WhatsApp, Telegram).
- Брзото и променливо однесување на корисниците на Интернет (на пример, појавата на нова технологија, популарноста на нови веб-страници/апликации за кратко време). Покрај тоа, брзо се појавуваат нови алатки, поттикнати од силната конкуренција во технолошкиот сектор, што може да им обезбеди на трговците со луѓе нови средства за поврзување и искористување на жртвите.
- Предизвици во сортирањето на онлајн рекламите за да се идентификуваат оние поврзани со ТЛ – во контекст и на сексуалните и на несексуалните услуги. Рекламите за сексуални услуги обезбедени од жртвите на ТЛ често ги користат истите страници, терминологија и формулации како оние објавени од независните сексуални работници. „Црвените знаменца" за идентификување на рекламите поврзани со трудовата експлоатација сè уште се недоволно развиени или не се користат постојано.
- Отсуство на специјализирани единици во полицијата и/или недостаток на специјализирани истражувачи за трговија со луѓе со напредни компјутерски вештини. Недостаток на службеници обучени да вршат тајни операции на Интернет (на пр. со креирање и одржување на „лажен" профил).
- Недостаток од обука на полициските службеници за специфичностите на ТЛ (на пример, начинот на делување на престапниците, платформите на кои тоа се случува, како тајно да им пристапат на трговците со луѓе и да креираат веродостојни онлајн профили).
- Можност за отстранување/промена на разговорите (електронските докази) од страна на трговците со луѓе.

- Процесот на испраќање барања до компаниите за социјални медиуми (често со седиште во странска јурисдикција) одзема многу време и некои компании дури и не одговараат на таквите барања.
- Кратки периоди на задржување податоци за IP адреси и потешкотии при пристап до нив.
- Јазични бариери.

2.2. Предизвици за кривичното гонење

На земјите-членки им беше претставен список со шест потенцијални предизвици за кривичното гонење, идентификувани врз основа на преглед на тековната база на знаење, како и претходните активности спроведени од Советот на Европа, вклучувајќи ја и Работилницата во 2019 година на тема „Засилување на Акцијата против трговијата со луѓе во дигиталната ера на Советот на Европа"[13]. Слика 4 го прикажува **резултатот за сериозност** за секој од шесте предизвици[14].

Слика 4. Оценки за сериозноста за предизвиците на кривичното гонење



обезбедување на докази од други земји / недостаток на обука за обвинителите / несоодветни законодавни алатки / поддршка од приватниот сектор / екстрадиција на обвинители / доделување на надлежност на јурисдикција

Забелешка: опсег на резултати = [0, 100]

Севкупно, предизвиците на обвинителството имаат пониски резултати од оние за истрагата, при што само „добивањето докази од други земји" е нешто повисоко од 50 (оценките повисоки од 50 укажуваат дека предизвикот нашироко се смета за посериозен отколку само „незначителен проблем"). Ова најверојатно се должи на фактот дека, ако случајот навистина пристигнал во фаза на кривично гонење, повеќето пречки биле успешно отстранети во фазата на истрага.

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

[14] За секој предизвик, од земјите-членки беше побарано да ја оценат неговата сериозност користејќи скала од три точки („Обично не претставува проблем", „Мал проблем" и „Голем проблем"). Ваквите информации потоа беа трансформирани во резултат со доделување вредност од 0, 1 и 2 во „не претставува проблем", „мал" и „голем". Резултатите потоа беа пресликани во опсегот [0, 100].

Во продолжение нудиме дополнителни квалитативни докази за три предизвици: доделување на надлежност (јурисдикција), екстрадиција на осомничени и обука на обвинители. Предизвиците поврзани со помошта од приватниот сектор се разгледуваат во Дел 2.4, додека предизвиците кои произлегуваат од законодавните алатки се разгледуваат во Поглавје 5. Предизвиците поврзани со добивањето докази од други земји се разгледуваат во Делот 2.3, кој ги прикажува пречките за меѓународната соработка.

- *Доделувањето на надлежност (јурисдикција)*: генерално, доделувањето на надлежност (јурисдикција) се смета за мал предизвик меѓу земјите-членки, сепак може да се појават повремени прашања во случаите преку користење на ИКТ во врска со истовремената јурисдикција. Во некои случаи, може да се појават предизвици во идентификацијата на осомничените и, најважно, нивната локација, што значи поврзување на одредена IP адреса со лице, а потоа тоа лице со локација во одредена јурисдикција.

- *Екстрадиција на осомничени*: Генерално, ова се смета за релативно незначителен предизвик. Европскиот налог за апсење (EAW) и Европскиот налог за истрага (EIO) се сметаат за две важни алатки кои „овозможија ефективно (и исто така со одредена брзина) да се одговори на предизвиците што ги носи транснационалноста" (португалски власти). Работата на Европравда е спомената како пример за добра практика. Швајцарските власти ги истакнаа пречките со кои се соочуваат поради неможноста од издавање на EAW и EIO. Слично на тоа, британските власти укажаа дека „излегувањето на Обединетото Кралство од ЕУ може да влијае на екстрадицијата" бидејќи „забраната за државјанство од некои земји значи дека [Обединетото Кралство] повеќе не може да екстрадира некои државјани на ЕУ и бара дискусии за тоа која земја го врши кривичното гонење". Разликите во законодавството за кривично гонење помеѓу земјите може да создадат предизвици во екстрадицијата на осомничените.

- *Обука на обвинителите*: Неколку земји ја истакнаа важноста од соодветна обука за обвинителите во врска со ТЛ преку користење на ИКТ, истакнувајќи дека во некои случаи оваа обука недостасува или не е соодветна. Обуката на обвинителите се смета за клучна во гарантирањето на издржаноста на случаите преку користење на ИКТ, како и во гаранцијата дека електронските докази се правилно собрани и искористени и дека случаите (и доказите во нив) се соодветно презентирани пред судијата/поротата. Некои земји, како што е Норвешка, планираат да ја засилат таквата обука преку ангажирање на обвинител со искуство во случаите на трговија со луѓе кој ќе им држи предавања на колегите. Понатаму, експертизата може да не е постојано достапна во сите обвинителства во една земја. Ова прашање, меѓу другото, го истакнаа и холандските власти. Како одговор, холандското обвинителство, заедно со националната полиција, моментално го проценува нивото на експертиза во рамките на службата. На ваквиот процес на мониторинг во државата може да се гледа како на пример на добра практика за да се обезбеди доследност на нивото на експертиза во рамките на една јурисдикција. Исто така, некои земји-членки забележаа случаи во кои обвинителите не беа запознаени со постапката за барање електронски податоци од приватни компании; во други случаи, обвинителите не беа запознаени со процедурите за прибавување докази и соработка од други земји, на пример преку формирање на Заеднички истражен тим или издавање на европски налог за истрага. Унапредената обука на обвинителите треба да го олесни процесот на поврзување со други земји, како и со приватни компании. На крајот, земјите-членки го изразија ставот дека интердисциплинарната обука со елементи од ТЛ и ИКТ треба да биде обезбедена и на судиите.

Понатаму, од земјите-членки беше побарано да наведат со кои **дополнителни предизвици** се соочуваат во гонењето на случаите на ТЛ преку користење на ИКТ. Во продолжение е дадено резимето на идентификуваните предизвици:

- Британските власти го истакнаа проблемот со докажувањето на учеството и *mens rea* на поединечните сторители во случаите преку користење на ИКТ при постоењето на групна активност, на пример во просториите за разговор (chatrooms) на интернет каде што еден екран може да прикажува злоупотреба на жртва на трговија со луѓе додека другите екрани може да прикажуваат други корисници кои како возрасни единки согласно учествуваат во определени активности. Докажувањето на учеството на различни поединци може да биде предизвик со оглед на различните улоги за кои станува збор.

- Дополнителен предизвик истакнат во поднесокот од страна на британските власти се однесува на презентирањето на доказите пред поротата (или судијата). Во случаите преку користење на ИКТ, презентирањето на техничките докази често се врши од експерт запознаен со технологијата (кој објаснува како, на пример, функционира преносот во живо од просториите за разговор (chatrooms) на интернет, неговите функции и какви снимки можеби се снимени, вклучително и описот на тоа што содржи снимката). Развивањето на институционална експертиза меѓу службениците за тоа како ефективно и точно да се презентираат електронски докази станува сè повредна. Уште еден поврзан предизвик се однесува на презентацијата на големи количини електронски материјал пред поротата. Решението што се разгледува во Обединетото Кралство е употребата на таблети.

2.3. Предизвици за меѓународната соработка

Студијата побара од земјите-членки да ги наведат предизвиците со кои се соочуваат во однос на транснационалните истраги и судската соработка во контекст на ТЛ преку користење на ИКТ. Повеќето од нагласените предизвици не се специфични за ТЛ преку користење на ИКТ, туку влијаат на прекуграничните истраги и општо на судската соработка, на пр., јазичните бариери, различната правна основа, координацијата на паралелните истраги, брзата размена на информации. Сепак, специфичностите на ТЛ преку користење на ИКТ, често ги влошуваат. Ова е особено случај кога станува збор за електронските докази. Дополнително, во контекст на ТЛ преку користење на ИКТ, кога станува збор за добивање на меѓусебна правна помош и обезбедување докази во таквите случаи честопати брзината и временската рамка се критични.

2.3.1. Барања за меѓусебна правна помош

Долгиот период за одговор кога станува збор за обработка на барањата за меѓусебна правна помош (МПП) беше означен од страна на мнозинството земји-членки како една од главните пречки за меѓународната соработка. Севкупно, процедурите за меѓусебна правна помош се сметаат за бавни, понекогаш непредвидливи и имаат потреба од меѓународно договорени унифицирани шаблони. Како што забележаа шпанските власти, „премногу извори на информации бараат судско овластување за пристап до нив". Ваквите барања треба да се обработуваат преку МПП, што, пак, ги комплицира и ги продолжува истрагите. Сегашниот систем е опишан како „несоодветен" од неколку

земји. Барањата за МПП меѓу земјите-членки на СЕ може да се случат во две различни сценарија: (а) како дел од рамката на ЕУ за судска соработка (вклучително и преку помош од страна на Европол и Европравда) и (б) надвор од рамките на ЕУ. Бидејќи предизвиците и процедурите може да бидат радикално различни во зависност од сценариото, важно е да се дискутираат посебно.

Соработката како дел од правната рамка на ЕУ. Земјите-членки на СЕ, кои се исто така членки на Европската унија, сметаат дека координираната рамка за полициска и судска соработка со ЕУ е корисна и е способна да го ублажи процесот. Тука е вклучена работата на агенциите на ЕУ како што се Европравда и Европол. Сепак, предизвиците сè уште постојат. Според француските власти, „алатките за меѓународна соработка, иако се интересни, се бавни: европскиот налог за истрага (ЕИО) трае неколку месеци, а Заедничкиот истражен тим (ЗИТ) е тешко да се спроведе". Една од главните пречки за имплементацијата на ЗИТ е потребата од паралелна истрага во другата земја(-и). Ова беше истакнато и од норвешките власти.

Соработката надвор од правната рамка на ЕУ. Ова се смета за процес кој одзема повеќе време и се карактеризира со поголеми сложености отколку во горенаведеното сценарио поради недостаток на усогласеност меѓу различните правни системи (како што беше истакнато, меѓу другото, од кипарските и шпанските власти). Швајцарските власти истакнаа дека одговорот на „барањата за меѓународна правна помош честопати зависи од добрата волја или интересот на странските обвинители". Ова воведува елемент на непредвидливост и недоследност во процесот. Ваквите „преговори меѓу обвинителствата честопати се долги". **Појасните процедури за работа, засилената редовна размена меѓу точките за контакт и барањата за МПП кои се јасно поставени** и за кои е дискутирано на почетокот ќе помогнат во изедначувањето на процесот. Властите во Северна Македонија истакнаа дека сите барања за МПП треба да поминат низ централизирано одделение во рамките на Министерството за правда, што претставува кочница и често ги забавува процедурите. Тие предложија да се осмислат алтернативни механизми кои ќе им овозможат на одредени клучни институции да воспостават директен контакт со нивните меѓународни колеги (на пр. Јавното обвинителство, трудовиот инспекторат, Министерството за внатрешни работи).

Норвешките власти ја истакнаа потребата за подобрување на постоечкиот договор и воспоставување нови договори со земјите на потекло на жртвите кога тие се надвор од ЕУ. Ова е точка што ја покренаа и француските власти, кои нагласија дека „голем број криминални организации кои користат ИКТ потекнуваат од земји со кои меѓународната соработка е или недоволна или непостоечка. Тоа е случај со кинеските мрежи и мрежите од Русија и Украина". Благодарение на ИКТ, овие криминални мрежи можат да ги организираат своите операции на начин што ќе им овозможат на главните членови да ги контролираат активностите на проституција од нивната земја на потекло - честопати знаејќи дека барањата за судска соработка нема да бидат навремено исполнети, ако и воопшто бидат исполнети. Бавното темпо или недостатокот на соработка влијае врз идентификацијата на сторителите, врз собирањето на докази и исклучувањето на веб-страниците на Интернет.

ЗУМ (ZOOM) | Што може да се научи од судската рамка на ЕУ?

Нема сомнеж дека судската рамка на ЕУ нуди поинтегриран правен простор кој ја олеснува судската соработка споредено со ситуацијата со која се соочуваат земјите-

членки кога соработкате е вон оваа рамка (иако со ограничувања и предизвици). Кои елементи од таквата рамка би можеле да се прошират вон соработката на земјите во рамките на ЕУ? Ова е тешко прашање кое бара сеопфатна правна анализа, но овде можеме да скицираме некои прелиминарни предлози. Поднесокот на швајцарските власти (т.е. земја надвор од судската рамка на ЕУ) убаво ги сумира клучните предности на рамката на ЕУ, особено на Европскиот налог за истрага (ЕИО):

- се заснова на заеднички збир на правила со широк опсег на примена;
- поставува јасни рокови за прибирање докази;
- основите за одбивање се ограничени;
- го намалува административниот товар преку воведување на единствен стандарден формулар;
- обезбедува заштита на суштинските права на одбраната.

Јасно е дека некои мерки може да се прошират само доколку се дел од сеопфатен збир на споделени правни правила. Сепак, земјите-членки можеби ќе сакаат да разгледаат кои специфични аспекти на ЕИО можат да функционираат надвор од рамките на ЕУ. Ова може да ја опфати соработката меѓу земјите-членки на Конвенцијата за акција против трговијата со луѓе на Советот на Европа и Европската конвенција за човекови права. Мерките околу утврдувањето на рокови за собирање докази и намалување на административниот товар преку воведување стандардизирани процедури потенцијално би можеле да се спроведат без радикални промени во домашните правни системи. Може да се предвидат и некои засилени, заеднички правила, под услов одредбите наведени во Европската конвенција за човекови права да се почитуваат од една држава.

Дополнителните прашања поврзани со МПП. Доказите поднесени од земјите-членки, исто така, укажуваат на предизвиците во обработката на МПП кои произлегуваат од недостатокот на персонал соодветно обучен за составување и справување со таквите барања - како и употребата на застарена технологија. На пример, некои земји посочија дека не секогаш користат безбедни е-пошта и други форми на електронска кореспонденција кога разменуваат документи со странски партнери. Развивањето на употребата на безбедни форми на електронски комуникации, вклучувајќи правила и заштитни мерки, и промовирањето на нивното усвојување меѓу сите земји-членки може да придонесе на некој начин да се подобри меѓународната соработка меѓу земјите. Дополнително, споделувањето на практични информации за точките за контакт/посветените единици во земјата кои можат да послужат како „привилегиран контакт" во случај на случаи на ТЛ, вклучувајќи ја ТЛ преку користење на ИКТ, може исто така, на еден начин, да ги олеснат процедурите.

2.3.2. Електронски докази

Додека предизвиците поврзани со добивањето електронски докази честопати се поврзани со МПП, природата и релевантноста на таквите докази поставуваат голем број дополнителни предизвици за кои вреди да се дискутира одделно.

Како што истакнаа австриските и британските власти, електронските докази може да го отежнат идентификувањето на точната локација на податоците. Одредувањето на

земјата под чија јурисдикција спаѓаат податоците можеби не е секогаш едноставно – со што изготвувањето на барањата за МПП станува предизвик. Португалските власти сметаат дека системот за добивање електронски докази од други земји не е „погоден за намената", и беше предложено дека можеби Вториот дополнителен протокол на конвенцијата од Будимпешта (Компјутерски криминал)[15] би можел да понуди подобрувања на сегашниот систем. Слично на тоа, грчките власти повикаа на заедничка правна рамка за брза размена на дигитални докази (напоменувајќи дека постои постоечка заедничка правна рамка за зачувување на доказите).

Покренато е прашање во врска со времето кога може законски да се поднесе барање за електронски докази. Според британските власти, „понекогаш органите на прогонот бараат пристап до содржината на комуникацијата пред да покажат соодветен степен на сомнеж, но предусловот за добивање таква помош треба да биде исполнет пред да се сподели содржината". Ова особено влијае на раните фази на истрагата. Слично на тоа, австриските власти го истакнаа предизвикот за „високиот праг кој треба да се достигне пред да се добијат податоците и бараната содржина од некои држави". Истите власти го покренаа прашањето за тоа каков тип на информации може да се побараат во текот на истрагата и на која правна основа (на пример, со или без судски налог). Австриските власти повикаа на „стандардизиран пристап до информациите за CID за време на истрагите за ТЛ" (на пр. барање информации за претплатниците од операторите на мобилната мрежа). Тие истакнаа дека „во некои земји [ова е] возможно само откако надлежниот суд ќе испрати Европски налог за истрага. Во Австрија, тоа е возможно без судски налог за време на истрагите на CID".

Како што веќе беше споменато претходно во овој извештај (Дел 2.1.6), правилата за должината на чување на податоците се означени како особено проблематични. Неколку земји изразија загриженост за непостоењето на хомогена регулатива за чување на податоците - со што се попречува размената на електронски докази. Некои земји можеби не поседуваат закони за чување на податоцитете.
На крај, неколку земји изразија загриженост за пристапот до електронските докази што се чуваат на компјутерските сервери лоцирани надвор од нивната јурисдикција. Искуствата во овој поглед варираат во зависност од земјата и компанијата која ги поседува податоците. Сепак, постојат многу докази за потешкотиите во идентификацијата на компанијата, лоцирањето, добивањето согласност за соработка и пренос на доказите. Земјите-членки ја изразија потребата од посеопфатна рамка која ќе го регулира чувањето и преносот на електронски докази, како и од заедничка правна рамка која би ги заменила тековните *ad hoc* билатерални работни договори помеѓу државата и приватната компанија која ги поседува податоците.

2.4. Предизвици за соработката со приватните компании

Студијата ги истражуваше предизвиците со кои се соочуваат земјите-членки кога работат со ИКТ компании и даватели на услуги на интернет, вклучително и поставувачите на содржини и социјални медиуми во справувањето со ТЛ. Иако некои од овие предизвици се преклопуваат со прашањата кои веќе беа дискутирани погоре, сепак е корисно да се понудат некои дополнителни размислувања за прашањата истакнати од земјите-членки. Во продолжение е резимето на овие предизвици:

[15] Втор дополнителен протокол на Конвенцијата за компјутерски криминал усвоен од Комитетот на министри на Советот на Европа - Вести (coe.int)

- Добивање навремен одговор од компаниите на давателите на интернет услуги и поставувачите на содржини. Пристапувањето до поставувачите на содржини преку писма испратени преку релевантни органи може да подразбира долг временски период на чекање – со што се појавува ризик дека содржината може да биде избришана до моментот кога ќе се постапи по барањето. Француските власти го истакнаа долгото време на одговор на барањата за мета податоци поврзани со сметките на сторителите; кога станува збор за податоците поврзани со содржините, честопати треба да има барање за МПП, што може да потрае неколку месеци пред да се реализира бидејќи компаниите често се наоѓаат надвор од јурисдикцијата на земјата барател (и Европската унија).

- Појаснување на законските барања под кои работат ИКТ компаниите и давателите на интернет услуги. Австриските власти изразија загриженост дека „меѓународните провајдери често наметнуваат формалистички, законски неоправдани барања на органите на прогонот како предуслови за обезбедување информации и предавање на кориснички податоци и содржина. Спроведувањето на налозите од обвинителството понекогаш е многу комплицирано". Според белгиските власти, одбивањата честопати не се соодветно мотивирани и објаснети. Властите на Босна и Херцеговина ги истакнаа потешкотиите во добивањето нелични податоци за време на истрагите (пред да биде издаден судски налог). Идентификацијата на самиот давател на интернет услуги може да создаде предизвици – како што истакнаа финските власти.

- Француските власти ги истакнаа прашањата поврзани со непризнавањето на обвинителството како независен правосуден орган при издавањето на формално барање за добивање на податоци. Дополнително прашање се барањата на компаниите да обзнанат голем број докази од истрагата што е во тек пред да може да се донесе одлука за предавање на податоците од страна на правниот оддел на компанијата.

- Белгиските власти забележаа недостаток на повратни информации и коментари во врска со операциите кои компаниите ги извршиле во рамките на својата организација, на пр. во врска со отстранувањето на определена содржина. Тие, исто така, ги истакнаа потешкотиите во комуникацијата со компаниите - честопати надополнети со честите промени во однос на лицата за контакт.

- Како што веќе беше истакнато, непостоењето на усогласено законодавство кога станува збор за зачувување на податоците и несоодветните законски одредби се означени од страна на земјите како клучни предизвици. Во Норвешка, на пример, на давателите на интернет услуги не им е дозволено да складираат информации за IP-адресите повеќе од 21 ден, и од нив не се бара да складираат информации за врската помеѓу претплатникот и IP адресата. Според норвешките власти, ова прави „потешкотии на полицијата во идентификувањето на осомничените за ТЛ преку користење на ИКТ". Овој проблем е поголем кога се работи со компании кои се формирани со цел обезбедување анонимни и шифрирани услуги.

- Молдавските власти го истакнаа непостоењето на назначени контакт точки во рамките на приватните компании кои работат со социјалните медиуми и другите мрежни апликации. Предложено е да се воспостави точка за контакт за секоја земја/област (во зависност од бројот на корисници). (Може да се размислува и за контакт точки одредени врз основа на јазикот што се зборува). Молдавските власти предложија воспоставувањето на контакт точки да биде задолжително за давателите на интернет

услуги, поставувачите на содржини и социјалните медиуми. Прашањето за јазичните вештини во компаниите беше истакнато од словачките власти, кои забележаа дека на големите компании кои работат во повеќе земји често им недостига персонал со јазични и правните вештини релевантни за секоја земја во која работат.

- На давателите на интернет услуги не им е секогаш јасно кои се националните агенции одговорни за одредени одлуки, на пр. симнување нелегална содржина. Словачките власти предложија да се воведе улогата на „доверлив означувач", односно да се идентификуваат конкретни агенции кои имаат задача да се поврзат со меѓународните провајдери со цел да отстрануваат содржини и да постапуваат според други законски одредби. Доверливиот означувач би имал отворен канал за комуникација со компаниите и би воспоставиле меѓусебна доверба.

Неколку земји, вклучувајќи ги Кипар, Ирска, Летонија, Луксембург, Малта, Холандија и Обединетото Кралство, посочија дека давателите на интернет услуги, поставувачите на содржини и компаниите за социјални медиуми генерално биле кооперативни кога станувало збор за прашања поврзани со ТЛ и сексуална експлоатација на деца. Сепак, британските власти укажаа на потребата да се оди подалеку и да се работи со онлајн компании „за да се **осмисли начин на кој би се оневозможила** трговијата со луѓе на нивните веб-страници и би се овозможила соработката со органите на прогонот за да се спречи појавата на трговија со луѓе".

Кипарските власти ја наведоа употребата на Сириус – платформа за олеснување на прекуграничниот пристап до електронските докази со кои располага Европол – како пример за добра практика. Таквата платформа им дава можност на органите на прогонот директно да комуницираат со приватни компании за зачувување и откривање на податоците. Ова го истакнаа и француските власти (Проект Е-Докази).

2.5. Доказ од невладини организации

Покрај доказите од земјите-членки, студијата побара од невладините организации кои обезбедуваат помош на жртвите да ги наведат предизвиците што ги забележуваат во контекст на ТЛ преку користење на технологијата.

2.5.1. Предизвици за идентификацијата и истрагата

Генерално, доказите од невладините организации се во согласност со предизвиците наведени од земјите-членки и она што беше претходно дискутирано во ова поглавје. Поконкретно, невладините организации го истакнаа следниот збир на фактори кои го попречуваат откривањето на ТЛ преку користење на технологијата со луѓе и истрагите кои произлегле во тој контекст:

- Недостаток на капацитет кај органите на прогонот, вклучувајќи недостаток на обука, хардвер и софтвер, како и ограничена употреба на специјални истражни техники. Некои невладини организации забележаа недостиг од специјализација кај полицијата и судството во однос на ТЛ поврзана со технологијата, како и недостаток на капацитет во рамките на големите податоци. Сепак, веб-скрејпинг алатките кои ги следи Хоуп нау [Hope Now] (Данска) во 2016-2018 год. постигнаа скромни резултати.

- Технолошкото опкружување кое брзо се менува, како и *начинот на делување* на сторителите. На професионалците им е тешко да останат во чекор со ТЛ преку користење на технологија, што ја попречува нивната способност навремено да ги идентификуваат случаите и да започнат истраги. Познавањето на техничкото опкружување и практиките честопати претставуваат паралелни процеси кои не се преклопуваат (на пр., органи на прогонот, приватни компании, невладини организации, академски кругови).

- Користење на приватни форуми, виртуелни простории за разговор (chatrooms) или шифрирани апликации за контакти помеѓу сторителите и жртвите. Ова го отежнува (а) откривањето на таквите контакти и (б) нивното обезбедување како доказ што треба да се користи на суд. Невладините организации предложија да вклучат информации/предупредувања за безбедното користење на приватните канали за комуникација.

- Потешкотии во демаскирањето на анонимните сторители за време на преносот во живо на онлајн експлоатација, како и потешкотии во собирањето докази за такви злоупотреби, освен ако не се направат слики од екранот (screenshots) од видео снимките.

- Професионалците сметаат дека е предизвик да утврдат дали лицето кое стои зад онлајн-профилот/огласот доброволно ги обезбедува услугите наведени врз основа на информациите што се јавно достапни (на пр., во случај на онлајн реклами за сексуални услуги). Тоа е затоа што сторителите можат да креираат и да ги уредуваат онлајн профилите во име на нивните жртви. Исто така, на сторителите им е лесно повторно да создаваат профили кога претходните ќе им бидат забранети.

- Правилата за заштита на податоците и приватноста може да ја попречат идентификацијата на жртвите, како и на трговците со луѓе. Правилата на GDPR ја ограничуваат употребата на технологијата за откривање на дигитални траги што ги оставиле и жртвите и сторителите (на социјалните медиуми, на интернет, но и во врска со финансиските сметки). Недостига сеопфатна анализа на дигиталните траги на жртвите, вклучувајќи, на пример, недвижен имот, банкарски сметки, трансакции преку банкомат, трансакции со кредитни картички и медицинска евиденција во насока на потпомагање на истрагите.

- Недостаток на интердисциплинарна технолошка соработка меѓу приватните компании, јавните агенции и невладините организации за целосно искористување на зголемениот број на податоци за ТЛ. Фондацијата Састејнабл Рескју (Sustainable Rescue Foundation) ги наведе следниве фактори кои ја попречуваат меѓусекторската соработката со податоци:
    - независните центри не успеваат да ги привлечат органите на прогонот или владата;
    - непостоењето на технолошка стратегија во националните акциски планови за ТЛ;
    - ИТ групите за спроведување на законот немаат капацитет или буџет да развијат, тестираат, имплементираат, обучуваат, ажурираат и одржуваат апликации за откривање на ТЛ навремено;

- потешкотии во споделувањето на податоците на жртвите;
- комерцијални интереси.

• Ограничени истраги за ТЛ од финансиските институции. Можностите за идентификација „Запознајте го вашиот клиент„ (KYC) не се искористуваат поради недостатокот на обука и свесност за ТЛ, како и поради сложеноста на системот за известување (квалитетот на она што алармира, исклучително големиот број на лажно позитивни, долгото време на одговор, итн.).

• Недостаток на инвестиции во способностите на вештачка интелигенција (ВИ) и употреба на машинско учење за операции, предвидување и превенција. Фондацијата Састејнабл Рескју (Sustainable Rescue Foundation) укажа на употребата на машинско учење во медицинскиот сектор како пример каде што „информациите се споделуваат помеѓу клиниките, болниците, лекарите и академската заедница без да се нарушува законодавството за приватност. Ова е направено преку користење на FAIR (Findable, Accessible, Interoperable, Reusable [достапно, пристапно, интероперабилно, повторно употребливо]) принципите за посета на податоци за совпаѓање на метаподатоци и Федерираното учење за длабока анализа од повеќе извори". Тие, исто така, забележаа дека „во моментов нема таква инвестиција или стратегија во организациите за ТЛ".

• Несподелувањето на податоци помеѓу различни субјекти на локално, регионално, национално или меѓународно ниво поради недостатокот на оперативни способности во рамките на органите на прогонот и ограничувањата поставени од страна на националните законодавства. Дополнително, податоците честопати се собираат во неструктурирана форма, што го отежнува споделувањето и понатамошната анализа на доказите.

• Невладините организации кои обезбедуваат директна поддршка на жртвите на ТЛ, преку онлајн платформи, консултации преку онлајн разговори (chats) и линии за помош, немаат капацитет, ресурси и технички алатки за редовно откривање на онлајн експлоатацијата преку користење на технологијата.

• Непостоење на свест за ризиците и потенцијалните последици поврзани со употребата на технологијата кај луѓето изложени на ризик од трговија со луѓе. Ова е особено клучно кај децата и младите. Општо земено, постои недостиг на свест кај пошироката јавност за ТЛ преку користење на технологијата, што резултира со слабо известување и пријавување.

2.5.2. Предизвици за соработка со органите на прогонот

Сите невладини организации пријавуваат некаков облик на соработка со органите на прогонот, вклучително и сигнализирање на случаи на ТЛ или обезбедување помош на жртвите по барање упатено од властите. Размислувајќи за нивната соработка со органите на прогонот, невладините организации ги истакнаа следните предизвици:

• Конфликтни цели или различни пристапи меѓу невладините организации и органите на прогонот, вклучително и одлуките за тоа дали некој случај треба дополнително да се истражува.

- Прашања поврзани со заштитата на податоците и приватноста.

- Недостаток на повратни информации за случаите што невладините организации ги пријавиле до властите.

- Недостаток на ресурси за поддршка на соработката меѓу органите на прогонот и невладините организации (ова беше истакнато и во врска со иновативните „теренски лаборатории" формирани во Холандија, во чиј одбор учествува и Фондацијата Састејнабл Рескју (Sustainable Rescue Foundation)).

- Кога станува збор за децата, постои недостиг на обука меѓу органите на прогонот за тоа како да им се пристапи на малолетните жртви и како да се убедат да соработуваат со истрагата. Ла Страда Молдавија истакна дека истрагите во кои се вклучени деца имаат дополнителна сложеност кога станува збор за ракувањето со доказите, бидејќи „децата обично се чувствуваат криви, виновни или се срамат за она што им се случило, не соработуваат, не сакаат родителите да дознаат што им се случило или други луѓе да ги видат нивните сексуално експлицитни видео материјали. Плашејќи се, многу од нив одбиваат да поднесат жалба", со што се спречуваат понатамошните истраги од страна на органите на прогонот.

2.6. Технолошки компании

Facebook посочи дека корисниците „ретко ја пријавуваат" содржината поврзана со трговијата со луѓе. Тие понатаму истакнаа дека недоволното пријавување може да се должи на голем број фактори, вклучувајќи: (а) жртвите на трговија со луѓе можеби немаат слобода да пријават или можеби не се свесни за нивните услови на експлоатација; (б) купувачите на услуги обезбедени од тргувано лице можеби не се свесни дека купуваат услуга од жртва на ТЛ или се демотивирани да пријават „бидејќи сакаат да ги искористат недозволените или значително поевтините услуги обезбедени преку експлоатација". Во други случаи, се забележува дека „за одредени форми на трговија со луѓе, како што е домашната послуга, бидејќи генерално може да биде општествено прифатен феномен во некои региони, случајните минувачи не сфаќаат дека можат или треба да ја пријават оваа содржина".

Што се однесува до предизвиците за соработка со органите на прогонот, IBM забележа дека има „голем број на пречки"; првенствено, тие ја истакнаа „загриженоста за законитоста на таквата соработка, особено во врска со загриженоста за приватноста на податоците и правната сложеност на повеќе јурисдикции". Тие повикаа на „појаснување за меѓународните правни дозволи за собирање и споделување податоци (со овластени тела за спроведување на законот)". Facebook посочи дека прекуграничната природа на човечката експлоатација „носи предизвици". На пример, тие забележаа дека сторителите може да се со седиште во друга земја од онаа каде што жртвите се тргувани и злоупотребувани: како таква, „повеќе јурисдикции може да бидат вклучени во истрагата за криминална мрежа. Координацијата меѓу органите на прогонот во рамките на ЕУ и надвор од неа додава дополнителна сложеност на напорите за борба против трговијата со луѓе„.

2.7. Дополнителни докази од анализата на состојбата

Покрај доказите обезбедени од земјите-членки, невладините организации и технолошките компании, студијата, исто така, спроведе и истражување преку анализа на достапната база на докази за предизвиците поврзани со откривањето, истрагата и гонењето на онлајн ТЛ преку користење на технологија.

Од особен интерес се доказите поврзани со предизвиците во **идентификацијата на огласите за работа поврзани со трговијата со луѓе**. Се сугерираше дека идентификувањето на реклами наместо жртви може да биде добар начин за искористување на технологијата: ова се навраќа на основните дела на CE (2007) и Фајн Тјуне Проектот (Fine Tune Project) (2011). Фајн Тјуне Проектот (Fine Tune Project) (2011) понуди прелиминарна листа на **црвени знаменца во контекст на трудовата експлоатација**. Тие вклучуваат: (а) нереално висока плата за неквалификувани работни места; (б) во описите на работните места недостигаат детали, вклучително и непостоење на опис на улогата на работното место, локацијата, местото на работа и дневното работно време; (в) непостоењето на адреса на компанијата или агенцијата за вработување; и (г) непостоењето на детали за контакт освен телефонски број или генеричка е-пошта. Сепак, доказите сугерираат дека идентификацијата на вистинските позитивни (т.е. реклами поврзани со трговија со луѓе) останува да биде голем предизвик. Неколку автори укажаа на **потешкотиите во избирањето** на вистинските огласи од оние поврзани со трговија со луѓе, и покрај напорите вложени во развивањето индикатори за потенцијален ризик (како и повторното толкување на општите индикатори на UNODC и ILO за да се прилагодат на онлајн контекстот: Ди Никола и др. 2017; Раетс и Јансенс 2018; Володко и др. 2019):

а. Во збир од 430 литвански огласи за работа преку Интернет, анализирани од Володко и сор. (2019), 98,4% содржеле барем еден показател за трговија со луѓе, што укажува на тоа дека таквите показатели често се вообичаени карактеристики на пазарите на труд со ниска квалификација. Некоја надеж, сепак, произлегува од наодот дека само 15% од огласите презентирале повеќе од пет индикатори, што укажува на тоа дека со дополнително усовршување и соодветни аналитички техники, некои стратегии за намалување на штетите би можеле ефикасно да се имплементираат.

б. Покрај рафинирањето на достапниот збир на црвени знаменца/индикатори (и нивното постојано ажурирање, што претставува дополнителен предизвик), се предлагаат пресметковни пристапи засновани на веб-скрејпинг, обработка на природен јазик, препознавање на ентитети и „ознаки" и техники за машинско учење поопшто како потенцијален пат напред (Володко и др. 2019 меѓу другите; исто така ОН Делта 8.7). Иако потенцијално ветува, овој пат отвора нови предизвици, вклучувајќи: (1) потребата да се воспостави „основна вистина" за моделите, што може да се направи само преку непосредна соработка помеѓу органите на прогонот и приватниот сектор; (2) потребата да се искористи знаењето на приватниот сектор, бидејќи органите на прогонот едвај ги имаат потребните вештини во рамките на своите организации; (3) потребата внимателно да се проценат етичките прашања поврзани со техниките за машинско учење од големи размери;и (4) потенцијалот за дискриминаторски практики како и прашањата за заштита на податоците и споделувањето на информациите.

Во некои случаи, огласите за работни места за модели, во секторот забава и – во некои земји – сексуални услуги во странство може да се користат за регрутирање поединци кои потоа се принудени на сексуална експлоатација. Предложени се голем број црвени знаменца за да се одделат огласите поврзани со трговија со луѓе од легитимните,

вклучително и огласите кои: (а) се лошо напишани и нејасни; (б) се премногу ветувачки; (в) се премногу широки; (г) не ја наведуваат земјата на дестинација (со наведување на „егзотични дестинации"); и (д) не го содржат целото име на лицето за контакт, агенција за регрутирање и/или компанија која би го вработила успешниот кандидат (Ди Никола и др. 2017). Сепак, прелиминарните обиди за проверка на отворено достапните докази користејќи ги овие критериуми, уште еднаш укажаа, на потешкотиите во одвојувањето на огласите поврзани со случаите на трговија со луѓе од грешките во бинарниот систем (false positive).

Откривањето на случаи на сексуална експлоатација врз основа на **онлајн огласи за сексуални услуги** е подеднаков предизвик, т.е. откривање на сексуалните услуги обезбедени од жртви на трговија со луѓе и нивно разликување од доброволно обезбедените сексуални услуги од поединци единствено врз основа на текстот и визуелните слики вклучени во огласот. Предложени се некои показатели за експлоатација, вклучително и несогласувања меѓу описите на профилите, сликите и локациите; таквите несовпаѓања може да се вкрстат и на повеќе веб-страници (Ди Никола и др. 2017). Се покажа дека телефонските броеви играат клучна улога, на пример во откривањето на присуството на ист телефонски број во реклами, веб-страници и објави кои им се припишуваат на различни лица (потенцијално црвено знаме). Се сугерираше дека препознавањето на лицето може да се користи како техника за да се забележат недоследности и црвени знаменца, слично со пристапот усвоен за детектирање на сексуални материјали во кои се вклучени малолетници (Раетс и Јансенс 2018).

Сепак, прелиминарните обиди за примена на гореспоменатите стратегии за откривање покажаа јасни предизвици. Во обидите да ги идентификуваат жртвите на сексуална трговија во САД преку огласи за придружба преку интернет, Ибанез и Ганзан (2014, 2016а и 2016б) користеа телефонски броеви и индикатори за движење, но не успеаа да обезбедат јаки резултати. Дополнително, некои од показателите наведени кај Ибанез и Ганзан од 2014 година се прилично збунувачки и можеби воопшто не укажуваат на трговија со луѓе; во некои случаи, тие може да укажат на спротивна ситуација.

3. Стратегии и добри практики

Откако разговаравме за предизвиците, студијата сега ги истражува стратегиите што земјите-членки ги развија за откривање и истражување на онлајн ТЛ преку користење на технологија, во насока на поттикнување на меѓународната соработка и идентификување и помош на жртвите. Потоа следи дискусија за доказите обезбедени од невладините организации и технолошките компании за истите прашања.

3.1. Откривање на случаи на ТЛ преку користење на ИКТ

3.1.1. Општи стратегии

Земјите укажаа дека спроведуваат различни стратегии за откривање случаи на онлајн ТЛ преку користење на ИКТ. Најчесто споменуваната стратегијата беше **следењето на интернет**, вклучувајќи ги форумите и, во некои случаи, TOR (Dark Web) мрежите. Ова често се комбинира со употребата на **разузнавачки информации од отворени извори (OSINT)**, што е многу вообичаена истражна стратегија која се состои од собирање податоци од социјалните медиуми и други јавно достапни онлајн извори за мрежата на контакти, условите на живот и финансиската состојба на едно лице. OSINT може да се користи „проактивно", на пр., за откривање на потенцијални случаи на ТЛ, за идентификување на потенцијалните сторители и жртви или за добивање нови информации. Некои земји формираа **„компјутерски-патроли" со специјализирани службеници** задолжени за спроведување на OSINT истраги на Интернет. Некои јурисдикции дозволуваат тајни онлајн истраги (компјутерска инфилтрација). Во Холандија, специјализирани истражувачи со **„дигитално знаење"** може да се ангажираат во истрагите за трговија со луѓе за да се соберат онлајн докази за ТЛ. Финските власти го истакнаа неодамнешното основање на пододделение за справување со онлајн ТЛ во рамките на Националниот истражен тим (тие исто така пријавија присуство на подружница за онлајн разузнавање што работи на мрежата, вклучувајќи го Dark Web).

Поврзани со OSINT истрагите, земјите ја наведоа употребата на **техники за анализа на социјалните мрежи** за да се разбере и реконструира мрежата на контакти на сторителот и/или жртвата. На пример, ако жртвата А е поврзана со регрутерот Б, тогаш може да се проценат сите контакти на регрутерот Б за да се идентификуваат потенцијалните жртви. **Поврзаните информации** се клучни и сè повеќе се користат од полициските сили преку таканаречената „анализа на врски" или пософистицирани техники за „анализа на социјалните мрежи".

Дополнителните **проактивни стратегии** вклучуваат употреба на технолошки алатки за пребарување на онлајн докази (на пр. веб-роботи, видете и во продолжение) и стратешки истраги за *начинот на делување* на ИКТ на сторителите во случаи на ТЛ. Генерирањето – и ажурирањето – на таквото стратешко (пошироко) знаење за феноменот може да обезбеди информации за сеопфатниот пристап, како и за конкретните насочени истраги. Меѓутоа, не сите земји-членки посочија дека користат „стратегии". Неколку земји-членки експресно укажаа дека нивните истраги за ТЛ преку користење на ИКТ, остануваат „реактивни".

Властите известија дека воспоставиле директен контакт со давателите на онлајн услуги за да се идентификуваат случаите на ТЛ преку користење на ИКТ. Во земјите каде што рекламирањето онлајн сексуални услуги е легално, властите може „да извршат насочено филтрирање на телефонски броеви и [анализа] на кориснички податоци поврзани со [претпоставени] сторители" (поднесок од Унгарија). Кантоналните полициски сили во Швајцарија вршат „насочени проверки" на онлајн огласи за сексуални услуги со цел откривање потенцијални жртви на ТЛ.
Алатките за веб-скрејпинг специјално развиени за извлекување информации од веб-страници се користат од страна на некои агенции за спроведување на законот во Обединетото Кралство за да се идентификуваат ризиците и ранливостите на веб-страниците со содржини за возрасни (ASW). Силите на британската полиција користат веб-роботи за пребарувања на ASW за да соберат податоци кои потоа се користат за анализа на активноста на ASW и потенцијално ги претворат овие податоци во активна разузнавачка информација.

Неколку земји го споменаа расположливиот **механизам кој корисниците на интернет може да го искористат за да пријавуваат содржина и веб-страници** за кои се сомневаат дека се поврзани со нелегални активности, вклучително и сексуална и трудова експлоатација (видете во продолжение неколку примери).

3.1.2. Стратегии кои се однесуваат на конкретна земја

Во насока на понатамошно истражување на различните стратегии развиени од страна на земјите за справување и спротивставување на злоупотребата на интернетот, вклучително и онлајн огласите за работа, во контекст на трговијата со луѓе преку користење на технологијата, сега нудиме краток преглед на механизмите и иницијативите кои се однесуваат на конкретна земја. Ваквите стратегии треба да се читаат заедно со добрите практики разгледувани во следниот дел, како и дискусијата за домашните правни рамки поврзани со идентификацијата и отстранувањето на онлајн содржините поврзани со трговијата со луѓе вклучени во веб-анексот.

Во Албанија постои **механизам на дозволи** поврзани со онлајн огласите за работа, а тие се издаваат/ се контролирани од институции (не се наведени во поднесокот).

Австриските власти ги интензивираа проактивните пребарувања на различни онлајн платформи од избувнувањето на Ковид-19 за да ги идентификуваат жртвите и сторителите вклучени во ТЛ користејќи **специјални софтверски технологии** (на пр. веб-роботи), **службеници специјализирани за пребарување на разузнавачки информации преку користење на отворени извори** (OSINT), како и **тајни агенти** (онлајн тајни истраги). Активностите се спроведуваат заеднички од страна на истражителите на трговија со луѓе и службениците специјализирани за ИТ. Се верува дека овој модел може да понуди образец за идни истраги.

Белгиските власти посочија дека сегашниот „аболициски модел" усвоен во однос на проституцијата го прави склучувањето договори со веб-страниците кои објавуваат реклами за сексуални услуги правно невозможно. На него се гледа како на „ограничување" на сегашното законодавство. Невладината организација „Фокус врз детето" [Child Focus] во моментов развива кампања за подигање на свеста на клиентите кои користат веб-страници на кои се прикачуваат/хостираат реклами за сексуални услуги за да ги информираат за ризикот дека може да наидат на малолетно лице. Оваа кампања се спроведува во партнерство со засегнатите веб-страници.

Хрватските власти пријавија дека вршат проверки на **профилите на социјалните мрежи** на поединци поврзани со специфични криминални истраги, на пр. сексуална злоупотреба и сексуална експлоатација на деца, за да се идентификуваат потенцијалните жртви и регрутери. Ваквите проверки ги вршат специјализирани службеници за компјутерски криминал.

Во Кипар, постојат кампањи за подигање на свеста организирани од Одделот за компјутерски криминал (CCD) наменети за учениците и нивните родители како дел од Националната стратегија за подобар интернет за децата. Од 2014 година, CCD води и платформа за известување за компјутерски криминал (www.cyberalert.cy).

Во Естонија, граѓаните можат да контактираат со „**веб-позорниците**" со цел да пријават содржина на социјалните мрежи потенцијално поврзани со нелегални активности, вклучително и ТЛ.

Францускиот закон им дозволува на истражителите **компјутерско инфилтрирање во криминалните мрежи**. Органите на прогонот вработуваат истражители за компјутерско патролирање на интернет за да **откријат огласи** и да **идентификуваат криминални мрежи**. Исто така, се вршат насочени операции за надзор на одредени интернет форуми, користејќи тајни истражни техники онаму каде што е потребно. Истражувачите исто така користат интернет огласи за да ги проверат локациските податоци собрани преку други извори со намера да ги идентификуваат местата што се користат за ТЛ. Информациите собрани од различни извори се систематизираат и се користат за **реконструкција на криминалните мрежи, односно односите меѓу местата, престапниците и жртвите**. Покрај тоа, француските органи на прогонот работат на воспоставување **протоколи за соработка** со компаниите на социјалните мрежи и онлајн приватните платформи за изнајмување за да се поттикне обезбедувањето информации. Бидејќи поставувачите на онлајн содржини во некои случаи може да бидат преоптоварени од обемот на барања за пренос на информации и барања за докази, властите предложија **да се осмислат подиректни – и поедноставени – процедури кои ќе ја поткрепат соработката** помеѓу поставувачите на содржината и органите на прогонот. На пример, „Wannonce", француска страница што се користи за реклами поврзани со малолетничка проституција, испраќа до органите на прогонот линк што овозможува директно пребарување во нивната база на податоци по обезбедување на адреса на е-пошта. На крајот, член 6(I)(7) од Законот бр. 2004-575 од 21 јуни 2004 година за „Доверба во дигиталната економија" (LCEN) бара од давателите на интернет пристап и поставувачите на содржини на веб-страниците да помогнат во борбата против ширењето на материјали поврзани со конкретни повреди на законот, вклучувајќи и ТЛ. Од нив се бара да постават лесно достапен и видлив механизам кој ќе му овозможи на секое лице да **означува сомнителен материјал**. Компаниите исто така се обврзани навремено да ги информираат националните власти за какви било недозволени активности што им се пријавени и кои се извршени од примателите на нивните услуги. Граѓаните можат да пријават нелегална содржина на интернет до полицијата и жандармеријата преку веб-страница (www.internet-signalement.gouv.fr). Пријавената содржина ја испитува PHAROS (*Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements*), која е специјализирана полициска единица.

Во Финска, финската телефонска линија за заштитата на децата (Nettivihje) нуди начин за пријавување на онлајн материјали за сексуална злоупотреба на деца и трговија со деца. Nettivihje тесно соработува со Националното биро за истраги и нивниот тим

специјализиран за сексуални злосторства. Финската полиција има и можност за онлајн дојави за пријавување на сомнителни активности на интернет, вклучувајќи материјали потенцијално поврзани со сексуални кривични дела врз деца. Овој шаблон потенцијално може да се прошири надвор од сексуалната експлоатација на деца.

Во Германија, полицијата почна (мај 2020) да користи **алатка за автоматско пребарување** за анализирање на голем број податоци објавени на веб-страниците на огласите за возрасни. Алатката за пребарување ги структурира податоците со цел да помогне во извлекувањето на релевантни информации. Ова се прави паралелно со употребата на специфични индикатори. Властите сметаат дека употребата на оваа автоматизирана алатка е „многу корисна„.

Грчките власти го споменаа **следењето на веб-страниците и форумите кои рекламираат огласи за работа** или услуги за откривање на онлајн случаи на ТЛ. Ова се прави преку тесна соработка помеѓу Единиците за борба против трговија со луѓе на грчката полиција и Одделот за компјутерски криминал. Дополнително, Одделот за компјутерски криминал на грчката полиција разви активности за подигање на свеста и едукативни активности кои се фокусираат на одговорното користење на новите технологии и онлајн ризиците, на пример, „Семинарите за Денот на безбедно сурфање" и веб-страницата и апликацијата „Cyberkid", информирањето на учениците, родителите и наставниците за насилството на интернет и ризиците со кои што тие може да се соочат на веб-страниците на социјалните мрежи. НВО „Насмевката на детето" одржува редовни настани на Денот за безбеден интернет (9 февруари).

Во Исланд, Метрополитенската полиција во Рејкјавик ги одржува таканаречените „**интернет недели**", за време на кои тие ги чешлаат популарните веб-страници кои рекламираат сексуални услуги, барајќи случаи на ТЛ. Во случај на сомнителни активности, полицијата ќе побара судска наредба за прислушување на телефонските броеви наведени во огласите и ќе започне истрага.

Во Ирска, Единицата за координација на трговијата со луѓе и Единицата за истраги на An Garda Síochána (ирската полиција) се поврзуваат со различни социјални медиуми и компании за регрутирање со цел да ја подигнат свеста за потенцијалните објави кои имаат за цел регрутирање за ТЛ. Ирските и некои меѓународни ИКТ компании обично соработуваат кога An Garda Síochána бара да се отстранат онлајн содржините што се оценети како нелегални.

Во Латвија постои официјална веб-страница за огласи за вработување што ги води Државната агенција за вработување. Веб-страницата се обидува да спречи случаи на трудова експлоатација со **нудење безбеден простор за огласи за работа**.

Во Република Молдавија, во моментов нема конкретен автоматизиран механизам за идентификација на огласи и онлајн содржини кои потенцијално се поврзани со ТЛ, и властите во моментов работат со Холандија на набавка на веб-робот изработен од страна на холандските органи на прогонот.

Во Холандија, **полицијата може да постави онлајн лажни профили** (*lokprofiel*) за да ги идентификува – а потоа и да ги истражи – случаите и сторителите на ТЛ. Дополнително, Министерството за правда и безбедност во моментов ја истражува улогата на технологијата во сите фази на ТЛ преку стручни состаноци и истражувања спроведени во соработка со Центарот против детска експлоатација и ТЛ (ЦКМ).

Во Норвешка, Центарот за компјутерски криминал моментално развива **база на податоци за онлајн сексуални реклами** објавени на локална веб-страница. Ваквите информации ќе ја дадат основата за понатамошна анализа.

Во Словенија, во 2005 година беше формиран Центар за побезбеден интернет за да се подигне свеста и да се помогне во откривањето на нелегални онлајн содржини. Тој нуди три главни услуги: (а) **центар за подигање на свеста** за одговорно користење на интернетот и новите технологии (Safe.si) чија цел е да им обезбеди на децата, тинејџерите, родителите, наставниците и социјалните работници онлајн/офлајн активности, образование, работилници, содржини, кампањи за подигање на свеста; (б) услуга за помош на децата, младите и родителите (позната и како „Том Телефон") со професионални советници кои нудат совети за безбедност на интернет, исто така, преку **онлајн соби за разговор (chatrooms)**; (в) анонимно онлајн известување за нелегална онлајн содржина.

Во Шпанија, властите користат **следење на социјалните мрежи** преку компјутерски патроли фокусирани на откривање на жртви на трговија со луѓе. Патролите се спроведуваат од страна на Централната истражна единица на граѓанската организација Гардија специјализирана за трговија со луѓе и тие беа интензивирани за време на пандемијата со Ковид. Policía National, исто така, неодамна создаде истражна група специјализирана за случаи на трговија со луѓе на интернет (Оперативна група VI за компјутерска трговија со Централната бригада за трговија со луѓе на Policía Nacional).

Во Шведска, полицијата врши **редовен надзор на веб-страниците** кои рекламираат активности во врска со проституција за идентификување на местото и времето на таквите активности (според шведскиот закон, сите набавени сексуални услуги се нелегални).

Во Швајцарија, некои кантонални полициски сили користат **тајни истраги за да ги проверат огласите** на веб-страниците за возрасни, како и лицата вклучени за откривање на случаи на трговија со луѓе.

Во Обединетото Кралство, Службата за прашања поврзани со злоупотребата при посредувањето при вработување и кршењето на човековите права (Gangmasters and Labour Abuse Authority) заедно со Crimestoppers го користеа Facebook за да ги информираат барателите на работа за лажно огласување за работа на социјалните мрежи. Тимот **креираше огласи за вработување на Facebook** кои обезбедуваа хиперврска (hyperlink) до веб-страницата на Crimestoppers, која пак даваше информации за индикаторите за ризик при барање на вработувања во градежната индустрија. Кампањата беше насочена кон романските мажи на возраст од 18-34 години и допре до над 900.000 луѓе. Имаше зголемување од 13% во пријавите за ТЛ и 400% зголемување во пријавите за ТЛ кои се однесуваат на романски жртви. Како дел од повеќеагенцискиот пристап (Проект AIDANT) кој ги обединува Националната агенција за криминал, граничните сили, имиграциските служби, управата за јавни приходи и царината на Нејзиното височество, Службата за прашања поврзани со злоупотребата при посредувањето при вработувањето и кршењето на човековите права како и полициските сили, властите изготвуваат и тестираат нови методологии за пријави од индустријата. Единицата за трговија со луѓе за модерно ропство на Националната агенција за криминал (MSHTU) работи на подигнување на стандардите на веб-страниците на услугите за возрасни (ASW) преку подобрување на начинот на кој компаниите ја идентификуваат ТЛ и експлоатацијата на нивните платформи и ги известуваат органите на прогонот. Полициските сили исто така користат

автоматизирани процедури за истражување на отворени извори за собирање информации од огласи на веб страниците на услуги за возрасни (ASW). Ставот што го заседоа британските власти е дека затворањето на ASW е ризично, бидејќи веројатно нема да доведе до елиминација на побарувачката, наместо тоа ќе резултира со преместување на огласите на други платформи, на штета на благосостојбата на жртвите на трговија со луѓе и на благосостојбата на сексуалните работници/чки. Дополнително, апликацијата Farm Work Welfare е развиена со цел да се допре до сезонските работници и работодавачите во секторите за земјоделие и производство на храна и претставува шема преку која може да се слушне гласот на работниците (SAFERjobs, www.safer-jobs.com) за да се овозможат транспарентни синџири на снабдување и да се собираат разузнавачки информации за злоупотребите на пазарот на трудот. Кај организациите за кои е утврдено дека не се усогласени, се применуваат постапки за примена на законот и се упатуваат пораки до нивниот краен работодавец за подигнување на свеста на работодавецот, а потенцијално може да се изгуби и бизнисот (стратегија „именувај и посрами").

Во Украина властите почнаа да ги блокираат онлајн каналите на Telegram кои шират информации за сексуална експлоатација.

3.2. Истрага на случаи на трговија со луѓе преку користење на ИКТ

Овој дел ги истражува стратегиите и добрите практики смислени од земјите-членки во насока на зголемување на ефективноста на истрагите на ТЛ преку користење на ИКТ (таквите стратегии и добри практики треба да се читаат заедно со стратегиите поврзани со идентификацијата на случаите дискутирани погоре, бидејќи идентификацијата и истрагата можат да бидат тесно поврзани).

Неколку земји ја истакнаа важноста од обезбедување на **континуирана обука и развојни активности засновани на најдобрите локални и глобални практики** на службениците за спроведување на законот. Формирањето и обуката на специјализираните единици за трговија со луѓе преку користење на ИКТ беа споменати како важна стратегија. Генерално, **инвестирањето во човечки капитал** од многу земји-членки се смета за неопходно исто како и инвестирањето во технолошката опрема. Помеѓу специјализираните профили што земјите ги идентификуваа како клучни за ефективна истрага на ТЛ преку користење на ИКТ, има службеници специјализирани за „нови технологии", „оперативни криминалистички аналитичари", за „тајни истраги" и „истражувачи на отворени извори - OSINT" (називите се оние што се наведени во францускиот поднесок, но други земји посочија на слични профили). Како што забележаа грчките власти, треба да се обезбеди обука не само за тоа како да се користат технолошките алатки, туку и за „нивната етичка употреба со почитување на човековите права и заштита на податоците" (повеќе за обуката има во следното поглавје).

Како во моментов се спроведува обуката варира од земја до земја. Едниот модел е моделот каде на националните центри за компјутерски криминал, онаму каде што се формирани, им се доверува задачата за развивање на алатки и техники и знаење за нив, а потоа тие имаат задача да го *дисеминираат* ова знаење меѓу полициските единици и/или да понудат помош преку интегрирање на други специјализирани единици, на пр. единици за трговија со луѓе. Јасно е дека знаењето за „напредните истраги и анализи со компјутерска технологија, вклучително и безбедноста на трагите

и доказите од дигиталните уреди, ИКТ системите, интернет провајдерите" е клучна предност (норвешки поднесок). Неколку земји (но не сите) посочија дека поседуваат единица која е посветена на справувањето со криминалот со голема технолошка компонента, на пр., Единици/Центри за компјутерски криминал или Одделенија за високотехнолошки криминал. Други полициски единици, на пр. специјализираните единици за трговија со луѓе, може да побараат поддршка од таквите единици.

Неколку земји ја истакнаа важноста од вклучување на специјализирани истражители со „**дигитално знаење**" во истрагите за трговија со луѓе. Таквите службеници може да се ангажираат за да пребаруваат онлајн индиции за ТЛ. Според еден оперативен модел предложен од француските власти потребно е присуство на персонал специјално обучен за спроведување истраги на интернет и на социјалните мрежи, кој би бил вклопен во секоја единица специјализирана за борба против ТЛ. Од суштинско значење е можноста овој персонал да биде составен од полициски службеници кои дале заклетва или полициски службеници кои не дале заклетва, на пр. преку создавање на групи за техничка поддршка на „традиционалните" истражители. Оваа идеја **се оддалечува од традиционалниот полициски модел** кој се потпира исклучиво на полициските службеници кои дале заклетва и го усвојува принципот кој веќе го следат некои полициски сили, односно ангажирање на полициски службеници кои не дале заклетва, а кои работат во полицијата во потехнички улоги (на пример, аналитичари).

Покрај обезбедувањето обука за службениците, бугарските власти ја истакнаа важноста од ангажирањето на IT експерти во истрагите за трговија со луѓе, како и зајакнатата соработка со приватниот сектор. Ова го повторија и кипарските власти кои го посочија создавањето тимови од истражители и аналитичари специјализирани за трговија со луѓе и компјутерски криминал како потенцијална добра практика. Вредноста на **меѓуагенциската истражна работа** со вклучување и соработка на широк спектар на специјализиран персонал беше истакната и во поднесокот од Швајцарија каде, на пример, беа формирани заеднички тимови и овој модел може да се прошири на ТЛ преку користење на ИКТ.

Германските власти укажаа на важноста од подобрување на **размената на знаење** меѓу институциите и **зајакнување на ИКТ вештините** меѓу полициските службеници. Според шпанските власти, од клучно значење е и „да се зголеми свеста за криминалот на интернет" и „од самиот почеток да се вклучат специјалисти за технолошки криминал" во истрагите за трговија со луѓе. Неколку земји посочија дека обуката за тоа како да се надгледуваат и координираат истрагите за трговија со луѓе со голема технолошка компонента, исто така, треба да се обезбеди и/или да се зајакне меѓу обвинителите, бидејќи електронските докази стануваат сè посуштински во случаите за трговија со луѓе.

Постои прилично распространет консензус во врска со **важноста поврзана со набавката и пристапот до специјализиран софтвер** за подобрување на истрагите за ТЛ преку користење на ИКТ. Во Холандија, властите создадоа веб-робот алатка за собирање и систематизирање на големи количини на податоци. Во моментов, холандските органи на прогонот ја испробуваат оваа алатката во судска постапка за ТЛ за да изградат судска рамка. Според холандските власти, веб-роботот „се фокусира на огласи со ризик од сексуална експлоатација и моментално се тестира"; властите исто така работат на утврдување дали „постои доволна правна основа и практична употребливост за нејзина употреба во формални истраги".

Слично на тоа, **важноста на големите податоци (big data), како и подобрувањето на способностите на големите податоци**, беше истакната од

неколку други земји, вклучувајќи ги Естонија, Република Молдавија и Грција. Развивањето или набавувањето на алатки кои можат автоматски да преземаат веб-страници и други видови електронски информации се смета за клучно во спроведувањето на истрагите. На пример, во 2020 година Бирото за криминалистичка полиција на Литванија доби лиценца за софтвер за собирање информации од онлајн извори и лиценца за специјализиран софтвер за анализа на таквите информации. Сепак, не е важна само можноста за собирање податоци. Од суштинско значење е и способноста на таквите алатки за **складирање** на **такви информации на безбеден начин** за да можат *самоуверено* да се користат „како доказ на суд или како разузнавачки информации за да се изгради случај" (поднесок од Шведска).

Два други типа на алатки се сметаат за клучни во спроведувањето на ефективни истраги за ТЛ преку користење на ИКТ. Прво, алатките за преземање информации од мобилни телефони кога лозинката не е достапна (поднесок од Шведска). Второ, развојот и воведувањето на алатки кои овозможуваат дешифрирање на разговорите преку апликациите за лична комуникација. Шведските власти истакнаа дека таквите алатки треба да можат и да ги дешифрираат разговорите во реално време. Во Австрија, Службата за криминалистичко разузнавање развива специфичен софтвер за испитување на мобилни телефони за да се идентификуваат жртвите на ТЛ.

Швајцарските власти ја истакнаа потребата од зголемување на **тајните истраги** - оттука и инвестирањето во обуката на специјализираните службеници. Слично на тоа, тие ја истакнаа важноста од специјално обучени полициски службеници во областа на ТЛ. Тајните истраги норвешките власти ги сметаат за „најефикасни истраги", особено кога се комбинираат со собирање на големи податоци од веб-пребарувањата на OSINT, како и со трансферите/протокот на пари. Во Холандија, полицијата моментално ја тестира употребата на „лажни профили" за идентификување на трговците со луѓе во нивниот обид да регрутираат потенцијални жртви. Слично на тоа, шпанските власти ја истакнаа потребата од прилагодување на домашното законодавство во насока на целосно искористување на можностите што ги даваат тајните онлајн истраги.

Британските власти проценуваат дека **раслојувањето на информациите** е од клучно значење за да се истражи ТЛ преку користење на ИКТ. Збогатувањето на разузнавачката слика преку комбинација на истражување на отворените извори и системското истражување на органите на прогонот се смета за добра практика. Тие, исто така, предложија да се напуштат едноставните листи на индикатори. На пример, британските власти истакнаа дека во контекст на сексуалната експлоатација, истражителите вообичаено следат процес од три чекори, наспроти пропишаната листа на индикатори, за идентификување на огласите со висок ризик за ASW. Според таквиот процес, ризикот се идентификува онаму каде што огласите за ASW се дел од мрежа, каде што има индикатори за принуда и контрола и каде што автентичноста на компјутерската сметка на огласот е сомнителна.

Неколку земји ја истакнаа важноста од унапредување на прекуграничната соработка и обезбедување брза размена на податоци на оперативно ниво. Австриските власти ја посочија **меѓусебната размена на службеници** со земјите на потекло на жртвите како пример за добра практика. Генерално, зајакнатата меѓународна соработка со истражните органи во земјите на потекло се смета за добра практика.

Финските власти ја истакнаа важноста од спроведување на **стратешка анализа** во насока на генерирање на знаење во врска со последните трендови и ажурираните информации за *начинот на делување* на сторителите (вклучувајќи ја технологијата и

веб-страниците што ги користат сторителите). Овој став е поддржан од полските власти. Препознаен е фактот дека постојаното следење на феноменот е тешка активност која одзема време, со што го зголемува притисокот на (често) веќе оптоварените полициски ресурси. Сепак, на пристапот до ажурираната база на знаење, вклучувајќи ги техниките за регрутирање што ги користат сторителите, се смета за многу ефикасна алатка во спречувањето и борбата против ТЛ. Оваа активност за собирање на знаењата треба да има меѓународна димензија - идеално со одреден степен на меѓународна координација. Врз основа на овие споделени докази, поединечните земји може да започнат таргетирани полициски операции и да склучат договори за соработка онаму каде што тоа е потребно.

Неколку земји забележаа дека истрагите би биле олеснети доколку се овозможи **поедноставно меѓународно чување на доказите и пристап до нив**. Ова потенцијално се претвора во олеснети и рационализирани процедури за процесирање на прашања испратени до единиците одговорни за зачувување на податоците во странски земји (барања за чување податоци), како и преку олеснување на постапката во врска со барањата за меѓусебна правна помош. Како што истакнаа полските власти, меѓу другото, „приватниот сектор најчесто поседува информации од интерес за органите на прогонот (на пример, податоци за претплатниците)" и „ефикасното и брзо стекнување на таквите податоци од страна на полицијата е важно за позитивно решавање на истрагата".

3.3. Унапредување на меѓународната соработка

Размислувајќи за нивното искуство во справувањето со прекугранични случаи на ТЛ преку користење на ИКТ, земјите ги идентификуваа следните „добри принципи" за поттикнување на меѓународната соработка:

- Искористување на ресурсите достапни во рамките на агенциите како што се Европол и Европравда (Eurojust), како и формирање на заеднички истражни тимови.

- Воспоставување контакт со други држави во **раната фаза** од истрагата. Ова бара организациски мерки за олеснување на таквите брзи интеракции (на пр., преку јасни процедури и јасни контакт точки).

- Здобивање со многу добро **разбирање на правниот контекст и можностите** за соработка со засегнатата земја или земји за да се избегнат блокадите и да се обезбеди навремена соработка.

- Создавање **координативни состаноци** за размена на информации и докази што е можно побрзо и поекспресно, за да се воспостави заедничка стратегија од *самиот почеток*; да се олесни извршувањето на барањата за меѓународна правна помош и да се отстранат пречките поврзани со прифатливоста на доказите во дадена земја.

- Здобивање со **заедничко разбирање** на стандардизираните пристапи и обезбедување на **транснационална интероперабилност** на органите на прогонот преку транснационални сесии за обука.

Покрај овие општи принципи, постојат и голем број конкретни примери на добри практики идентификувани од земјите-членки. Ваквите практики може да се групираат во шесте главни категории дадени подолу.

Заеднички истражни тимови. Пример за добра практика во меѓународната правна соработка пријавена од бугарските власти е заедничкиот истражен тим формиран во 2019 година со Франција – и помошта од Европравда – насочена кон трговијата со луѓе, сексуалната злоупотреба на деца и трговијата со бремени жени за продажба на нивните деца. ЗИТ спроведоа голем број истражни активности во Бугарија, Франција, Германија и Грција. Генерално, неколку поднесоци ги посочија заедничките истражни тимови како пример за добра практика. Како што објасниј авструските власти, тие овозможуваат „помалку бирократска размена на информации кога станува збор за транснационални истраги, како и поделба на надлежностите меѓу правосудните органи кои учествуваат во истрагата".

Соработка меѓу трудовите инспекторати. Извршната агенција на бугарскиот Генерален инспекторат за труд ја истакна важноста од координирани инспекции и истраги кои се спроведуваат заеднички низ земјите кога станува збор за сложени прекугранични случаи кои вклучуваат потенцијална трудова експлоатација меѓу упатените работници од земјите[16]. На заедничките акции спроведени помеѓу трудовите инспекторати на Бугарија и Франција (проект *Eurodétachement*) се гледа како на примери на добра практика. Акциите вклучуваа заеднички инспекции на компаниите за привремени вработувања кои испраќаат работници во Франција, како и информативни состаноци за бугарските работници испратени во странство или директно вработени во Франција (најмногу во земјоделието). Одржани се и онлајн состаноци за размена на информации и добри практики за прекугранични инспекции. Овој пример е особено интересен, бидејќи ја покажува **важноста на соработка на други органи**, покрај полициската соработк, во справувањето со ТЛ. Сепак, ваквата соработка добива помалку внимание во информациите за политиките (policy briefs). Земјите-членки треба да ја разгледаат можноста за подобрување на соработката меѓу другите органи покрај полицијата – особено во контекст на ТЛ за трудова експлоатација.

Стратешка соработка. Германските власти ја истакнаа важноста на стратешката соработка, на пример преку ОА 7.1 на проектот ЕМПАКТ (*Европска мултидисциплинарна платформа против криминални закани*) на Европол. Овој проект се фокусира на онлајн трговијата со луѓе. Во рамките на ЕМПАКТ проектот, Холандија и Обединетото Кралство развиваат визуелна претстава за ТЛ овозможено со помош на злоупотреба на ИКТ.

ЕУ/меѓународно координирани компјутерски патролни акции. Холандските власти и португалските власти ги посочија Деновите за заедничко дејствување ЕМПАКТ/координираните компјутерски патролни акции на Интернет/Darknet како пример за добра практика во меѓународната соработка. Разузнавачките податоци најпрво се собираат во одделните земји, а потоа се започнуваат координирани акции.

Искористување на мрежата на службеници за врски. Полските и француските власти ја истакнаа важноста на акредитираните службеници за врски во олеснувањето на размената на информации. Француските власти посочија случај во кој поддршката добиена од романските службеници за врски со седиште во Франција овозможи истовремено да се извршат апсења во двете земји. На овој начин, властите можеа да ја таргетираат целата транснационална криминална мрежа, вклучително и нејзиниот шеф

[16] Според Директивата 96/71/ЕЗ и Информацискиот систем за внатрешен пазар (ИМИ).

кој ги водеше операциите во Франција, а живееше во Романија. Норвешките власти ја истакнаа придобивката од постоењето на контакт точка на Филипините за споделување информации за тековните случаи, со што се избегнува дуплицирање на истрагите и конфликтите. Преку контакт точката, норвешките и филипинските власти можеа да споделат искуства, трендови и студии, вклучително и за онлајн ТЛ.

3.4. Идентификација на жртвите и помош

Овој дел се фокусира на начините на кои земјите-членки ги користат технолошките алатки во врска со: (а) идентификација на жртвите; (б) помош и (в) споделување на информации меѓу ризичните заедници.

3.4.1. Технолошки алатки за идентификација на жртвите на ТЛ

Употребата на технолошки алатки кои се потпираат на **препознавање на лица** се чини дека е широко користена во случајот на сексуална експлоатација на деца (CSE), на пр. за проверка на сликите со постоечките меѓународни бази на податоци како што е базата на податоци NCMEC (Национален центар за исчезнати и експлоатирани деца, САД) или ICSE на Интерпол[17]. Сепак, се чини дека употребата на таквите алатки е поограничена надвор од оваа област. Финските власти посочија дека ги тестираат алатките за препознавање лица за да ги идентификуваат жртвите на сексуална експлоатација на интернет, особено во контекст на веб-камерите. Тие, исто така, сугерираа дека употребата на такви алатки може да се прошири со цел да опфати поширок опсег на ситуации на трговија со луѓе. Летонските власти спомнаа употреба на специјализиран софтвер за препознавање слики (PhotoDNA, Clear View) од случај до случај. Во Унгарија, наменска употреба на алатки за препознавање на лица може да се користат за време на истрагата за да се идентификуваат потенцијалните жртви. Меѓу неколкуте земји кои посочија дека користат технолошки алатки, Германија неодамна воведе алатка за скенирање на веб-страници со огласи за сексуални услуги во голем број на податоци за да помогне во идентификацијата на жртвите на ТЛ. Австриските истражители имаат пристап до **веб-роботи** и (под одредени услови) алатки за препознавање на лица. Во Обединетото Кралство, властите користат алатки за пребарување на веб-страниците (web-scraping) во насока на собирање и анализирање на податоците од веб-страниците со содржини за возрасни (ASW) со цел да им помогнат во идентификацијата на жртвите на ТЛ.

Во однос на употребата на **индикаторите за ТЛ** („**црвени знаменца**"), неколку земји изјавија дека *се* потпираат на индикаторите за идентификација на случаите на ТЛ; сепак, ова се „општи" показатели за трговија со луѓе и не се однесуваат конкретно на ТЛ преку користење на ИКТ. Ова не изненадува, бидејќи развојот на индикатори („црвени знаменца") кои конкретно се однесуваат на ТЛ преку користење на ИКТ е далеку од јасен – како што беше дискутирано нашироко во Поглавје 2. Норвешките власти изјавија дека, иако „имаат збир на индикатори за да се идентификуваат жртвите на ТЛ", тие треба да се ревидираат и да се прошират за да се прилагодат на „околината за истрага на криминалот преку користење на ИКТ". Оваа работа е преземена од Норвешката национална експертска група за ТЛ.

Британските власти објавија дека користат листа на индикатори за помош при **идентификацијата на жртвите на ASW**. Нивното искуство за користење на такви индикатори заедно со алатките за пребарување на веб-страниците (web-scraping) говорат многу. Според доставените докази, иако овие индикатори можат да пружат

[17] Меѓу технолошките алатки што ги користат земјите во борбата против сексуалната експлоатација на деца (CSE), постојат „Gridcop" и „IcacCops". Исландската полиција го користи „Griffeye" за обработка, сортирање и анализа на слики и видеа запленети за време на истрагите на CSE и за вкрстување на овие слики со меѓународните бази на податоци.

одредена помош, тие „треба да се користат заедно со мрежната анализа и проценките на автентичноста на сметката за да се гарантираат најдобрите практики". Ова укажува на потешкотиите во автоматизирањето на идентификацијата на жртвите – и границите на претерано потпирање на однапред поставената листа на индикатори. Покрај тоа, британското искуство ја покажува важноста од комбинирањето на различни методи, вклучувајќи ја **анализата на социјалните мрежи** и **човечката проценка** на доказите. Уште еднаш, јасно се појавува клучната улога на аналитичарите/истражителите – како и потребата од нивно ефективно обучување. Алатките може да бидат навистина вредни во самото намалување на податоците, како и во работата на голем обем на информации; сепак, тие треба да бидат користени од добро обучени оператори со познавање на одредена тема/прашање (на пр. ТЛ).

Користењето на вештачката интелигенција и технолошките алатки за идентификација на жртвите не е без предизвици, вклучувајќи ги **етичките прашања** и потенцијалот за дискриминација (на пример, профилирањето врз основа на дискриминаторски критериуми; видете ја и дискусијата во Поглавје 6). Шведската полициска управа изрази загриженост во врска со „употребата на вештачка интелегенција за идентификација на жртвите на трговија со луѓе".

На крајот, Канцеларијата на грчкиот Национален известувач и Лабораторијата за права на Универзитетот во Нотингем пилотираат проект со помош на сателитски податоци и методи на далечинско набљудување за следење на работните услови и мобилноста на работниците мигранти во земјоделието. Грчкиот известувач е во процес на развој на дополнителни технолошки апликации за идентификација на жртвите на ТЛ во земјоделскиот сектор, а развојот на нови технолошки апликации го издвои како клучна компонента на Националниот акциски план 2019-2023 година.

3.4.2. Иницијативи засновани на технологија за помош на жртвите и ширење на информации до ризичните заедници

Овој дел претставува преглед на иницијативите кои се потпираат на технологија, а кои се осмислени со цел да им помогнат на жртвите и да ги прошират информациите до ризичните заедници. Ве молиме имајте предвид дека иницијативите дискутирани во продолжение се идентификувани од страна на земјите-членки.

Механизми за онлајн известување и линии за помош. Неколку земји имаат механизми за анонимно пријавување на злоупотреба, како и добивање првична помош преку телефонски линии за помош. Некои линии за помош нудат 24-часовна поддршка и можат да ги упатат жртвите до социјалните услуги, преку објаснување на процедурите и нивните права. Во Холандија неколку организации нудат **дигитална помош преку функцијата за разговор (chat)** („Fier" и „Slachtofferhulp Nederland" се две од тие организации). Ваквите организации нудат првични совети, помош и можност за анонимно пријавување на сексуална експлоатација. Функцијата за разговор (chat) не е само реактивна, туку служи и за проактивно воспоставување на контакт со поединци изложени на ризик. Холандското Министерство за правда и безбедност во моментов истражува како оваа алатка може дополнително да се развива во соработка со релевантните засегнати страни. Во Франција, Министерството за внатрешни работи води платформа за пријавување сексуално и родово-базирано насилство (PVSS). Жртвите можат да стапат во контакт со службено лице преку **инстант пораки/онлајн разговори (chats)**, да пријават и да добијат прва помош.

Онлајн официјални материјали. Информативните материјали произведени од властите често се објавуваат на официјалните веб-страници. Во Австрија, на пример, информациите за жртвите на трговија со луѓе што ги изработува Сојузното Министерство за внатрешни работи, како и невладините организации, се достапни на неколку јазици на различни онлајн платформи и социјални медиуми. На веб-страницата на Сојузното Министерство за правда, жртвите на ТЛ можат да пристапат до материјали на 16 јазици за нивните права на психосоцијална и правна поддршка. Во Полска, Министерството за внатрешни работи и администрација и Министерството за надворешни работи спроведоа онлајн информативна кампања преку веб-страницата „e-konsulat" со банер на кој се прикажуваат информации за ТЛ на неколку јазици и се пренасочуваат посетителите на Интернет до Центарот за консултации и интервенции за Жртви на трговија со луѓе (KCIK). Покрај официјалните канали, неколку земји ја истакнаа и важната улога која ја играат НВО-ата во ширењето на информации преку нивните веб-страници, како и преку нивните официјални сметки на социјалните медиуми како што се Facebook, Instagram и Youtube.

Онлајн алатки и апликации. Бугарската Национална комисија за борба против трговијата со луѓе претстави онлајн алатка за превенција како дел од годишната кампања за спречување на ТЛ за трудова експлоатација. Онлајн алатката беше создадена во соработка со чешка невладина организација и беше наменета за Бугари кои бараат работа во Чешка. Алатката обезбедува информации за работните услови и ризиците од прекршување на правата на работниците. Како што е наведено од страна на бугарската комисија, „ефективноста на овој пристап беше истакната со фактот дека набргу откако алатката почна да функционира, беше создадена лажна алатка со цел да привлече потенцијални жртви на трудовата експлоатација". Во Литванија, неодамна беше развиена апликација наречена „Raktas" (достапна на Google Play) за да се подигне свеста кај Литванците кои живеат и работат во странство за раните знаци на ТЛ. Во иднина, апликацијата ќе вклучи објект за разговор преку кој литванската жртва или претпоставената жртва на ТЛ ќе може да контактира со литванска невладина организација во реално време и да побара поддршка. Португалската управа за работни услови ја разви апликацијата „ACT", Agir Contra o Tráfico. Естонските власти известуваат за употребата на масовно известување преку СМС/текстуални пораки како дел од кампањата против сексуалната експлоатација. Во 2017 година, Шпанија ја лансираше мобилната апликација „Chicas Nuevas 24 horas: Happy" за да им овозможи на младите да го откријат, преку видео игра, патувањето на една девојка (Хепи) од нејзиниот роден град во Нигерија до нејзиното искуство на сексуална експлоатација во Шпанија.

Онлајн кампањи за подигање на свеста. Во Бугарија, Националната комисија за борба против трговијата со луѓе (NCCTHB) спроведува три кампањи за превенција и информирање на национално ниво секоја година со серија настани кои се фокусираат на спречување на трговијата со луѓе и за принудна работа и за сексуална експлоатација. Материјалите се дистрибуираат и на интернет. Над два милиони бугарски активни корисници беа достигнати на Facebook и Instagram за време на кампањата октомври/ноември 2018 година. Генерално, активностите на NCCTHB и поврзаните онлајн алатки за превенција се објавуваат редовно на социјалните медиуми. Ваквите објави достигнуваат приближно 100.000 корисници/годишно. Дополнително, дискусиите за ИКТ, интернет, социјалните медиуми и влијанието на новите технологии врз ТЛ, како и нивната употреба за регрутирање и експлоатација на жртви, се вклучени во различни активности за подигање на свеста на национално и локално ниво, насочени кон младите и студентите. Извршната агенција на Генералниот инспекторат за труд организира и учествува во информативни кампањи за ризиците поврзани со работата во странство;

исто така, има телефонска линија за совети и известување која е отворена и за бугарските граѓани кои работат во странство.

Во Ирска, тековната кампања „Син превез на очите" [Blue Blindfold] што ја води Министерството за правда редовно дистрибуира информации до ризичните заедници преку посветена веб-страница, печатени медиуми и кампањи на социјалните медиуми.

Во Германија, Сојузното Министерство за економска соработка и развој разви проекти со партнерските земји за спречување и борба против ТЛ. На пример, како дел од проектот „Спречување на трговијата со луѓе во Западен Балкан и поддршка на жртвите", Регионалната иницијатива за миграција, азил, бегалци (MARRI) создаде упатства и информативни материјали за кампањи за подигање на свеста на јавноста и ги направи достапни на интернет. Бидејќи интернетот се повеќе се користи за регрутирање жртви на ТЛ, една од алатките се фокусираше на заканите дека децата се изложени додека се приклучени на интернет[18].

Во Романија, Националната агенција против трговија со луѓе (NAATIP) води кампањи на Facebook, YouTube и, од 2020 година, на Instagram, Twitter и LinkedIn. Објавите на Facebook имаат регистрирано влијание од 2,5 милиони корисници во 2020 година (+300% во однос на претходната година). Примерите на кампањи вклучуваат:

(а) секојдневно објавување на социјалните мрежи на превентивни пораки против трговијата со луѓе за различни видови на експлоатација (сексуална експлоатација, трудова експлоатација и принудно питачење);

(б) онлајн кампањата „Совршената работа – едностана илузија" во партнерство со OLX Romania (веб-услуга за поставување/хостирање на објави) чија цел е да се спречи трговијата со луѓе преку зголемување на свеста кај луѓето кои бараат вработување преку онлајн платформи;

(в) приклучување на двајца познати романски влогери на YouTube со заедничка публика од 1,3 милиони следбеници за зголемување на видливоста и ефективноста на пораките за борба против трговијата со луѓе на NAATIP. Влогерите снимија две видеа за ТЛ, кои постигнаа околу 100.000 прегледи на YouTube во првите часови од преносот.

Накратко, важно е да се забележи дека, како што истакнаа бугарските власти, ефикасната кампања бара „екстензивна подготвителна работа" за целосно да се разбере нејзината намера и соодветно да се развие нејзината порака. На крајот на краиштата, за тоа се потребни инвестиции. Добра практика е да се работи со приватни компании во продукција на **социјално рекламирање**. Ова може да се направи, на пример, преку публикации спонзорирани од каналите на социјалните медиуми како што се Facebook и Instagram (платформата може да обезбеди слободен простор, како и експертиза за дизајнирање кампања/порака). Јасно е дека таргетираните и добро развиени онлајн кампањи можат да бидат корисна алатка. Примерот на кампањата што ја водеше Бугарската национална комисија за борба против трговијата со луѓе е значаен. Како дел од кампањата – дизајнирана да ја подигне свеста за ТЛ за трудова експлоатација – беше продуциран и циркулиран визуелен приказ на пример за измамничка понуда за работа. Корисниците помислија дека понудата за работа е вистинска и почнаа да се јавуваат во канцеларијата на Националната комисија, поставувајќи прашања за работата (види Дел

[18]„Малолетници кај кои постои ризик од компјутерски-трговија" (toolboxes.marri-rc.org.mk/tips/minors-at-risk-of-cyber-trafficking).

1.1.2 за повеќе детали во врска со кампањата). Овој пример го покажува потенцијалниот досег/влијание на измамничките огласи за работа, но истовремено за Комисијата ова претставуваше „добра можност да ги информира оние што бараат работа подготвени да прифатат ризични понуди".

Сепак, како што предупредија бугарските власти, постои **ризик од претерано потпирање на онлајн кампањите** кога се обидуваат да допрат до потенцијалните жртви. Во некои случаи, таквите жртви доаѓаат од „ранливи заедници" кои се карактеризираат со ниско образование и ограничено познавање на технолошките алатки и ресурси. Во тие околности, достапноста заснована на директен (личен) пристап (сè уште) има важна улога како превентивна стратегија.

Конечно, инспирацијата за иницијативи може да дојде од проекти кои се справуваат со прашања слични на онлајн ТЛ преку користење на технологија. Во Финска, на пример, невладината организација Women's Line започна проект наречен *Turv@verkko*, кој има за цел да го спречи насилството врз жените и девојчињата преку ИКТ и да им помогне на жртвите. Слично на тоа, Youth Exit и *Sua varten* се насочени кон младите корисници на интернет за да спречат сексуално вознемирување онлајн. Иако не се директно поврзани со ТЛ, ваквите иницијативи може да понудат корисни информации за развој на проекти насочени кон жртвите на трговија со луѓе.

3.5. Докази од невладини организации

Невладините организации пријавија голем број стратегии за подобрување на помошта за откривање на жртвите и подигање на свеста во врска со онлајн трговијата со луѓе преку користење на технологијата.

Ла Страда Интернешнал, КОК (Германија), Астре (Швајцарија) и Ла Страда Молдавија ја истакнаа важноста **адекватните и ажурирани информации** да бидат лесно достапни на интернет за жртвите на трговија со луѓе и поединците подложни на експлоатација и злоупотреба. Тука треба да се вклучени информациите за организациите за поддршка и линиите за помош. Ваквите онлајн платформи треба **да овозможат и самоидентификација** на жртвите. Ла Страда Интернешнал истакна дека релевантните информации добиени од невладините организации треба да се споделат со органите на прогонот - откако ќе се добие согласност од засегнатото лице. Предвидени се иницијативи за зголемување на самопријавувањето и во врска со трудовата експлоатација, на пр. во форма на онлајн платформи и апликации преку кои луѓето можат анонимно да пријават злоупотреба на трудот (докази од Фондацијата Састејнабл Рескју, Холандија).

Достапноста на онлајн информациите и механизмите за самоидентификација треба да се поврзат со **кампањите за подигање на свест**. Ла Страда Интернешнал смета дека два вида кампањи се особено важни: (а) оние кои се директно насочени кон потенцијалните жртви и поединци кои се изложени на ризик од експлоатација и злоупотреба; и (б) оние кои се насочени кон засегнатите страни за да ги препознаат ризиците од трговијата со луѓе преку користење на технологија и како да пријават. Различни и еднакви (Албанија) и КОК (Германија) ја истакнаа важноста од едукација на корисниците на ИКТ за ризиците поврзани со технологијата. Тие предложија да се водат пошироки кампањи **за подигање на свеста за тоа како трговците со луѓе би можеле да ја искористат технологијата** и ризиците со кои може да се соочат

поединци во ризик (особено помладите корисници). Треба да се стави акцент на регрутирањето, конкретно на тоа како може да започне потенцијалната експлоататорска ситуација (т.е. како трговците со луѓе воспоставуваат првични контакти). Компаниите кои обезбедуваат онлајн и ИКТ услуги треба да бидат дел од овој ангажман. Центарот за права на мигрантите Ирска исто така забележа дека компаниите на социјални медиуми треба да работат на одвраќање од дејствието.

Во продолжение, неколку невладини организации, вклучително и Ла Страда Интернешнал и од Фондацијата Састејнабл Рескју, ја истакнаа важноста од зголемување и подобрување на **размената на податоци** меѓу релевантните засегнати страни. Овие размени треба да вклучуваат ажурирано знаење за ризиците поврзани со технологијата.

Невладините организации ја истакнаа важноста од унапредување на знаењето за ризиците поврзани со ИКТ, и поопшто за ТЛ преку злоупотреба на технологија на организациите кои им помагаат на жртвите и даваат советодавните услуги. Бидејќи **чувањето на електронските докази** е клучно во градењето на ефикасни истраги, од клучно значење е советниците и невладините организации кои се непосредно вклучени во првите редови да бидат запознаени со стратегиите за чување на дигиталните докази (на пр. со складирање на историите на разговорите (chat history)). Нудењето на сеопфатна обука за безбедноста на податоците и следење на нивната трага на интернет на советниците и невладините организации се смета за клучна.

ФИЗ (Швајцарија) забележа дека ИКТ, вклучително и социјалните медиуми и онлајн информациите, можат да им помогнат на невладините организации да воспостават контакти со потенцијалните жртви и да соберат дополнителни информации за околностите на експлоатација. Доколку се предупредени за сомнителна ситуација, невладините организации може **да ги искористат достапните онлајн информации за да воспостават контакт со претпоставената жртва**.

Центарот за права на мигрантите Ирска и Астре (Швајцарија) предложија да се формираат посебни единици за истрага на дигитален криминал со експертиза за ТЛ преку злоупотреба на интерент. Праксис (Грција) повика на зајакнување на експертизата на органите на прогонот за ИКТ и поврзаните ризици. Исто така, тие повикаа на засилена соработка и размена меѓу властите и приватните компании.

Доказите од невладините организации потврдуваат дека „**црвените знаменца**" за случаите на ТЛ преку користење на технологија не се употребуваат нашироко. Невладините организации известуваат дека користат стандардни индикатори, но тие бараат **ревидирање на таквите индикатори** за да се земат предвид специфичностите на ИКТ – особено во однос на регрутирањето и искористувањето преку ИКТ. КОК (Германија) сугерираше дека следењето на веб-страниците каде клиентите разменуваат искуства за купување сексуални услуги може да обезбеди навестувања за присилна проституција/ТЛ. Прегледот на „црвените знаменца" може да вклучи индикатори кои се применуваат на таквите веб-страници.`

3.5.1. Фокус на иницијативите кои се потпираат на технологијата

Ла Страда Интернешнал смета дека нејзините членови и другите невладини организации „сè повеќе" ја користат технологијата. Сепак, иако „техничките ресурси и можности се енормно зголемени", степенот до кој невладините организации ја користат технологијата останува „ограничен". Според Ла Страда Интернешнал, технологијата

најмногу се користи за регистрирање податоци, а потоа и нивна анализа и за следење на активностите за поддршка. Сè повеќе, невладините организации користат технологија, вклучително и социјалните медиуми, за да водат кампањи (на пр., кампањи за подигање на свеста; видете во продолжение) и да обезбедат информации, како и да „стапат во контакт со ризични групи или да се вклучат со онлајн заедниците " (поднесок од Ла Страда Интернешнал). Како дел од тековната студија, од невладините организации беше побарано да наведат примери на иницијативи кои се потпираат на технологија за подобрување на откривањето на онлајн ТЛ преку користење на технологија, идентификација на жртвите и спречување на идни случаи. Во продолжение е даден краток преглед на ваквите иницијативи врз основа на доказите обезбедени од невладините организации.

Онлајн самопријавување и контакт со потенцијални жртви

- Ла Страда Молдавија укажа на онлајн механизми за децата сами да ги пријават безбедносните прашања на интернет (www.siguronline.md). Тука се вклучени непријатните ситуации со кои можеби се соочило детето додека било на интернет. Детето потоа ќе биде ставено во контакт со специјализиран советник и, доколку се утврдат докази за сексуална злоупотреба или експлоатација на интернет, случајот ќе биде пријавен кај органите на прогонот.

- Во Швајцарија, Астре забележала зголемен број жртви кои сами ги побаруваат нивните услуги, како и потенцијални жртви кои се упатени до нив од страна на пријатели или клиенти благодарение на онлајн присуството на организацијата. Астре нуди и онлајн формулар за воспоставување контакт и барање помош. Понатаму, ФИЗ укажа на успешното користење на платформите на социјалните медиуми за воспоставување контакт со потенцијалните жртви на трговија со луѓе, доколку се знае името на лицето. Веб-страницата на швајцарската „Национална платформа против трговија со луѓе" содржи линкови до голем број организации кои можат да понудат поддршка.

- Правична работа [Fair Work] (Холандија) ги користат социјалните медиуми за да допрат до заедниците на мигранти за да ги идентификуваат жртвите на трговија со луѓе или експлоататорските ситуации. Правична работа [Fair Work] прво ги идентификува Facebook страниците кои се релевантни за одредена целна група, а потоа споделува информации преку таквите страници. Организацијата создава анонимни лични сметки, кои ги менаџираат волонтерите, а кои се користат за превенција. Бидејќи работниците мигранти често ги користат социјалните медиуми за да најдат информации, социјалните медиуми може да се искористат за да им се помогне на загрозените поединци „да станат помалку изолирани и повеќе оснажнети" и да ги намалат ризиците од ТЛ (поднесок од Ла Страда Интернешнал). Сепак, ова не е секогаш лесна задача, бидејќи не е секогаш „лесно за жртвите да знаат каде да бараат соодветни информации, на кои информации да им веруваат; со кого да контактираат и да дознаат кој најдобро може да им помогне, особено ако тие имаат малку познавање за земјата и нивните права во таа земја".

- Ла Страда Интернешнал укажа на напредокот на некои од нејзините членки, кои нудат онлајн консултации (chat) преку кои се добиваат совети и се пријавува експлоатација и злоупотреба – дополнително на услугите кои се даваат преку телефонската линија за помош.

- Ла Страда Интернешнал, исто така, објави дека нејзините членки вообичаено користат онлајн платформи, како што се Facebook, Instagram, LinkedIn и нивните сопствени веб-страници, за да информираат за нивната работа. Слично на тоа, КОК (Германија) пријави дека нејзините членови ги користат веб-страниците, Facebook и WhatsApp за ширење информации и воспоставување канал за комуникација со потенцијалните жртви. Клучно е тоа што една организација нуди број на WhatsApp на клиентите за да пријават знаци на потенцијална експлоатација меѓу сексуалните работници/чки.

Мобилни апликации за подигање на свеста и барање помош/информации

- Ла Страда - Чешка Република беше вклучена во создавањето на SAFE, апликација развиена од IOM Словачка во форма на интерактивна игра дизајнирана да спречи ТЛ. Со играње на играта, корисниците го проценуваат нивниот ризик во однос на ТЛ; апликацијата содржи и информации за безбедно патување, работа во странство и корисни контакти во случај на итни случаи. Астра (Србија) разви апликација BAN Human Tracking [СТОП за трговијата со луѓе], дизајнирана со цел да ги освести младите за ситуациите кои потенцијално водат до експлоатација и да им даде совети како да ги забележат. Тие планираат да ја надградат со функција за известување за експлоататорски практики.

- Ла Страда Интернешнал го истакна развојот на апликации од невладините организации за пријавување на експлоатација и злоупотреба како, на пример, апликацијата развиена од Ансин [Unseen] (Велика Британија). Во Албанија, Различни и еднакви учествува во различни мобилни апликации (на пр., „*#raporto #shpeto*“) дизајнирани да им помогнат на жртвите на трговија со луѓе и родово-базирано насилство („*#GjejZa*“).

- Ла Страда Интернешнал понатаму го истакна развојот на апликации за поддршка на ранливите групи преку, на пример, обезбедување пристап до информации или права за вработување во земјата на дестинација. Пример е апликацијата Workenn: Игра за интеграција на мигрантите на пазарот на труд, произведена како дел од проектот Сириус за да им се помогне на мигрантите кои бараат работа. Пример вон Европа-Apprise Audit е платформа развиена од клубот Меконг и Универзитетскиот институт на ОН во Макао, што овозможува безбедни и доверливи интервјуа на работниците на јазикот на испитаниците.

Онлајн кампањи за подигање на свеста

- Ла Страда Молдавија спроведе кампања за подигање на свеста за време на „Денот за побезбеден интернет 2019“ чија цел беше да се подигне свеста за сексторзијата кај младите. Луѓето беа охрабрени да пријавуваат случаи преку безбедносен механизам за пријавување на интернет (www.siguronline.md). Кампањата достигна околу 70.000 онлајн корисници. Истата организација тестираше стратегии за профилирање за да ги таргетира онлајн корисници со избирање на возрасната категорија, интереси и профили.

- Различни и еднакви (Албанија) спроведе неколку онлајн кампањи за подигање на свеста користејќи социјални мрежи и апликации (вклучувајќи Facebook, Instagram, Twitter, веб-страница и YouTube) фокусирани на превенција од ТЛ, сексуална злоупотреба и семејно насилство (достигнувајќи околу 15.000 корисници). Беше започната кампања, заедно со други невладини организации, за време на пандемијата со Ковид-19.

- Нови пут (Босна и Херцеговина) спроведе неколку кампањи за подигање на свеста фокусирани на употребата на технологијата во однос на ТЛ и сексуалната експлоатација на децата.

- Astra (Србија) спроведе кампањи за подигање на свеста за главните начини на регрутирање, вклучително преку понуди за работа на Интернет, за груминг преку Facebook и социјалните мрежи, како и за стратегии за контрола и искористување на жртвите (вклучувајќи следење на жртвите преку употреба на опциите за локација достапни во најчесто користените апликации).

Понатамошни иницијативи

- Во 2018 година, Астра (Србија) спроведе експеримент „виртуелно девојче" - профил на 15-годишно девојче кое навигира низ Интернетот. Во рок од 24 часа, овој профил прими над 3.000 барања, вклучувајќи понуди за работа и експлицитни сексуални понуди од возрасни мажи (доказ поднесен од Ла Страда Интернешнал).

- Различни и еднакви (Албанија) обезбедува, како дел од нивната програма за реинтеграција, обука за користење на компјутер и технологија, која вклучува техники за заштита на податоците.

- Ла Страда Интернешнал забележа некои јавно-приватни иницијативи во кои се вклучени НВО-а, на пр. проект започнат од Универзитетот во Амстердам со големите холандски банки за да се идентификуваат случаите на трговија со луѓе. Невладините организации со седиште во Холандија, вклучувајќи ги FairWork, CoMensha и Ла Страда Интернешнал, беа консултирани како дел од оваа иницијатива.

Идни чекори и решавање на критични прашања

Постои голем консензус меѓу невладините организации дека може да се направи повеќе за да се искористи технологијата, особено за ширење на информации, да се пристапи и да се комуницира со потенцијалните жртви – како и да се добијат совети и извештаи. ФИЗ (Швајцарија) предложи дополнително да се развијат алатки за анонимно пријавување насилство и експлоатација и да се обезбедат контакти со невладини организации кои нудат услуги за заштита на жртвите и советување. КОК (Германија) ја истакна важноста од понатамошен развој на визуелни прикази, на пр. видеа, слики и апликации, кои ќе се користат за време на обуката и ќе се споделуваат онлајн, вклучително и меѓу ризичните заедници.

Невладините организации, исто така, покренаа некои **критични прашања** поврзани со иницијативите и технолошките алатки. Ла Страда Интернешнал истакна дека технолошките алатки генерално се произведуваат како дел од самостојни проекти и „често не вклучуваат периоди на тестирање". Така, ни остануваат ограничени докази за нивната ефикасност. Понатаму, кога финансиската поддршка за проект завршува, често нема долгорочна финансиска стратегија за промовирање и искористување на произведените алатки. Ова е особено проблематично, бидејќи за алатките е потребно „континуирано ажурирање и обука".

Ла Страда Интернешнал понатаму забележа дека иницијативите „често немаат доволно вклученост на НВО-а и други засегнати страни кои треба да ги користат алатките во пракса, па затоа отсуствува чувството на сопственост". Исто така, истакна дека сè уште останува „нејасно какво е влијанието на технологијата врз ефективното спречување или борба против ТЛ", прашувајќи дали „надзорот и профилирањето на државните граници, како и на други локации [доведоа] до вистинска идентификација на жртвите на трговијата со луѓе" и дали лицата идентификувани преку технологија потоа добиле „помош и заштита". Тие повикаа на **поголема евалуација и проценка на влијанието** на „сите развиени технолошки алатки". „Дали овие - честопати скапи - алатки им служеа на потребите на заинтересираните страни за борба против трговијата со луѓе и дали алатките се всушност тестирани и добро искористени и ако не, зошто не?", се запрашаа тие.

Од суштинско значење е тоа што невладините организации истакнаа дека, генерално, сè уште има ограничена достапност на технолошките алатки што практичарите можат да ги користат. За да одговараат на потребите на невладините организации, **алатките треба да бидат „евтини и лесни за употреба"**. Фондацијата за одржливи ресурси дополнително предупреди дека „алатките создаваат вишок на податоци за различни корисници", затоа е важно да се развијат имајќи ги предвид специфичните потреби и сеопфатна стратегија за да се избегне дуплирање на алатките кои извршуваат (лесни) функции додека истовремено недостигаат алатки кои извршуваат повеќе стратешки, сложени функции.

3.6. Доказ од технолошки компании

Facebook објави различни **соработки со невладини организации** ширум светот во насока на создавање на едукативни кампањи за подигање на свеста за ризиците од сексуалната експлоатација на интернет – особено кај младите корисници – како и за правата на потенцијалните жртви на трговија со луѓе за трудова експлоатација и домашно ропство. Ваквите кампањи обезбедуваат и информации за телефонските линии за трговија со луѓе кои нудат помош и поддршка. Како пример, Facebook ја посочи Кампањата за свесност за трудова експлоатација/домашно ропство (слугување) започната во март 2021 година во партнерство со Стоп за трговијата со луѓе [Stop the Traffick], за да им обезбеди информации на домашните работници и нискоквалификуваните работници на Филипините за нивните права, локални упатства за регрутирање за апликации за работа во странство и достапни линии за помош за да се избегне нелегално регрутирање и злоупотреба.

Facebook, исто така, објави дека е создаден скратен пристап за обезбедување информации и дополнителни ресурси за луѓето кои пребаруваат клучни зборови поврзани со трговијата со луѓе заради сексуална експлоатација. Ваквите клучни зборови се развиени од внатрешни и надворешни експерти.

За да се справи со прашањето за недоволно известување, Facebook посочи дека работат на „проактивно пронаоѓање и преземање акција за содржината поврзана со трговија со луѓе". Тие забележаа „зголемување" на нивната способност „да детектираат насилни содржини [кои] произлегуваат директно од големите инвестиции на техничките и оперативни тимови на Facebook ".

IBM и Stop the Traffik, невладина организација со седиште во Обединетото Кралство, соработуваа во 2014 година за да го создадат Traffik Analysis Hub – нов правно лице кое води **заедничка платформа за споделување податоци**, поткрепена со безбеден облак (cloud) и повеќејазична аналитика на содржини базирана на вештачка интелигенција и геопросторна аналитика. Тоа вклучува 95 организации ширум светот. Целта на платформата е да ја прекине глобалната трговија со луѓе со здружување помеѓу невладини организации (на пр. StopTheTraffik, LibertyShared, CrimeStoppers и Save The Children UK), органи на прогонот (на пример, Европол, Интерпол и различни американски полициски органи) и финансиски институции (на пр. , Western Union, Barclays, Standard Chartered, Lloyds и Paypal). Како што е наведено од IBM, Traffik Analysis Hub користи приспособени модели на ВИ (вештачка интелигенција) специфични за доменот за да добие соодветен обем на релевантни податоци и да ги класифицира овие информации врз основа на класификација развиена од експертите на Traffik Analysis Hub. Податоците потоа се споделуваат меѓу организациите учеснички. Еден од клучните резултати е „Забрзувачот за црвени знаменца", библиотека со типологии развиени од трансакциите со црвено знаменце идентификувани во сметките на жртвите. Ваквите индикатори со црвено знаменце треба да се имплементираат во системите за мониторинг на финансиските институции-учеснички. Дополнително, Traffik Analysis Hub има за цел да развие алатка за предвидување базирана на корелација која ќе помогне да се идентификуваат карактеристиките на заедниците изложени на ризик кои можат да станат жртви на трговија со луѓе.

IBM, исто така, информира за неодамна започнат **бесплатен онлајн патоказ за обука** за луѓе кои се заинтересирани да станат аналитичари на податоци во доменот на ТЛ. Обуката вклучува модули за трговија со луѓе (Вовед во ТЛ; како да се забележат знаците на ТЛ), како и модули за наука за податоци и примена на технологии за анализа на податоци.

IBM, исто така, спонзорира онлајн натпревари DataJam кога експертите на IBM работат со повеќесекторски тимови за да осмислат иновации во примената на технологијата за прекин на трговијата со луѓе. Примерите вклучуваат:

- Алатки за скрејпинг на онлајн-локациите за рекламирање за возрасни и примена на маркери за присилно учество (на пр. јазикот на третата страна, повеќе огласи со исти идентификатори за контакт, огласи кои се однесуваат на познати националности на жртвите согласно онлајн history) и вршење гео-просторна анализа на кластери на огласи од „интерес".

- Алатки за скрејпинг на пораки на пазари и форуми на Deepnet/Darknet, примена на маркери специфични за ТЛ преку вештачка интелигенција, идентификување на трендовски теми и кориснички деноминатори (handle), креирање мрежни модели на теми за понатамошна анализа од страна на органите на прогонот.

- Алатки за валидација на огласи за работа преку интернет за паметни телефони, што им овозможува на поединците да ја потврдат легитимноста на огласите за работа преку интернет пред да се пријават на истите.

Во врска со **соработката со органите на прогонот**, Facebook спомена голем број Јавни/Приватни партнерства (ЈПП) во кои се вклучени, како што е Експертската група за трговија со луѓе на Интерпол (HTEG), за справување со експлоатацијата на луѓето. Како дополнителен пример, Facebook објави дека имплементира систем за онлајн барања за органите на прогонот („LEORS") за да се насочат правните барања за податоци за сметките на Facebook (вклучувајќи барања поврзани со трговија со луѓе). Барањата поднесени преку LEORS се решаваат преку тимови со седиште во Соединетите Американски Држави, Ирска и Сингапур.

3.7. Дополнителни докази од анализата на состојбата

Покрај доказите обезбедени од земјите-членки, невладините организации и технолошките компании, студијата, исто така, спроведе и анализа на документи од тековната база на докази за стратегиите и алатките употребени за борба против онлајн трговијата со луѓе преку користење на технологија.
ОБСЕ и Технологијата против трговијата со луѓе [Tech against Trafficking] (2020) спроведоа истражување на ИКТ алатки и иницијативи подготвени со цел борба против трговијата со луѓе. Тие идентификуваа 305 алатки/иницијативи, подготвени од компании од приватниот сектор, добротворни организации и влади (огромното мнозинство на англиски јазик). Од тие алатки: 26% се дизајнирани за идентификација на жртви и трговци со луѓе; 16% за подигање на свеста; 14% за управување со синџирот на снабдување; 13% за трендови на податоци и мапирање; 10% за идентификација на корпоративен ризик; 9% за ангажирање и зајакнување на работниците и 12% за други цели. Алатките и иницијативите што ги истражуваа ОБСЕ и Технологијата против трговијата со луѓе [Tech against Trafficking] се обидуваат да го постигнат следниот сет на цели: (а) споделување на информации до ризичните заедници, вклучително и мигрантите; (б) едукација за ризиците кои произлегуваат од трговија со луѓе, барање помош и пријавување на потенцијални случаи; (в) отстранување на можностите за експлоатација; (г) идентификација на жртвите; (д) собирање на јавно достапни информации за борба против ТЛ; (ѓ) проценка на ризиците од трговија со луѓе; (е) следење и усогласеност; (ж) идентификување и постапување по типологии. Слично на тоа, Раетс и Јансенс (2018) ги идентификуваа следните (општи) начини на кои алатките кои користат технологија може да се користат во борбата против трговијата со луѓе: (а) собирање и анализа на податоци; (б) блокчејн со можност за следење и потекло (следење на синџирите на снабдување); (в) вештачка интелигенција (ВИ) и машинско учење за добивање висока пресметковна моќ; (г) препознавање на лица (веб-роботи); (д) технологија за жртвите и преживеаните: идентификување и поддршка на жртвите, информирање на различни јазици. Мураскиевич (2018) го идентификуваше индексирањето на веб-страниците (web-crawling); аналитика на податоци; патролирање со цел утврдување на предвидливост; употреба на блокчејн; географски информациски системи (ГИС); онлајн бази на податоци; и иницијативи кои се потпираат на придонесот и соработката од толпата (crowdsoursing) како дополнителни начини на кои алатките базирани на технологија може да се операционализираат за борба против ТЛ. Честопати е нејасно кои од овие алатки навистина функционираат, кои од нив можат корисно да се надградат и кои навистина даваат придобивки за жртвите на трговија со луѓе (некои од анкетираните алатки се чини дека се дизајнирани да собираат информации согласно

кои потоа е тешко да се дејствува). Треба да се постапи по информациите добиени преку технологијата. Во случајот што го дискутираа Ренде Тејлор и Ших (2019), беше откриено дека тешко се постапува по пријавите на работниците преку електронски апликации и нивни повратни информации/коментари за експлоатацијата во синџирите на снабдување.

Во литературата е наведено дека на технологијата тешко може да се гледа како на замена на знаењето добиено од терен. Понатаму, според органите на прогонот, интервјуирани од Елиот и Мекартан (2013), технологиите за мобилни телефони, вклучително и апликациите, можат да бидат дел од пакетот алатки за борба против трговијата со луѓе, но тие не се волшебно стапче. Оперативно, на давателите на интернет услуги се гледаат како на субјекти кои поседуваат важен дел од електронските докази, па оттука неколку извори укажаа на важноста од одржување на тесна соработка со приватниот сектор. Таквата соработка треба да опфати механизми кои го олеснуваат стекнувањето докази, отстранувањето на таквите докази секогаш кога е соодветно и брзото известување до органите на прогонот во конкретни случаи. Во исто време, идентификувани се голем број пречки за споделување информации помеѓу различните актери. Тие вклучуваат прашања за приватноста и безбедноста на податоците. Упатени се и повици за заеднички меѓународни (мултилатерални) стандарди кои ја поткрепуваат соработката помеѓу органите на прогонот, невладините организации и приватниот сектор.

Само многу мал збир на специфични алатки беа повеќекратно спомнати од неколку извори. Тие ги вклучуваат: (а) Проектот Артемис [Project Artemis] на Microsoft, кој разви алатка за откривање на техники за груминг преку оценка на резултатите од анализа на ризиците од минати разговори, по што следува означување на најсомнителните кои се предмет на понатамошно испитување од аналитичар; (б) PhotoDNA од Microsoft, која создава единствен дигитален потпис (hash) на сликата, кој потоа се користи за откривање на сексуална експлоатација на деца.

Меѓународната конфедерација на синдикати извести за кампањата за подигање на свеста што ја води AidRom за да им даде информации на луѓето кои бараат работа на интернет во странство. Оваа кампања вклучуваше совети за тоа како да забележите сомнителни реклами и ги дава следниве упатства: „1. Обрнете внимание на изворот на снабдување. Повеќето специјализирани сајтови за барање работа не ги проверуваат објавите од компаниите за вработување. 2. Никогаш не прифаќајте понуда што доаѓа од поединци. 3. Внимателно прочитајте го договорот за посредување за вработување. Ако плаќате сума пари за да се вработите, погрижете се да знаете за што плаќате и на што се согласувате како услови. Откако ќе се потпишете, тешко е - или невозможно - да се направат измени. 4. Прашајте што е можно повеќе детали за работата за која сте примени. 5. Ако работата изгледа премногу добра за да биде вистинита...веројатно не е вистина!". Интернетот се користи како алатка за заштита од навредливо вработување. Не е јасно колку долго траеше оваа кампања и дали е надградена или спроведена во други земји.

Два проекти, исто така, често се наведуваат како примери за добри практики: Spotlight на Thorn и Polaris Project, двата со седиште во САД. Spotlight е веб алатка развиена за да им помогне на истражителите да ги идентификуваат децата- жртви на трговија со луѓе преку користење на онлајн докази. Сепак, има многу малку информации за софтверот во јавниот домен. Polaris ги анализира податоците главно собрани преку Националната телефонска линија за трговија со луѓе, дополнети со други (неодредени) извори на информации.

Придонесот од толпата (crowdsourcing) за откривање на жртви се наведува како граѓанска иницијатива со помош на користење на технологија, од која TraffickCam често претставува главен пример. Тој бара од луѓето да фотографираат хотелски соби за да можат потоа да се користат за идентификување на локациите на жртвите. Сепак, не е јасно дали таквите иницијативи се ефективни. Понатаму, тие може да покренат прашања за приватност, како и потенцијален ризик од осветништво. Иако укажувањата од клиентите се многу вредни, иницијативите за придонес од толпата (crowdsoursing) треба внимателно да се проверат и да се избалансираат против ризикот од создавање виртуелни (и невиртуелни) групи на осветници.

Поопшто, ICAT (2019) идентификуваше голем број начини на кои технологијата може да игра позитивна улога во справувањето со трговијата со луѓе. Тие вклучуваат: (а) помагање на истрагите; (б) унапредување на гонењето; (в) подигање на свеста; (г) обезбедување услуги на жртвите; и (д) фрлање ново светло на составот и работењето на мрежите за трговија со луѓе. Различни извори укажаа на важноста на „**дигиталните отпечатоци**", што значи дека онлајн содржините и поврзаните уреди се исклучително богат извор на информации (Мирја 2017; Мичел и Бојд 2014). Клучно е тоа што можно е да се мапираат **криминалните мрежи** врз основа на сајтови за социјално вмрежување (Мирја 2017; исто така ICAT 2019 и TRACE 2015). Собирањето и анализата на дигиталните докази може да го **намали товарот на жртвите** да обезбедат докази против трговците со луѓе (како и докази во нивна одбрана).

4. Обука: каква обука постои, каква е потребна

4.1. Обука за органите на прогонот: каква обука постои и каква е потребна

Студијата најпрво ја разгледа обуката што моментално им се обезбедува на органите на прогонот за откривање и истражување на случаи на онлајн ТЛ преку користење на технологија. Потоа, беше спроведена „анализа на потребите" со цел да се идентификуваат дополнителните потреби за обезбедување на обуки кои би можеле да се понудат за да се зголеми ефикасноста на откривањето на ТЛ и на истрагата, како и на идентификацијата на жртвите.

Општо земено, различни земји обезбедуваат различни нивоа на обука за органите на прогонот, спроведени во различни формати. Севкупно, огромното мнозинство земји известуваат дека спроведуваат обука за ТЛ. Публиката на таквата обука, сепак, варира меѓу земјите, при што некои бараат од сите полициски службеници кои би можеле да дојдат во контакт со потенцијална жртва да поминат таква обука, додека други ја ограничуваат обуката на специјализираните единици.

Кои се елементите за обука кои земјите ги сметаат за клучни во однос на онлајн трговијата со луѓе преку користење на ИКТ? Постои консензус за фактот дека полициски службениците треба да добијат обука за (а) како да откриваат случаи и жртви; (б) како да се соберат, складираат и обработуваат **електронските докази**, вклучувајќи ги и методите за извлекување информации од компјутери и други дигитални медиуми; и (в)

како да се користат релевантни софтверски пакети, вклучително и **анализа на масивни податоци (Big Data Analysis)** и веб-роботи (онаму каде што тоа е дозволено со домашното законодавство). **Обуката за OSINT** се смета за суштинска од неколку земји. Истражувачките техники кои вклучуваат **тајни онлајн истраги**, исто така, се сметаат за клучни.

Иако огромното мнозинство земји кои известија дека обезбедуваат елементи на оваа обука, тие исто така истакнаа некои предизвици, вклучувајќи ја: (а) потребата од постојано да се осовременува обуката и, во некои случаи, значително да се подобрат тековните обуки кои се обезбедуваат; и (б) потребата од зголемување на процентот на персонал кој ќе биде обучуван. Некои земји изразија загриженост во врска со ограничената обука што често се обезбедува во врска со прашања поврзани со ИКТ и, што е уште поважно за ТЛ преку користење на ИКТ. Предложено е да се **осмислат и да се обезбедат интензивни курсеви за обука за ТЛ преку користење на ИКТ**, кои ќе ги покриваат и техничките прашања. Повторно, различните земји би се нашле во поинаква позиција во однос на дигиталните можности на органите на прогонот, но неколку земји ја споменаа потребата од нудење на **дополнителна обука за употребата на ИКТ** во насока на унапредување на откривањето на случаите за ТЛ.

Земјите, исто така, укажаа на потребата од изведување на почетна и континуирана обука земајќи го предвид опкружувањето кое постојано се менува кога станува збор за истрагите. Ова, пак, бара ресурси за подготовка на модули за обука (вклучувајќи истражување за нови случувања во контекст на ТЛ преку користење на ИКТ) и нивно спроведување.

Не е невообичаено земјите-членки да имаат свои службеници кои посетуваат модули за обука организирани од меѓународни организации или од други земји. Размената на информации и знаења на меѓународно ниво секако е добра практика. Покрај тоа, за земјите со ограничени буџети и ресурси, придобивките може да бидат значителни. Сепак, бидејќи некои елементи за обука многу зависат од контекстот, постои потреба сите земји да бидат во позиција да развијат знаење во своите земји и да понудат обука која *исто* така ги зема предвид локалните специфичности на феноменот (ограничен број земји во моментов не организираат никаква обука за ТЛ и ТЛ преку користење на ИКТ, вклучително и за OSINT, туку се потпираат само на обука обезбедена од надворешни организации).

Различни земји имаат различни организациски структури, особено кога се станува збор за тоа каде се наоѓа знаењето за ИКТ. Сепак, од клучно значење е да се истакне важноста од избегнување на кочниците во секојдневното работење поради распределбата на вештините која не секогаш е најоптимална. На пример, важно е **знаењето да не е распоредено во изолирани силоси**, со што се попречуваат ефективните истраги. Предвидено решение е да се размислува за двонасочен систем на обука помеѓу службениците специјализирани за ТЛ и службениците специјализирани за ИКТ. Друга стратегија е да се дисеминира одреден степен на ИКТ вештини меѓу различни единици, вклучувајќи ги и единиците за трговија со луѓе. Гледајќи напред, **ризикот од кочници** е особено акутен. Бидејќи злосторствата преку користење на ИКТ, вклучително и ТЛ, веројатно ќе се зголемат, постои потреба да не се потпираме премногу на централизирани центри за компјутерски криминал. Идеално, таквите центри треба да се користат само во случаи кои се карактеризираат со многу високо ниво на технолошка софистицираност - *што се чини дека не го претставува типичниот случај на ТЛ преку користење на ИКТ*. Со цел да се избегнат кочниците во системот, од клучно значење е да се вклучи општо/основно **„компјутерско" знаење во**

рутинската обука што им се обезбедува на истражителите наместо да се гледа ова како збир на „специјализирани" вештини.

Врз основа на доказите од земјите-членки, можеме да идентификуваме шест широки области кои се сметаат за критични во градењето на капацитети. Тие вклучуваат:

- Собирање и анализа на информации од отворени извори (OSINT).
- Собирање податоци од профилите на социјалните мрежи и апликациите за комуникација, како и од Darknet/TOR мрежата.
- Испитување на информациите присутни на уредите за комуникација и складирање на информации, вклучувајќи информации избришани од корисниците, како и знаење од областа на шифрирање.
- Способност да се потврдат податоците добиени од ИКТ извори со дополнителни докази стекнати во текот на кривичната истрага.
- Идентификација на жртви/потенцијални жртви во онлајн опкружувањето.
- Обука за економски и финансиски криминал со елемент посветен на онлајн трансакции и потенцијални криптовалути.

4.1.1. Дизајнирање идни обуки и добри практики

Доказите од земјите-членки укажуваат на голем број конкретни иницијативи кои би можеле да се усвојат за унапредување на обезбедувањето на обуката во контекст на онлајн ТЛ преку користење на технологија. Во продолжение се дадени неколку предлози за дизајнот на идните модули за обука.

- Креирање на студии на случај и сценарија засновани на ТЛ кои ќе бидат вклучени во **обуката за „дигитална истрага"**. Таквата обука може да се подели на две нивоа: Ниво 1 може да се спроведе за сите службеници од првите редови, додека Ниво 2 може да вклучи обезбедување на напредни обуки кои ќе бидат спроведени за помал број на слушатели. Може да се замисли дека барем еден дел од оваа обука ќе биде во форма на учење во мали групи за да се поттикне размената на идеи и дискусијата околу практиките.

- **Додавање ИКТ елемент на постоечката обука за ТЛ**. Додека неколку земји споменаа обезбедување обука за ТЛ, само мал број експресно укажа на вклучувањето на елементи фокусирани на ИКТ во оваа обука. Бидејќи сè повеќе и повеќе интеракции се одвиваат онлајн, од клучно значење е да се вклучат ИКТ елементи во „традиционалната" обука за трговија со луѓе. Техничката обука може да вклучува елементи за најдобрите практики во истражувањето на ТЛ преку користење на ИКТ, како и национални и меѓународни искуства.

- Спроведување на заеднички активности за обука кои вклучуваат повеќе земји изготвени преку разгледување на актуелните трендови. На пример, ако има докази дека жртвите имаат тенденција да се регрутираат во земјата А, а потоа да се експлоатираат во земјата Б, би можело да биде корисно доколку се организира заедничка активност за обука во која ќе бидат вклучени службеници од А и Б. Пресликувајќи ги заедничките

истражни тимови (ЗИТ) таквите активности би можеле да ги **наречеме ЗАО („Заеднички активности за обука“).**

- Регрутирање на цивилни лица кои работат во полициските служби кои поседуваат технички вештини. Тие службеници можат да се интегрираат во специјализираните единици (на пр. единиците за трговија со луѓе), да развијат знаење за техничките прашања во врска со ИКТ во организацијата и тоа знаење да го прошират во рамките на единицата/организацијата.

- Организирање заеднички сесии за обука на кои ќе се **вклучат специјализирани истражители и обвинители** за да се запознаат двете групи актери за можностите што ги нудат новите истражни методи, на пр. употребата на компјутерски-инфилтрација или онлајн тајни операции, како и собирање електронски докази (вклучувајќи заплена на виртуелни средства). Таквата обука може да ги опфати и техничките и правните аспекти со цел да се зајакне употребата на нови методи ориентирани кон ИКТ меѓу истражителите и обвинителите.

- **Споделување на знаење на меѓународно ниво**, на пр. преку учество во меѓународна/регионална обука фокусирана на специфичните аспекти на истражување на ТЛ преку користење на ИКТ (примерите наведени од земјите-членки го вклучуваат семинарот „Меѓународна соработка во однос на компјутерски криминалот и електронските докази“ организиран од Советот на Европа и заедничкиот проект на ЕУ Cyber@East, спроведен на 7-9 декември 2020 година).

Земјите идентификуваа голем број конкретни иницијативи како примери на добри практики:

- Во Австрија, Заедничката оперативна канцеларија против трговија со луѓе и криумчарење на луѓе (пододдел на Службата за криминалистичко разузнавање) организира обуки и семинари за трговија со луѓе, прекугранична трговија во синџирот на проституција и идентификација на жртви. Специфична обука беше обезбедена на австриската полиција, судските власти, Федералната канцеларија за имиграција и азил (BFA), Федералниот управен суд (BVwG), финансиските власти, трудовите инспекторати и правните советувалишта за откривање на онлајн случаи на ТЛ, вклучително и на социјалните мрежи. Од суштинско значење е тоа што таквата обука отиде подалеку од спроведување на законот и ги вклучи трудовиот инспекторат, советодавните служби и финансиските власти. Понатаму, полициските службеници специјализирани за ИКТ добија специфична обука фокусирана на ТЛ за сексуална експлоатација. Од друга страна, службениците специјализирани за ИКТ обезбедија обука за колегите специјализирани за трговија со луѓе/прекугранична трговија во синџирот на проституција со Службата за криминално разузнавање/CID. Ова е добар пример за двонасочната обука дискутирана погоре - и претставува образец кој потенцијално би можел да се реплицира на друго место.

- Во Бугарија, во 2020 година, на неколку специјализирани работилници за полициски службеници, обвинители и судии се дискутираше за истрагата и гонењето на случаите на трговија со луѓе преку користење на отворени извори на податоци, вклучително и онлајн податоци.

- Како дел од договорите за партнерство со Романија и Бугарија во областа на ТЛ, Норвешка ќе организира две заеднички активности за обука за разузнавачки податоци обезбедени преку користење на отворени извори (OSINT) за романските и норвешките учесници. Целта на обуката е да се зајакне способноста на истражителите во Норвешка, Бугарија и Романија за идентификување и истражување на ТЛ преку користење на ИКТ.

- Во Грција, иницијативите за обука и едукација за компјутерски криминал имаат двонасочен пристап: (а) збир на универзитетски курсеви за подобрување на разбирањето на компјутерскиот криминал кај следните генерации научници и студенти по право, и (б) збир на пократки курсеви за обука на персоналот од органите на прогонот, правосудните органи и вработените во приватниот сектор за подобрување на нивното разбирање за компјутерски криминалот и начинот на кој секојдневно би одговориле на предизвикот.

- Во Велика Британија, органите на прогонот имаат формални стандардни оперативни процедури (СОП) или други насоки за проактивно следење, откривање, истрага и нарушување на ТЛ преку користење на ИКТ. Тие вклучуваат: мапирање на онлајн платформи каде што ризикот од ТЛ е висок; спроведување на тајни операции онлајн; користење на специфични показатели за потенцијалната трговија со луѓе на онлајн платформите; анализа и управување со пријавите добиени преку телефонските линии за онлајн сексуална злоупотреба и експлоатација на деца; употребата на специфични технолошки алатки за борба против ТЛ. Дополнително, истражителите добиваат обука за тоа како ефективно да ги постават информациите добиени од отворените извори со различните форми на разузнавачки податоци.

- Во Франција, првото ниво на обука на полициските службеници вклучува модули за: основи за дигитална истрага; анонимност, темната мрежа (dark net) и виртуелни валути; анализа на опкружувањето кога станува збор за прекршоци поврзани со компјутерски криминал; истражување на интернетот и социјалните мрежи (ова обично е проследено со специјализација на тема, на пр. измама или сексуална злоупотреба на деца); службеници кои се во првите редови за одговор кога станува збор за компјутерски криминалот (т.е. зачувување на дигиталното место на злосторството). Понатамошната специјализирана обука вклучува модули за: истраги на компјутерски криминал (собирање, обработка и анализа на докази од мобилни телефони и компјутери; акти на судска истрага поврзани со дигитални технологии, вклучувајќи правни прашања, меѓународна соработка и истражни стратегии); о-бука на аналитичари за следење/откривање на дигитални траги; стекнување податоци од телефон; истрага под псевдоними. Во моментов се креира еднонеделна обука посветена на ТЛ со цел трудова експлоатација (со цел да се започне во првата половина на 2022 година). Оваа обука ќе вклучува модул посветен на употребата на технолошки алатки.

4.2. Обука за обвинители и судии

Според доставените докази, обезбедувањето обука на обвинителите и судиите во однос на ТЛ преку користење на ИКТ, е прилично нерамномерно меѓу земјите-членки. Неколку земји посочија дека моментално не обезбедуваат никаква обука на судството за овој феномен. Други земји обезбедуваат општа обука за ТЛ без некој елемент конкретно фокусиран на прашања поврзани со ИКТ. Друга група земји посочија дека обезбедуваат обука за тоа како да се користат меѓународните правни инструменти во контекст на

компјутерски криминалот, на пр. Конвенцијата од Будимпешта и поврзаното домашно законодавство и/или за тоа како да се изградат случаи на компјутерски криминал. На крај, група земји ги вклучи елементите на криптовалути и познавањето на специфични технолошки алатки во нивната обука. Во идеални услови, сите земји треба да се **префрлат кон интегрирани обуки за ТЛ извршен со користење на ИКТ, за употреба на меѓународните правни инструменти во контекст на компјутерски криминалот**, како и импликациите од користењето на конкретните технолошки алатки во истражување на случаите на ТЛ (пр. веб-роботи и софтвер за дешифрирање на информации).

Се чини дека помал дел од земјите во нивните студии на случај поврзани со ТЛ вклучиле обука за компјутерски криминал. Слично на тоа, помал број на земји посочија дека обезбедуваат обука која вклучува и елементи за трговија со луѓе и ИКТ.

Земјите во нивните одговори на прашалникот идентификуваа голем број конкретни иницијативи како примери за добри практики:

- Во Република Молдавија, во првиот семестар за 2021 година, Националниот институт за правда одржа обука на 110 слушатели која вклучуваше аспекти на истрагите поврзани со ТЛ преку користење на ИКТ. Обуката вклучуваше сесии за (а) „карактеристиките на истрагите и судењата на кривични дела поврзани со трговија со луѓе и телесни елементи"; (б) „карактеристиките на истрагите и гонењето на кривичните дела во областа на борбата против трговијата со луѓе; (в) „карактеристиките на истрагите и судењата на случаи кои се однесуваат на прекугранично, транснационален и организиран криминал".

- Во Бугарија, Обвинителството при Врховниот суд им одржа семинари на истражителите и обвинителите за ТЛ и употребата на ИКТ во ТЛ. Обвинителството остана на ставот дека „работилниците одржани од експерти од областа на ИКТ се особено ефективни, бидејќи содржат практични примери за користење софтверски програми, како и можности и оперативни алатки за користење на мобилни апликации за откривање на сериозни кривични дела".

- Во Шведска има обвинители специјализирани за ИКТ, од кои некои се занимаваат со случаи на трговија со луѓе. Обвинителството организира интерна обука за спроведување истраги за кривични дела поврзани со ИКТ (вклучувајќи ја употребата на криптовалути во криминални активности). На овие обуки учествуваа бројни обвинители кои се занимаваат со случаи на трговија со луѓе. Понатаму, Академијата за обука на судии, која е дел од Управата на шведските национални судови и е одговорна за судска обука на судиите и другите правници, нуди обука за справување со криминал преку користење на ИКТ на различни нивоа.

- Летонските власти се повикаа на меѓународната обука за трговија со луѓе и компјутерски криминал организирана од полското обвинителство и обезбедена за обвинителите кои се специјализирани за организиран криминал (21-23 октомври 2019 година во Краков).

Конечно, неколку земји ја истакнаа важноста од унапредување на обуката на судиите и обвинителите во однос на електронските докази.

КВАДРАТЧЕ | Обука за НВО

Невладините организации обезбедуваат клучна обука и експертиза врз основа на нивното секојдневно искуство преку помагање и советување на жртвите – вклучително и на органите на прогонот и ризичните заедници и поединци. Сепак, тие ја изразија потребата од добивање на обука од самите органи на прогонот и меѓународните организации во врска со најновите случувања и во технолошкото опкружување како и во поглед на трговијата со луѓе, вклучително и промените во стратегиите за регрутирање.

Тие, исто така, ја истакнаа потребата од обука во врска со најдобрите практики и споделување искуства меѓу земјите. Ова е особено важно за дизајнот и координацијата на кампањите кои ги вклучуваат и земјите на потекло и дестинација.

Додека некои невладини организации имаат специјалисти за прашањата поврзани со онлајн безбедноста, генерално сè уште постои недостигот од обука во врска со технологијата, вклучително и употребата на специфични алатки за идентификување и помош на жртвите. Како што е посочено од Ла Страда Интернешнал, ова е „поради недостатокот на ресурси и капацитет", бидејќи „веќе е тешко да се добијат доволно средства за основните програми за поддршка".

5. Правни инструменти

Ова поглавје ги истражува меѓународните правни инструменти кои се важни во борбата против онлајн трговијата со луѓе преку користење на ИКТ. Прегледот на правните рамки за конкретна земја поврзани со идентификацијата и отстранувањето на содржините поврзани со ТЛ, како и на домашните правни инструменти релевантни во борбата против ТЛ генерално е достапен во веб-додатокот.

5.1. Меѓународни правни инструменти

Земјите-членки идентификуваа голем број правни инструменти како релевантни за борбата против ТЛ преку користење на ИКТ. Повеќето инструменти се општи и насочени кон справување со ТЛ без оглед на *начинот на делување* на трговците со луѓе. Најрелевантниот инструмент насочен кон кривичните дела направени преку користење на ИКТ е Конвенцијата од Будимпешта (компјутерски криминал) на СЕ, која неколку земји-членки ја наведуваат како „важна" алатка. Со оглед на нејзината важност, употребата на Конвенцијата за компјутерски криминал во контекст на ТЛ е дискутирана во посебен дел даден во продолжение. Дополнителни инструменти идентификувани од земјите-членки се следните:

• Конвенција на ОН против транснационалниот организиран криминал и нејзиниот протокол за спречување, сузбивање и казнување на трговијата со луѓе, особено жени и деца (2000)
• Европската конвенција за екстрадиција на СЕ (ЕТС бр. 024)
• Европската конвенција на СЕ за заемна помош во кривичната материја (ЕТС бр. 030)
• Конвенција на СЕ за акција против трговијата со луѓе (КЕТС бр. 197)
• Директива 2011/36/ЕУ на Европскиот парламент и на Советот од 5 април 2011 година за спречување и борба против трговијата со луѓе и заштита на нејзините жртви
• Акт на Советот од 29 мај 2000 година со кој во согласност со член 34 од Договорот за Европската унија се воспоставува Конвенцијата за заемна помош во кривичната материја меѓу земјите-членки на Европската унија.

За прашања поврзани со сексуална злоупотреба на деца:

- Конвенција на Советот на Европа (СЕ) за заштита на децата од сексуална експлоатација и сексуална злоупотреба (Конвенција од Ланзароте, КЕТС бр. 201)
- Директива 2011/93/ЕУ на Европскиот парламент и на Советот од 13 декември 2011 година за борба против сексуалната злоупотреба и сексуална експлоатација на деца и детска порнографија
- Одлука на Советот на Европската Унија од 29 мај 2000 година за борба против детската порнографија на Интернет 2000/375/ПВР.

За трудова експлоатација:

- Меѓународна организација на трудот, Конвенција бр. 189 и Препорака бр. 201 Во врска со пристојната работа за домашните работници, 2011 г.

- Меѓународна организација на трудот, Протокол од 2014 година кон Конвенцијата за принудна работа, 1930 година.

Дополнително, земјите-членки идентификуваа голем број меѓународни агенции и програми кои се инструментални за унапредување на меѓународната правна соработка, исто така во контекст на ТЛ преку користење на ИКТ. Тие вклучуваат:

- Интерпол
    - Проект IWOL (блокирање на домени поврзани со сексуална експлоатација на деца)
- Европол
    - EMPACT (ТЛ)
    - Денови на заедничка акција
- Европравда
- Селек (Центар на органите на прогонот во Југоисточна Европа).

Конечно, збир на специфични оперативни инструменти кои произлегуваат од доказите доставени од земјите-членки. Овој збир ги вклучува следните инструменти:

- Барања за правна помош
- Европски налог за апсење
- Европски налог за истрага
- Заеднички истражни тимови
- EU Prüm систем (размена на национална ДНК, отпечатоци од прсти и податоци за регистрација на возилото)
- Евиденција на имиња на патници во ЕУ (PNR)
- Европол СИЕНА
- Службеници за врски
- Систем за известувања од Интерпол.

5.1.1. Недостатоци во сегашната рамка

Генерално, земјите-членки изразија позитивен став и поддршка за достапните правни инструменти кои овозможуваат соработка меѓу земјите во борбата против ТЛ. Конвенциите на СЕ за (а) меѓусебна правна помош и (б) компјутерски криминал се сметаат за меѓу „најчесто" користените инструменти и, генерално, тие се оценети како „соодветни". Сепак, земјите-членки идентификуваа некои потенцијални недостатоци и области во кои сегашното законодавство може да се подобри. Ве молиме имајте предвид дека овие недостатоци ги рефлектираат – и ги надополнуваат – предизвиците поврзани со истрагата и гонењето на ТЛ преку користење на ИКТ, веќе дискутирани во Поглавје 1 – и треба да се читаат заедно со таквата анализа.

Главните недостатоци идентификувани од земјите-членки се однесуваат на:

- Отсуство на заедничко договорено (стандардизирано) правно опкружување кое ја поткрепува размената помеѓу давателите на интернет услуги и властите кога се занимаваат со конкретни истраги.

- Одредби кои овозможуваат навремен одговор од приватните компании на барањата за податоци за да се избегнат долги одложувања во обезбедувањето на таквите податоци. Сепак, таквите одредби треба да имаат предвид дека многу тесните временски рамки може да ги „казнат„ (да им бидат на терет) малите даватели на услуги во корист на големите даватели на услуги, бидејќи тие можат полесно да си дозволат скапи автоматизирани системи и/или услуги на повик (како што е нагласено од швајцарските власти).

- Одредби со кои приватните компании ќе се натераат да откриваат информации по директно барање/налог од друга земја.

- Одредби за примена на споделени правила за чување на податоците.

- Одредби за олеснување на сведочењата на жртвите и нивната употреба во друга земја. Ова би ги ублажило тешкотиите со кои се соочуваат земјите во убедувањето на жртвите да сведочат на суд од мноштво причини, вклучувајќи ја мобилноста на жртвите, тешкотиите во нивното лоцирање и континуираната ранливост.

- Одредби околу шифрирањето (на пр., давателите на услуги не се обврзани да го отстранат шифрирањето кога ги предаваат материјалите на властите).

- Прашања околу транснационалните мерки за веб-страниците кои поставуваат/хостираат материјали кои може да доведат до експлоатација на жртвите. Ова е особено сложено прашање кое е тесно испреплетено со разликите меѓу земјите-членки во нивниот пристап кон регулирање на проституција и различните [правни] режими усвоени во различни земји.

- Одредби кои воведуваат должност на будност од страна на компаниите во целиот нивен синџир на снабдување, насочени кон, на пример, употребата на ИКТ во контекст на вработување (пример за тоа е францускиот Закон бр. 399/2017 за должноста за будност како и Законот против ропство на Обединетото Кралство од 2015 година со кој се воведува должност за транспарентност во синџирите на снабдување).

- Употреба на терминологија која не секогаш дозволува законодавството да се развива паралелно со промените во *modus operandi* на трговците со луѓе.

- Разлики во транспонирањето на делото за ТЛ (според Протоколот од Палермо) во домашните законодавства. Овие разлики може да претставуваат предизвици за меѓународната соработка, на пример околу прашања поврзани со недостаток на согласност и принуда на жртвата.

- Европскиот налог за апсење се смета за вредна алатка; сепак, некои релевантни земји на потекло често се надвор од судската рамка на ЕУ.

- Европските истражни налози (EIOs) може да немаат флексибилност, на пр. може да има потреба од нов EIO ако истрагата зема нови насоки и може да им треба долго време на одговор.

- Заедничките истражни тимови (ЗИТ) се сметаат за „ефективни" средства; сепак, тие можат да бидат (а) сложени за спроведување; и (б) да изискуваат истрага во партнерските земји.

5.2. Конвенцијата од Будимпешта (компјутерски криминал) и борбата против ТЛ преку користење на ИКТ

Постои широк консензус меѓу земјите-членки за вредноста на Конвенцијата за компјутерски криминал – при што многу земји ја посочуваат како „многу вредна алатка". Неколку земји-членки ја сметаат Конвенцијата за компјутерски криминал како **клучна алатка за поддршка** во борбата против ТЛ преку користење на ИКТ.

Според доставените докази, земјите-членки ги сметаат одредбите поврзани со **процесното право** како највредни во контекст на извршување ТЛ со употреба на ИКТ (Поглавје II, Дел 2 од Конвенцијата), а не материјалните казнено-правни мерки предвидени во Поглавје II, Дел 1. Клучно е тоа што делокругот на одредбите од процесното право не зави од извршувањето на кривичното дело наведено во Дел 1 од Поглавје II. Случаите на ТЛ преку користење на ИКТ, веројатно потпаѓаат или под „кривични дела извршени со помош на компјутерски систем" или, барем, дела за кои е потребно „собирање докази во електронска форма" (член 14, став 2). Слично на тоа, Членот 23 наведува дека начелата на меѓународната соработка во контекст на Конвенцијата се применуваат на „истраги или постапки во врска со кривични дела поврзани со компјутерски системи и податоци, *или* за собирање докази во електронска форма на кривично дело" (курзивот е додаден). Земјите-членки ја истакнаа **важноста на неограничувачките процедурални мерки за кривичните дела кои се експлицитно наведени** (на пример, оние во Поглавје II, Дел 1). Сепак, се чини дека не сите земји се согласуваат со ова пошироко толкување на опфатот на Конвенцијата.

Конвенцијата јасно го постигнува својот целосен потенцијал само кога не е ограничена на кривичните дела кои се експлицитно наведени во Поглавје II, Дел 1. Ова е особено точно во контекст на ТЛ преку користење на ИКТ. Како што е наведено од финските власти, меѓу другото, „суштинските казнено-правни одредби од Конвенцијата од Будимпешта [кои] опфаќаат кривични дела преку користење на компјутер, како што се нелегален пристап, пречки во податоците, компјутерско фалсификување и повреда на авторските права и други слични прекршоци, само ретко или воопшто не се релевантни во контекст на ТЛ". Напротив, неколку земји-членки посочија дека се потпираат на одредбите на Конвенцијата за зачувување на податоците во контекст на истрагите за трговија со луѓе (особено членовите 16-21).

Неколку земји ја посочија корисноста на одредбите вклучени во Поглавје III од Конвенцијата (за меѓународна соработка) како правна основа за собирање и споделување електронски докази помеѓу земјите. Механизмите за взаемна помош предвидени со Поглавје III од Конвенцијата (членови 29-34) се сметаат за „корисни". Неколку земји експресно посочија дека претходно се потпирале на нив. Членовите 29 и

31 имаат добиено најмногу референци; членот 30 не е експлицитно споменат во поднесоците, сепак, може да понуди корисна алатка во контекст на ТЛ преку користење на ИКТ.

Воспоставувањето на 24/7 **мрежа на контакт точки** (член 35) исто така се смета за важна одредба, особено во контекст на собирање електронски докази. Меѓутоа, клучно е контакт точките да бидат лесно достапни од секоја земја. Ова зборува за **прашањето на кочниците во системот**. Каде се наоѓа контакт точката во системот на кривичната правда е клучно – а тоа може навистина да предизвика последици. Се применуваат различни модели. Во Република Молдавија, на пример, таквата контакт точка се наоѓа во рамките на Дирекцијата за истраги на компјутерски криминал; во Малта во Полициската единица за компјутерски криминал, а во Полска, во Бирото за борба против компјутерски криминал на Националната полициска команда. Во Франција, таа е во Централната канцеларија за борба против криминалот преку користење на информатичката и комуникациската технологија (OCLCTIC), додека во Летонија таквата контакт точка е лоцирана во Одделот за меѓународна соработка на државната полиција. Властите во Босна и Херцеговина експлицитно го спомнаа нивното „многу позитивно искуство" кое произлегува од фактот што контакт точката 24/7 „не се наоѓа во единицата за справување со компјутерски криминал". Во иднина, најверојатно е дека, со сè поцентралната улога што ја играат ИКТ и електронските докази, таквите контакт точки ќе бидат под зголемен притисок - и брзо ќе бидат преоптоварени ако не се екипирани со соодветен персонал. Можеби ќе се претпочитаат самостојни единици за поддршка наместо единиците за компјутерски-криминал – идеално екипирани со персонал кој поседува експертиза во различни области и видови криминал, вклучително и трговија со луѓе преку користење на ИКТ. Сепак, без оглед каков модел ќе се избере, земјата треба да го земе предвид прашањето за кочници.

5.2.1. Идни чекори: како Конвенцијата за компјутерски криминал може дополнително да се користи за борба против ТЛ

Неколку земји ја истакнаа важноста на Вториот дополнителен протокол на Конвенцијата. Во неколку поднесоци беше посочено дека Вториот дополнителен протокол ќе создаде вредни алатки за органите на прогонот - кои ќе се користат и во контекст на ТЛ преку користење на ИКТ - за подобрување на прекуграничните кривични истраги и дополнително подобрување на соработката во врска со обезбедувањето електронски докази. Членовите кои се нагласени како особено релевантни вклучуваат одредби поврзани со заеднички истраги, вклучително и заеднички истражни тимови; забрзано откривање на складирани компјутерски податоци; итна меѓусебна помош и директно откривање на информации за претплатниците.

Понатаму, земјите-членки ги предложија следните активности за подобрување на борбата против ТЛ преку користење на ИКТ, преку употреба на Конвенциите за компјутерски криминал:

- Целосно усогласување на сите национални законодавства со Конвенцијата за компјутерски криминал за да се искористи целосниот потенцијал што го нуди Конвенцијата.

- Поширока и подобрена обука за можностите што ги нуди Конвенцијата за компјутерски криминал. Од поднесоците произлегува дека не сите земји-членки во моментов ги користат алатките од Конвенцијата со целосен потенцијал.

- Повеќе јасност за опфатот на процедуралните одредби веќе вклучени во Конвенцијата и нејзините дополнителни протоколи, земајќи го во предвид степенот на несогласување помеѓу земјите-членки за тоа до каде сегашните одредби може да се применат за случаите на ТЛ. Додека некои земји-членки се на став дека се додека станува збор за електронските докази, Конвенцијата за компјутерски криминал може целосно да се примени, други предупредуваат дека употребата на Конвенцијата и протоколите, вклучително и Вториот дополнителен протокол, бара „погодни случаи" (што го прави предметот „погоден" не е наведено во поднесоците).

- Некои земји-членки изразија став дека Вториот дополнителен протокол треба да вклучи одредби за зајакнато споделувањето електронски докази, подобрување на модалитетите на меѓусебна правна помош, поттикнување соработка со давателите на интернет услуги и подобрување на прекуграничниот пристап до податоци.

- Помал број на земји-членки имаат став дека Конвенцијата за компјутерски криминал треба да се дополни или измени за експлицитно да го вклучи ТЛ во нејзиниот опфат. Бугарските власти ја изразија потребата од изработка на „каталог на кривични дела" на кој може да се применат алатките вклучени во Конвенцијата за компјутерски криминал и дополнителните протоколи. Сепак, се чини дека ова гледиште не е широко споделено меѓу земјите-членки, бидејќи изгледа постои преференца за поширок толкување на опсегот на Конвенцијата врз основа на (опсежните) барања за „собирање докази во електронска форма" (види исто така погоре).

- Словачките власти предложија спроведување на постапка за забрзување на обезбедувањето МПП преку создавање можност за испраќање на барање директно до субјект кој се наоѓа под јурисдикција на странска земја, под услов да е известен судскиот орган на таа земја.

КВАДРАТЧЕ | Предизвици идентификувани од НВО

Општо земено, невладините организации се на став дека предизвиците најчесто се последица на имплементацијата на тековните одредби, и произлегуваат од недостигот на ресурси на располагање на органите на прогонот и на организациите за поддршка а не од текстот на важечките законски одредби.

Ла Страда Интернешнал забележа **„јасни ограничувања" воведени со законодавството за заштита на податоците (GDPR) и правилата за приватност**. Пример е „законодавството за е-приватност предложено од ЕУ кое ги спречува технолошките компании да вршат скенирање поврзано со сексуалната експлоатација на деца онлајн" (сега привремено суспендирано по противењето на многу граѓански организации). Фондацијата Састејнабле Рескју [Sustainable Rescue Foundation] укажа на „јасна транзиција од физички докази кон дигитални податоци" што создава потреба од „дигитална форензика како прифатлив доказ за полицијата и обвинителството" во сите јурисдикции. Понатамошните предизвици што ги идентификуваа се однесуваат на GDPR на ЕУ; ажурирање на прописите и судската пракса за да се земат предвид компјутерскиот криминал и интернетот; осмислување на законодавството и оперативните правила прилагодени на дигиталните истраги.

Фондацијата Састејнабле Рескју, исто така, предложи да се разгледа законодавството од аспект на финансискиот криминал како решение за проблемот со претворање на информациите во прифатливи докази. На пример, јужноафриканските интегрирани наменски сили за спречување на перење пари, кои се партнерство помеѓу јавните субјекти и финансискиот сектор, може да поднесат барање за судски налог со кој се овластува пристап до релевантни информации што ги поседуваат финансиските и другите институции. Преку заверка овие информации (т.е. финансиската анализа на судски добиените финансиски информации) потоа може да се користат од страна на органите на прогонот.

6. Човекови права, етика и заштита на податоците

6.1. Доказ од земјите-членки

Во однос на **обработката на податоците и заштитата на податоците**, сите земји-членки го истакнаа усвојувањето на Законите за заштита на податоците - често усогласени со Регулативата на ЕУ 2016/679 на Европскиот парламент и на Советот од 27 април 2016 година (исто така наречена Европска Генерална регулатива за заштита на податоци: GDPR) и/или Конвенцијата на СЕ за заштита на поединци во однос на обработката на личните податоци (ЕТС бр. 108, повторно разгледана во 2018 година како верзија 108+). Принципите зад заштитата на податоците се слични кај земјите-членки. Тие вклучуваат законитост, ограничување на целта, минимизирање и пропорционалност на податоците, точност, ограничување на складирањето, интегритет и доверливост. Не е можно да се спроведе евалуација на имплементацијата на таквите принципи врз основа на доказите дадени во одговорите на прашалникот.

Во однос на **човековите права** и **личната заштита на жртвите**, голем број земји го истакнаа воведувањето на мерки за спречување на сторителите да стапат во контакт со жртвите; испрашувањето на сведоци преку видеоконференциска врска за да се спречи контакт со обвинетите; а во некои случаи и можноста жртвите анонимно да даваат докази пред суд за да се заштитат. Жртвите може да бидат сместени во **засолништа** и да им се пружи **помош**.

Во Франција, корисниците на платформата за пријавување сексуално и родово насилство треба да се **согласат на собирање лични податоци** кога првпат ќе се поврзат на платформата. Оваа согласност се обновува во текот на разговорот. Сепак, не е задолжително да се обезбеди нечиј идентитет за да се пристапи до просторијата за разговор (chatroom) – на тој начин дозволувајќи анонимни контакти.

Што се однесува до **податоците собрани за време на полициската работа**, вклучително и истрагите, земјите-членки истакнаа дека законите и прописите вообичаено пропишуваат дека таквите информации се предмет на доверливост и може да се споделуваат само под многу ограничени околности под строги процедури и овластувања. Земјите-членки посочија дека правилата според кои полициските сили можат да регистрираат податоци во специфични бази на податоци се вообичаено усогласени со полициската директива на ЕУ. Поединечни земји може да имаат построги национални барања. Како што истакнаа норвешките власти, посебните категории на лични податоци, на пр., за сексуалната ориентација, религијата и политичките ставови, може да подлежат на дополнителни барања и „може да се обработуваат само кога е „строго неопходно" за дефинирани цели". Нормално, истите правила и заштитни мерки се однесуваат на сите истраги и разузнавачка работа, вклучително и оние кои вклучуваат ТЛ преку користење на ИКТ. Од клучно значење е персоналот на органите на прогонот да биде соодветно обучен за регулаторните и етичките одредби кои ја регулираат обработката на личните податоци.

Полициската работа исто така треба да ги **балансира различните потреби и права**. На пример, како што забележаа финските власти, наредбата за ограничување на пристапот до електронската комуникација „може да се издаде само ако придобивките од забраната за пристап до информации може да се сметаат за значително поголеми од

ограничувањата на слободата на изразување и другите основни права на корисниците на мрежата" (член 185 од Законот за електронски комуникациски услуги 917/2014). Дополнително, мора да биде „технички имплементирана на таков начин што заштитата на доверливоста на комуникациите нема да биде загрозена". Поопшто, членот 226в од истиот закон пропишува дека „мерките поврзани со условите за користење на платформите за споделување видеа треба да бидат пропорционални со природата на предметната содржина и да ги земат предвид на пример потенцијалната штета и правата на давателите на услуги и корисниците". Финското Национално биро за истраги идентификуваше проблеми со доверливоста/приватноста на бирото во врска со употребата на техничките алатки кои се дадени за надворешна примена и тоа го има пријавено до Националниот полициски одбор.

Земјите-членки наведоа дека имаат воспоставено **протоколи согласно возраста**, кои се однесуваат на различни групи процедури и заштитни мерки кои се применуваат во зависност од тоа дали жртвата е дете. На пример, децата обично се сместени во посебни центри за поддршка; се користат различни техники и простории за испрашување, често со присутни психолози. Во некои земји, кривичните постапки во кои се вклучени деца се водат исклучиво од полициски службеници специјално обучени за работа со деца и малолетници.

6.2. Докази од невладини организации

Невладините организации ја истакнаа важноста и свесноста за правилата за заштита на податоците, доверливоста, безбедното складирање, како и процедурите околу добивање согласност.

Доказите од неколку невладини организации укажуваат дека, како стандардна процедура, организациите бараат согласност од жртвата пред да споделат информации со органите на прогонот. Како што е нагласено од страна на ФИЗ (Швајцарија), оваа согласност се однесува за споделување детали за SIM картичките и ингеренциите на социјалните мрежи. Ла Страда Интернешнал изјави дека сите нивни членови „не даваат никакви информации на полицијата без согласност на жртвата, освен ако има опасни ситуации каде што е итно потребна акција". Предизвикот се јавува кога жртвите не сакаат да поднесат жалба до полицијата „како резултат на ризиците кои ќе произлезат од тоа, вклучувајќи ги и ризиците нивната ситуација да им стане позната на другите, покрај ризиците од одмазда". Ла Страда Интернешнал проценува дека ова е случај со „многу жртви на трговија со луѓе".

Различни и еднакви (Албанија) ја спомена употребата на безбедносни протоколи во секоја комуникација со органите на прогонот, вклучително и шифрирањето. Внатрешните протоколи се изградени земајќи ја предвид потребата за зачувување на доверливоста на жртвите и заштита на нивните податоци. Слично на тоа, ФИЗ (Швајцарија) ја нагласи потребата од заштита на доверливоста на податоците како услов за добра соработка со органите на прогонот. Астра (Србија) истакна дека **доверливоста на жртвите** е „клучен дел од нашата работа" и откажувањето од неа „не е и не смее да биде услов за добивање поддршка и помош". КОК (Германија) истакна дека „заштитата на поединецот е поприоритетна од потребата за собирање докази". Праксис (Грција) остана на ставот дека, кога се споделуваат информации со органите на прогонот во рамките на правилата за заштита на податоците (споделување врз основа на согласност), нивната „примарна грижа секогаш е непосредната и ефективна заштита на потенцијалната жртва".

Прашањата за заштита на податоците и споделување на податоци може да генерираат **морални дилеми**. Како што посочи Ла Страда Интернешнал, споделувањето на податоци со органите на прогонот и поднесувањето жалби им помага на истрагите, кои пак потенцијално можат да спасат и заштитат повеќе жртви во иднина. Сепак, за тоа цената може да ја плаќа самата жртва, која може да биде изложена на ризици и закани, вклучително и социјална исклученост. Понатаму, може да има прашања поврзани со долгорочниот ефект од регистрирањето на жртвата и споделувањето на личните податоци, вклучително и потенцијално гонење и казнување од страна на властите (ова може да се влоши кога жртвата има нерегулиран престој во земјата во времето на регистрација). И Ла Страда Интернешнал и Ла Страда Молдавија сметаат дека изнаоѓањето на вистинска рамнотежа помеѓу потребите не жртвата од доверливост при добивањето на услугите како и потребата од собирање на докази во поддршка на борбата против ТЛ во поширок рамки може да биде „многу голем предизвик". Ова станува уште поакутно кога жртвата е дете: како што забележува Ла Страда Молдавија, децата често се плашат да дадат согласност и да пополнат формална жалба до полицијата, вклучително и поради стравот од реакцијата на нивните родители.

Според Ла Страда Интернешнал, правилата за заштита на податоците „го отежнаа споделувањето податоци меѓу невладините организации и другите релевантни засегнати страни". Во исто време, невладините организации се свесни дека може да биде тешко за „жртвите на ТЛ или ризичните групи да знаат кои податоци се зачувуваат и/или да се погрижат податоците да се корегираат, бришат, блокираат или избришат и да го искористат ова право", и покрај тоа што постојат протоколи за заштита на податоци.

Дополнителни проблеми произлегуваат од собирањето лични информации што може да се идентификуваат преку **техниките за извлекување податоци**. Састејнабл рескју фаундејшн (СРФ) се осврна на два одделни проекти кои моментално се спроведуваат во Холандија: РИВЕТ (СРФ) и *Ловитура 10 Еленас* (холандска полициска лабораторија). И двата проекта се фокусираат на трговија со Романки во Холандија за сексуална експлоатација. СРФ РИВЕТ користи екстракција на податоци насочена кон жртвите врз основа на интервјуа со 10 романски сексуални работнички и ја истражува употребата на технологија за откривање, собирање, чистење и анализа на податоци во насока на систематизирање на *modus operandi*. *Ловитура 10 Еленас* дигитално следи десет романски сексуални работнички за да разбере како функционираат криминалните мрежи. Како што беше посочено од РСФ, предизвикот е „како да се погрижиме сите романски сексуални работнички кои учествуваат во двата проекта да останат анонимни". Засолништата сакаат да ја заштитат анонимноста на сексуалните работнички и полицијата не може да ја сподели нивната оперативна база на податоци. СФР предложи споредба на податоци од повеќе страни како можно решение. Овој пристап се состои во анонимизирање на податоците што доаѓаат од различни збирки на податоци (на пр., НВО и полиција) на таков начин што тие потоа може да се споделат и читаат од различни системи за да се проверат, на пр., дали има дупликати на имиња.

Ла Страда Интернешнал повика на поголемо внимание во врска со потенцијалните ризици и штети генерирани од (во голем обем) собирањето на податоци и технолошки алатки, предупредувајќи дека, во моментот, фокусот е само „на позитивните аспекти и можности" на таквите алатки. Истата организација, исто така, тврди дека „потребна е поголема контрола врз користењето на податоците и безбедното складирање и обезбедување на ефективно почитување на сите правила за заштита на податоците". Жртвите, ризичните групи и невладините организации треба да имаат „повеќе можности

[…] да ги отфрлат барањата за податоци и да го минимизираат собирањето на податоци".

Невладините организации имаат тенденција за поседување на различни протоколи врз основа на тоа дали жртвата е дете или возрасен (**протоколи согласно возраста**).

6.3. Дополнителни докази од анализата на состојбата

ИКТ може да има значително влијание врз **човековите права** на поединците, вклучувајќи ги правата на приватност, слобода на изразување и слобода од дискриминација. Во литературата се покренати голем број прашања.

Според ОБСЕ (2020), можеме да наведеме бројни **етички прашања** што треба да се земат предвид при развивање технологија за борба против трговијата со луѓе. Тие вклучуваат: (а) заштита на приватноста на податоците; (б) протоколи за согласност потпишани од жртвите; (в) обука за луѓе кои ракуваат со чувствителни податоци, особено со податоци за жртвите; (г) безбедно складирање на податоците; (д) спречување на употребата на технологија за добивање чувствителни податоци за ранливите лица (сеопфатно собирање податоци за ранливите или маргинализираните популации, создавање ризици од дискриминаторски практики); и (ѓ) користење на технологијата на начин што не ги нарушува човековите права на жртвите, како и на оние на општата популација. ICAT (2019) исто така ги нагласува прашањата поврзани со **приватноста на податоците, етиката, транспарентноста, одговорноста и информираната согласност**. Тие ја нагласуваат потребата од гарантирање дека податоците се чуваат безбедно; дека се воспоставени протоколи за согласност; и дека се родово сензитивни и усогласени со возраста на жртвите. Понатаму, информациите објавени од органите на прогонот треба да се проценат со цел жртвите и нивните семејства да не бидат изложени на ризик.

ICAT (2019) и други извори укажаа на чувствителноста околу **споделувањето на податоци**. Кога податоците се споделуваат помеѓу земјите и/или релевантните агенции, тоа треба да се направи во согласност со принципите на приватност и доверливост. Забележано е дека може да настане потенцијален конфликт помеѓу потребата за доверливост кога жртвите пристапуваат до услугите и добиваат поддршка од една страна, и потребата за информации/докази за да се изгради ефективна истрага од друга страна. Гери и др. (2016) ја нагласија важноста на клучните правни принципи - принципите на правична информација - во врска со обработката на личните податоци (тука е вклучен и принципот на ограничување на целта). Се сугерира дека ваквите принципи остануваат важни и кога станува збор за трговија со луѓе, а особено во однос на жртвите.

Гери и др. (2016) исто така предупредуваат за ризикот од широко распространетите **алатки за следење** во борбата против трговијата со луѓе. Иако таквата технологија може да понуди нови можности за интервенирање во ситуации на трговија со луѓе, таа исто така се состои од **форма на надзор што е потенцијално многу инвазивна** за приватноста на една личност. Како што пишуваат тие, „може да открие многу информации во врска со нивниот личен живот, вклучително и нивната припадност кон одредена религија, воспоставувањето на лични односи и поврзаноста со други поединци, како и нивните секојдневни навики", со што ги става ранливите групи во ризик од дискриминација и профилирање. Сеопфатното следење на целото ризично население, на пр. групите на мигранти, може да има сериозни последици врз

приватноста на поединците. Гери и др. (2016) ја нагласуваат потребата од развивање на **механизми за утврдување дали технологијата за следење не се користи прекумерно или се злоупотребува**. Тие предлагаат да се избегнуваат системи кои вклучуваат централизирано складирање на лични податоци на жртвите или потенцијалните жртви. Поопшто, алатките кои се потпираат на технологија за борба против трговијата со луѓе треба **да се развијат и да се користат одговорно и етички**. Ваквите барања треба да се земат предвид во сите фази, од развојот до конечната употреба. Решенијата кои се потпираат на технологија, исто така, треба да се проценат според нивното ниво на инвазивност во приватноста на луѓето. Некои научници, меѓу кои и Миливојевиќ и др. (2020), предупредија за потенцијалните негативни последици од преголемата употреба на техники за препознавање на лица од маргинализираната популација, и поопшто за она што тие го дефинираат како „морален императив за „заштита и спасување"". И покрај фактот што тие го препознаваат потенцијалот на технологијата во насока на обезбедување поддршка во борбата против трговијата со луѓе, исто така ја истакнуваат важноста од ставањето на **најдобрите интереси на жртвите** во центарот на секое делување.

Неколку извори, меѓу кои и Миливојевиќ и др. (2020) и Гери и др. (2016), ја истакнаа важноста од **неисклучувањето на жртвите од технологијата**, бидејќи пристапот до технологијата може да биде нивниот единствен начин на комуникација со надворешниот свет и може да послужи како важен механизам за справување. Отстранувањето на пристапот до технологијата може да ги обесхрабри жртвите; Наместо тоа, треба да се даде предност на безбеден пристап до технологијата.

Конечно, во литературата **не се препознава доволно родовата сензитивност**. Препознаен е фактот дека видот на експлоатација е родово-сензитивен, при што жените почесто се експлоатирани за сексуални услуги, домашна работа и лична нега, а мажите почесто се експлоатирани во земјоделството, градежништвото и други мануелни занимања (на пр. продавници, перење автомобили) . Понатаму, се чини дека онлајн грумингот е повеќе поврзан со женските жртви отколку со машките жртви; сепак, доказите, исто така, сугерираат дека може да има и други ранливости во случај на онлајн груминг, на пример, лице кое е во установа во која се обезбедува нега (прелиминарните докази од Романија се вклучени во Ди Никола и др. 2017 година).

Препораки

Активности за подобрување на откривањето на случаи на трговија со луѓе преку користење на технологија

1. Органите на прогонот треба да инвестираат во градење на капацитети во областите на **следење на интернет, компјутерски патроли, тајни онлајн истраги (компјутерски инфилтрација), употреба на OSINT од специјализирани службеници, анализа на социјалните мрежи** и употреба на **алатки за автоматско пребарување** за анализа на докази. Развојот и употребата на таквите алатки мора да се придржуваат до принципите на владеењето на правото. Земјите треба да размислат за прилагодување на постојното законодавство за да се овозможат компјутерско патролирање и тајни онлајн истраги (компјутерски-инфилтрација) - со внимателно разгледување на етичките импликации. Властите, исто така, треба да размислат за инвестирање во алатки кои ќе им помогнат на истражителите при ракување и обработка на масивни податоци (способности за масивни податоци). Ресурсите би можеле да се здружат на наднационално ниво за развој на технолошки производи, како на пример веб-роботи и споделување на експертиза во нивната употреба.

2. Органите на прогонот и трудовите инспекторати треба да применат **построги регулативи и чести контроли на веб-страниците за огласи за вработување**. Ова може да се направи со поддршка на технолошките алатки развиени во соработка со приватните компании (на пр., онлајн алатки за валидација на огласите за работа, алатки за бришење на сајтови за огласите за работа и примена на индикатори за трговија со луѓе). Трудовите инспекторати **треба да развијат дигитална експертиза и да го зголемат своето онлајн присуство**.

3. Земјите/приватните даватели на услуги/НВО-а мора да ги подобрат **онлајн механизмите за доверливо известување**, овозможувајќи анонимно пријавување на случаи на ТЛ, како и самоидентификација на жртвите. Разговорите (chats), вклучително и чет-ботовите, и функциите за инстант пораки може да бидат вредни онлајн алатки. Земјите треба да соработуваат со приватни компании кои нудат онлајн услуги за **дизајни кои би ги оневозможиле трговците со луѓе**, да развијат **аналитика на содржината** за откривање на случаи на трговија со луѓе и да постават лесно достапни механизми за клиентите да ги **означуваат** сомнителните активности/реклами. Онаму каде што е дозволено со домашното законодавство, ова треба да се прошири и на компаниите кои нудат онлајн услуги за возрасни. Онлајн содржините и информациите (на пр. IP адреси) поврзани со означените активности/реклами треба да се чуваат безбедно од страна на компаниите.

Активности за подобрување на истрагата за ТЛ преку користење на технологија

4. Органите на прогонот треба да размислат за обука на службеници специјализирани и за ИКТ и за ТЛ. Земјите, исто така, треба да размислат за создавање **групи за техничка поддршка**, екипирани со полициски службеници кои дале или не дале заклетва со вградени ИКТ способности во единиците за трговија со луѓе. Понатаму, земјите треба да го разгледаат дизајнот на внатрешната **дистрибуција на дигиталните истражни способности** за да ги предвидат и избегнат потенцијалните **кочници во истрагите**. Бидејќи криминалот преку користење на ИКТ, вклучително и ТЛ, веројатно континуирано ќе се зголемува, недостатокот од службеници специјалисти на локално ниво и преголемото потпирање на помош од (зафатените) централизирани единици за компјутерски криминал веројатно ќе создадат кочници.

5. Органите на прогонот треба да се погрижат **сите службеници** да поседуваат соодветно ниво на експертиза за собирање и ракување со **електронски докази**. Обуката за електронските докази треба да биде составен дел на наставните програми за обука и постојано да се ажурира поради брзото менување на технолошкото и бихејвиоралното опкружување. Бидејќи зачувувањето на електронските докази е клучно за градење силни истраги, и **советниците и лицата од невладините организации кои се непосредно вклучени во работата во првите редови** треба да бидат запознаени со стратегиите за зачувување на дигиталните докази (на пример, со складирање на историите од разговорите (chat history)).

6. Земјите/меѓународните организации треба редовно да спроведуваат **стратешка анализа** за да генерираат знаење за новите трендови во врска со *начинот на делување* на сторителите, како и да бидат во чекор со бихејвиоралните модели на корисниците на

технологијата и технолошкото опкружување кои постојано се менуваат. Врз основа на овие стратешки докази, земјите потоа можат да започнат таргетирани полициски операции, да воспостават договори за соработка, како и да осмислат насочени кампањи за подигање на свеста. Знаењето треба редовно да се шири на национално и наднационално ниво.

7. Земјите треба да ја зголемат прекуграничната соработка преку **рационализирани процедури**, **споделување на најдобрите практики и технологии** (на пример, специјализиран софтвер) и засилена **дисеминација на практични информации** за контакт точките/посветените единици кои служат како „привилегиран контакт" во случајот на случаи на ТЛ, вклучително и ТЛ преку користење на ИКТ. Треба да се охрабри соработката и поддршката помеѓу земјите на дестинација и потекло (на пр., скапата технолошка опрема може да биде достапна само за побогатите земји).

Активности за зајакнување на гонењето на ТЛ преку користење на технологија

8. На обвинителите треба да им се обезбеди специфична **обука** за трговијата со луѓе извршена со употреба на ИКТ, ракувањето со електронски докази и нивно изнесување пред судија/порота. Земјите треба да преземат мерки за **обвинителите да бидат запознаени со процедурите** за барање електронски докази од приватни компании, како и за добивање докази и соработка со други земји во рамките на правната рамка на ЕУ (преку заедничките истражни тимови и европските истражни наредби) и вон правната рамка на ЕУ.

Активности за унапредување на соработката со приватни компании

9. Земјите треба да развијат **процедури за споделување податоци** од компаниите кои поседуваат релевантни податоци и да размислат за развој на **протоколи за соработка** со приватните компании, вклучително и социјалните мрежи и компаниите со голема економија на тезги (gig economy), како и платформите за изнајмување за да се поттикне навременото обезбедување на информации. Ваквите протоколи/процедури треба да ги разјаснат законските барања според кои работат компаниите за ИКТ, интернет провајдерите и поставувачите/хостирачите на содржини; да назначат контакт точка во компаниите; и да разјаснат кои национални агенции се одговорни за кои конкретни активности, на пр. барање докази или отстранување на содржини поврзани со ТЛ. Одбивањето да се споделат докази или да се отстрани содржината поврзана со ТЛ треба да биде навремено, експлицитно и образложено.

Активности за унапредување на меѓународната соработка

10. **Треба да се воспостави понепречен процес за барањата за меѓусебна правна помош (МПП)**, вклучувајќи појасни процедури, зголемена употреба на

подобрени мрежи на контакт точки, вклучувајќи ги контакт точките на европската правосудна мрежа (EJN), и барањата за МПП да бидат јасно поставени и дискутирани од самиот почеток. Земјите треба да се погрижат нивниот персонал да е соодветно обучен да ги обработува МПП, ЕИО и другите меѓународни алатки. Земјите и меѓународните организации треба да развијат **заеднички договорени и прифатени обрасци** во прилог на соработката за олеснување на комуникацијата, намалување на административните оптоварувања и минимизирање на грешките во барањата. Земјите, исто така, треба да развијат употреба на **безбедни форми на електронска комуникација** и да го промовираат нивното усвојување за полесна меѓународна соработка.

Активности за подобрување на обуката

11. Треба да се предвидат **заеднички активности за обука (ЗАО)** за земјите кои систематски се вклучени во заеднички случаи на ТЛ. Транснационалната размена на знаења може да се поттикне преку учество во меѓународна/регионална обука фокусирана на специфични аспекти на истражување на ТЛ преку користење на ИКТ. Таквата обука треба да вклучува студии на случај и сценарија за ТЛ преку користење на ИКТ. На обвинителите и судиите, исто така, треба да им се обезбеди обука за трговија со луѓе и за придружните правни инструменти.

12. НВО-ата треба да добијат обука за најновите случувања и во технологијата и во опкружувањето кога станува збор за трговијата со луѓе, вклучително и промените во стратегиите за регрутирање. НВО-оата треба да бидат во позиција да разменуваат искуства за најдобрите меѓународни практики.

Активности за подобрување на правните инструменти

13. Властите треба да осмислат **заеднички процедури за брза размена на дигитални докази со интернет провајдерите** и треба **повторно да ја проценат должината на обврските за чување на податоци** наметнати на интернет провајдерите (тековните периоди се прекратки со оглед на должината на полициските истраги). Треба да се направат напори да се усвои **заедничка рамка** во однос на обврските за чување на податоци и споделување на електронски докази.

14. За да го искористат целосниот потенцијал што го нуди **Конвенцијата за компјутерски криминал**, земјите треба (а) да ја завршат хармонизацијата на националните законодавства со Конвенцијата; (б) да ја прошират и да ја зајакнат обуката за можностите што ги нуди Конвенцијата, бидејќи не сите земји-членки во моментов ги користат алатките што им се достапни во нивниот целосен потенцијал; (в) да ја подигнат свеста за широкиот опсег на процедуралните овластувања и алатките за меѓународна соработка на Конвенцијата, особено во однос на случаите на ТЛ; и (г) брзо да ги спроведат мерките вклучени во Вториот дополнителен протокол.

15. Земјите треба внимателно да го проценат прашањето каде се наоѓа нивната **контакт точка** (во согласност со Конвенцијата за компјутерски криминал) во рамките на системот на кривичната правда за да се избегнат **кочниците**. Со сè поцентралната

улога што ја играат ИКТ и електронските докази, таквите контакт точки ќе бидат под зголемен притисок и брзо ќе бидат преоптоварени доколку не се екипирани со соодветен персонал. Земјите можат да размислат за екипирање на таквите контакт точки со персонал кој поседува експертиза за различни видови криминал, вклучително и ТЛ преку користење на ИКТ.

16. Земјите надвор од Европа треба да се охрабрат да ги **усвојат клучните меѓународни правни алатки**, како што се Конвенцијата на СЕ за компјутерски криминал и Конвенцијата на СЕ за взаемна помош во кривичната материја, за да се изедначи и унапреди меѓународната соработка.

17. Треба да се зголемат **соработката и синергиите** помеѓу механизмот за следење на Конвенцијата за борба против трговијата со луѓе (ГРЕТА и Комитетот на страните) и Т-CY, на пример, во форма на размена на мислења, како и заедничко градење капацитети за двете конвенции.

Активности за спречување на виктимизацијата и ре-виктимизација

18. Приватните компании, кои работат со властите и невладините организации, треба да го зголемат онлајн социјалното објавување/информирање за да се спречи виктимизацијата и да се подобри откривањето на ТЛ преку користење на технологијата. Земјите треба да ги зголемат напорите за да ги информираат поединците за нивните работнички права на јазик што го разбираат, во соработка со невладините организации и со компаниите кои обезбедуваат услуги за поставување/хостирање на огласи за вработување. Влијанието на кампањите треба рутински да се оценува.

19. Земјите, невладините организации и приватните компании кои обезбедуваат онлајн и ИКТ услуги треба да преземат иницијативи за **подигање на свеста за ризиците поврзани со технологијата, вклучително и како трговците со луѓе би можеле да ја искористат технологијата** и како може да започнат потенцијални експлоататорски ситуации. Училиштата и воспитувачите треба да бидат дел од овој напор, бидејќи децата и младите се изложени на зголемени ризици. Земјите и невладините организации треба да соработуваат со приватни компании кои нудат услуги за комуникација и пораки за да дизајнираат информации/предупредувања во системот за **безбедно користење на приватните канали за комуникација**.

20. НВО треба да понудат обука за техники на заштита на податоците и безбедно користење на технологијата како дел од **програмите за заштита и реинтеграција на жртвите**. Жртвите не треба да бидат исклучени од технологијата со што би се добил обратен ефект од посакуваниот.

Вкрстени активности

21. Земјите треба да вклучат технолошка стратегија во нивните **национални акциски планови** за борба против трговијата со луѓе.

Анекс 1 | Создавање на база на докази за онлајн ТЛ преку користење на ИКТ: Список на извори

Базата на докази е изградена врз основа на широко истражување на состојбата кое опфаќа различни извори, вклучувајќи: (а) меѓународни организации; (б) академска средина; (в) избрани национални известувачи; (г) НВО и добротворни организации; (д) приватен сектор. Вкупно 62 резултати се идентификувани како релевантни за целите на оваа работа. Резултатите кои беа разгледувани го опфаќаат периодот 2003 – 2020 година, сепак најголемиот дел од нив беа објавени од 2015 година наваму, а 22 беа објавени во последните три години. Сите разгледувани резултати се напишани на англиски јазик (со еден исклучок: француската верзија на извештајот изработен од Мирја, белгискиот „*Centre fédéral Migration*").

Меѓународни и национални организации

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). 9th General Report on GRETA's Activities.

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. OCSE (2020). Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools. OCSE 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

Академска средина

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, pp. 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. In: 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, funded by European Commission.

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, online at: 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.
НВО/добротворни/приватен сектор

НВО/добротворни организации/приватен сектор

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.

Веб-страници

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

60. The Counter Trafficking Data Collaborative: https://www.ctdatacollaborative.org/ (IOM, Polaris and 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. The Alliance 8.7 Knowledge Problem: https://delta87.org/ (Global knowledge platform exploring what works to eradicate forced labour, modern slavery, human trafficking and child labour, Target 8.7 of UN SDGs)

Анекс 2 | Прашалник за земјите-членки

Дел 1. Влијанието на ИКТ врз ТЛ

1. Врз основа на докази од вашата земја, би можеле ли да дадете примери за начините на кои ИКТ се користат од престапниците во контекст на ТЛ за сексуална експлоатација? (За секој пример, наведете детали за начинот на делување на трговците со луѓе и видот на користената технологија, на пр. Интернет, одредени веб-страници, социјални медиуми, апликации).

2. Слично на тоа, би можеле ли да дадете примери за начините на кои ИКТ се користи од страна на сторителите во контекст на ТЛ за трудова експлоатација? (За секој пример, ве молиме наведете детали за начинот на делување на трговците со луѓе, типот на технологија што се користи, на пр. Интернет, конкретни веб-страници, социјални медиуми, апликации *и* економскиот сектор во кој се врши експлоатација).

3. Кои се новите трендови во вашата земја во однос на употребата на ИКТ во ТЛ (нови видови технологија, нов начин на работа, нови видови на експлоатација...)? Дали идентификувавте нови онлајн практики кои може да го зголемат ризикот за станување на жртва на ТЛ (и за сексуална и за трудова експлоатација)?

4. Дали DarkWeb игра некаква улога во ТЛ во вашата земја? Ако е така, може ли да понудите некои детали? (Под DarkWeb мислиме на интернет страници кои се достапни само преку анонимизирани прелистувачи, како што е Tor).

5. Дали во вашата земја се користат ИКТ за олеснување на финансиските текови во контекст на ТЛ? Ако е така, на кои начини? До кој степен се користат криптовалутите или криптопаричниците?

6. Генерално, на скала од 1 до 5, како би го оцениле влијанието на ИКТ врз ТЛ во вашата земја?

1	**2**	**3**	**4**	**5**
Многу ограничено				Многу важно

Дел 2. Клучни предизвици со кои се соочуваат земјите-членки во откривањето, истрагата и гонењето на ТЛ преку користење на ИКТ

Откривање

7. Кои се стратегиите усвоени од вашата земја за откривање на онлајн случаи на ТЛ?

8. Поопшто, кои се предизвиците во откривањето на ТЛ преку користење на ИКТ?

9. Дали имате примери за најдобри практики за откривање случаи на ТЛ преку користење на ИКТ?

10. Каков вид на обука обезбедувате на истражителите и другите актери во кривичната правда за идентификување на случаи на ТЛ овозможена од ИКТ? Која дополнителна

обука би можела да се понуди за да се зголеми ефективноста на стратегиите за откривање? Како може да се зајакне онлајн идентификацијата на жртвите?

Истраги

11. Размислувајќи за **истрагите на ТЛ преку користење на ИКТ**, колкав проблем сметате дека би било следново:

	Обично не е проблем	Помал проблем	Голем проблем
Шифрирање на податоци			
Недостаток на техничко знаење кај органите на прогонот			
Голем обем на податоци што резултира со истраги кои одземаат многу време			
Брзина на технолошки промени (брзо појавување на нова технологија итн.)			
Недостаток на техничка опрема			
Недостаток на помош од приватниот сектор			
Несоодветни законодавни алатки, вклучително и алатки за меѓусебна правна помош			

12. За секој проблем што го сметате за „голем", наведете неколку примери и опишете ги чекорите, доколку ги има, кои се веќе преземени за негово надминување/ублажување. За секој „голем" проблем, какви решенија би можеле да се предвидат за негово надминување?

13. Дали има дополнителни проблеми кои не се наведени во табелата? (За секој дополнителен проблем, наведете детали за проблемот и решенијата што би можеле да се предвидат за негово надминување).

14. Според вас кои се најдобрите стратегии за спроведување ефективни истраги за ТЛ преку користење на ИКТ?

15. Каква обука моментално им се обезбедува на органите на прогонот во врска со истрагите за ТЛ преку користење на ИКТ? Кои дополнителни потреби за обука на органите на прогонот ги идентификувавте во врска со ТЛ преку користење на ИКТ? Дали има примери на практики за обука кои ги сметате за особено успешни?

Обвинителство

16. Размислувајќи за **кривичното гонење за трговија со луѓе преку користење на ИКТ**, колкав проблем сметате дека би било следново:

	Обично не е проблем	Помал проблем	Голем проблем
Припишување на јурисдикција			
Екстрадиција на осомничени			
Добивање докази од други земји			
Помош од приватниот сектор			
Несоодветни законодавни алатки, вклучително и меѓусебни алатки за правна помош			
Непостоење на обука кај обвинителите			

17. За секој проблем што го сметате за „голем", наведете неколку примери и опишете ги чекорите, доколку ги има, кои се веќе преземени за негово надминување/ублажување. За секој „голем" проблем, какви решенија би можеле да се предвидат за негово надминување?

18. Дали има дополнителни проблеми кои не се наведени во табелата? (За секој дополнителен проблем, наведете детали за проблемот и решенијата што би можеле да се предвидат за негово надминување).

19. Какви обуки во моментов се обезбедуваат на обвинителите и судиите во врска со ТЛ преку користење на ИКТ? Кои потреби за дополнителна обука на обвинителите и судиите ги идентификувавте во врска со ТЛ преку користење на ИКТ? Дали има примери на практики за обука кои ги сметате за особено успешни?

20. Дали вашата земја има специјализирани единици во рамките на органите на прогонот и судството задолжени да постапуваат со случаи на ТЛ со голема технолошка компонента (на пример, електронски и онлајн докази)? Ако одговорот е да, опишете ги нивните практики.

Меѓународна соработка

21. Кои се предизвиците на транснационалните истраги и судската соработка во контекст на ТЛ преку користење на ИКТ? Кои се главните пречки за ефективноста, доколку ги има, и како тие би можеле да се надминат?

22. Дали има примери на добри практики за унапредување на меѓународната соработка?

Дел 3. Постојни алатки за спречување и борба против ТЛ преку користење на ИКТ

23. Можете ли да ги опишете најрелевантните домашни правни инструменти што се користат во борбата против ТЛ преку користење на ИКТ? Дали вашето законодавство може да биде во чекор со технолошките промени? Ако да, како се прилагодувате на тие промени? Ако не, како може да се подобри?

24. Можете ли да ги опишете најрелевантните меѓународни правни инструменти кои се користат во борбата против ТЛ преку користење на ИКТ? Дали сметате дека постоечките инструменти се соодветни? На кои начини тие можат да се подобрат?

25. Дали има некои специфични недостатоци во сегашното домашно или меѓународно законодавство кои ја попречуваат борбата против ТЛ преку користење на ИКТ?

26. Дали имате некакви механизми насочени кон спречување на употребата на ИКТ за цели на ТЛ, вклучително и на социјалните медиуми и во врска со огласите за работа преку Интернет? Ако одговорот е да, ве молиме опишете ги постоечките практики и наведете го државниот орган одговорен за нивното спроведување.

Дел 4. Искористување на технологијата

27. Кои технолошки алатки, доколку ги има, се моментално достапни во вашата земја за идентификување на жртвите на ТЛ? Дали се користи вештачка интелигенција, препознавање лица и/или аналитика на големи податоци за да се идентификуваат жртвите? Дали имате збир на индикатори („црвени знаменца") за идентификување на жртвите?

28. Кои иницијативи кои се потпираат на технологијата постојат во вашата земја за да им се помогне на жртвите и да се дисеминираат информациите до ризичните заедници?

29. Кои иницијативи кои се потпираат на технологијата постојат во вашата земја за поддршка на истрагите и зајакнување на гонењето?

Дел 5. Соработка со приватни компании

30. На кои начини ИКТ компаниите, вклучително и давателите на услуги за поставување на содржини (хостирање) на интернет, социјалните медиуми и другите онлајн платформи, помагаат во идентификацијата и отстранувањето на содржините на Интернет поврзани со трговија со луѓе? Како се врши филтрирањето? Дали сегашниот механизам за филтрирање и отстранување е ефикасен? Ако не, како може да се зајакне? Можете ли да дадете неколку примери на добри практики?

31. Дали има барања во вашата законска рамка за филтрирање и отстранување на интернет содржини поврзани со трговија со луѓе и кои се санкциите за неусогласеност? Дали има кодекс на однесување за давателите на услуги/провајдерите? Дали правната рамка е ефикасна? Ако не, како може да се зајакне?

32. Кои се пречките со кои се соочува вашата земја во работата со ИКТ компаниите и давателите на услуги на интернет, вклучително и прикачувачите/хостирачите на содржини и социјалните медиуми, во справувањето со ТЛ? Како може да се изгради ефективно партнерство со ИКТ компаниите? Кои алатки – правни и оперативни – би можеле да помогнат во зајакнувањето на соработката со ИКТ компаниите?

33. На кои начини ИКТ компаниите се борат против финансиските трансакции поврзани со ТЛ? Како може да се зајакне соработката во овој домен?

34. Дали вашата земја има независно тело/регулатор задолжен за следење на интернет содржините? Ако одговорот е да, врз основа на што се врши таквата активност? Ако не, на кои начини се врши мониторингот?

Дел 6. Конвенција за компјутерски криминал (Конвенцијата од Будимпешта)

35. На кој начин, доколку постои, вашата земја ги користи одредбите од Конвенцијата за компјутерски криминал на СЕ (Конвенција од Будимпешта) за борба против ТЛ? Ако не, зошто е тоа така?

36. Дали постојат начини на кои Конвенцијата за компјутерски криминал (Конвенцијата од Будимпешта) и нејзините дополнителни протоколи би можеле дополнително да се користат за борба против ТЛ?

Дел 7. Заштита на човековите права

37. Кои мерки се во сила за да се заштитат човековите и граѓанските права на поединците, вклучувајќи ги податоците и правата на приватност, кога се борат против ТЛ преку користење на ИКТ? Ако се користат технолошки алатки, на пример за чешлање на Интернетот, кои протоколи се поставени за да се гарантира дека таквите алатки ги штитат сензитивните податоци, вклучително и за сексуалната ориентација, религијата и политичките ставови?

38. Дали имате родово-сензитивни протоколи поврзани со употребата на технологија за борба против ТЛ? Дали имате возрасно-сензитивни протоколи? Ако е така, може ли да ги опишете овие протоколи?

39. Како е заштитена доверливоста на податоците кога се споделуваат информации меѓу органите на прогонот и трети страни, вклучително и приватни компании и добротворни организации? Како е избалансирана потребата на жртвите за доверливост при пристапот до услугите наспроти потребата од собирање докази и информации за помош во борбата против ТЛ?

На крај, дали има нешто друго што не е опфатено во овој прашалник што го сметате за релевантно во контекст на борбата против трговијата со луѓе, преку користење на ИКТ?

Дополнителни материјали

Можете ли да споделите со нас какви било релевантни недоверливи материјали, вклучително и статистички податоци, соопштенија за медиумите, кратки извештаи на полициските операции, кои се однесуваат на ТЛ преку користење на ИКТ, вклучувајќи:

- Употреба на ИКТ во ТЛ;
- Предизвици во откривањето на ТЛ преку користење на ИКТ, вклучително и идентификација на жртвите;
- Предизвици во истрагата и гонењето на ТЛ преку користење на ИКТ;
- Соработка меѓу земјите во контекст на ТЛ преку користење на ИКТ;
- Соработка со ИКТ компании;
- Алатки за борба против ТЛ преку користење на ИКТ (правни и/или оперативни алатки);
- Иницијативи за борба против ТЛ кои се потпираат на технологија;
- Примери на добри практики.

Доколку вашиот национален известувач го истражувал прашањето за ТЛ преку користење на ИКТ, ве молиме споделете ги со нас релевантните извештаи/материјали.

Анекс 3 | Прашалник за НВО

Овој прашалник се обидува да го разбере влијанието на технологијата врз трговијата со луѓе (ТЛ) врз основа на докази од вашата работа на терен. Под технологија, подразбираме широк збир на информатички и комуникациски технологии (ИКТ) кои им овозможуваат на корисниците да разменуваат дигитални информации. Примери за тоа се Интернет, онлајн социјални медиуми и апликации за мобилни телефони.

Дел 1. Влијанието на технологијата врз ТЛ

1. Врз основа на доказите од вашата работа, би можеле ли да дадете примери за начините на кои технологијата (ИКТ) се користи од престапниците во контекст на ТЛ за сексуална, трудова или други видови експлоатација? (За секој пример, наведете детали за видот на експлоатација и користената технологија, на пр. Интернет, одредени веб-страници, социјални медиуми, апликации).

2. Дали идентификувавте нови онлајн практики кои може да го зголемат ризикот од станување на жртва на ТЛ?

3. Кои се предизвиците во откривањето на трговијата со луѓе преку користење на технологија? Како може да се зајакне идентификацијата на жртвите?

4. Дали имате примери на добри практики што сте ги развиле во откривањето на случаите на трговија со луѓе преку користење на технологијата и идентификувањето на жртвите?

5. Дали соработувате со органите на прогонот во справувањето со трговијата со луѓе преку користење на технологија? Кои се пречките за ваквата соработка и како тие би можеле да се надминат?

6. Каков вид на обука, доколку постои, обезбедувате на персоналот и волонтерите во врска со влијанието на технологијата врз ТЛ? Која дополнителна обука би можела да биде корисна за да се зголеми ефективноста на стратегиите за откривање? Дали имате тим во вашата организација специјализиран за ТЛ преку користење на технологија?

7. Дали има некои специфични недостатоци во сегашното домашно или меѓународно законодавство што ја попречува борбата против ТЛ преку користење на технологијата?

Дел 2. Користење на технологија за борба против ТЛ

8. Кои технолошки алатки, доколку ги има, се моментално достапни за да ви помогнат во идентификувањето на жртвите на ТЛ (на пр. специфични апликации, аналитика на големи податоци, индексирање на веб)? Дали имате збир на индикатори („црвени знаменца“) за да ги идентификувате потенцијалните жртви? Каков тип на технолошки алатки би било корисно да поседувате?

9. Кои иницијативи кои се потпираат на технологија, доколку ги има, ви се достапни за да им помогнете на жртвите и да дистрибуирате информации до ризичните заедници? Кои иницијативи кои се потпираат на технологија би било корисно да се развијат?

10. Дали сте воделе кампања за подигање на свеста фокусирана на употребата на технологијата за трговија со луѓе? Доколку сте воделе, може ли да наведете некои детали за таквите кампањи?

11. Дали имате родово-чувствителни протоколи поврзани со употребата на технологија за борба против ТЛ? Дали имате возрасно-чувствителни протоколи? Доколку имате, може ли да ги опишете овие протоколи?

12. Како е заштитена доверливоста на податоците при споделување на информациите со органите на прогонот? Како е избалансирана потребата на жртвите за доверливост при пристапот до услугите наспроти потребата од собирање докази за помош во борбата против ТЛ?

13. Врз основа на доказите од вашата работа, како би го оцениле влијанието на технологијата врз ТЛ на скала од 1 до 5?

1	**2**	**3**	**4**	**5**
Многу ограничено				Многу важно

На крај, дали има нешто друго што не е опфатено во овој прашалник што го сметате за релевантно во контекст на борбата против трговијата со луѓе, преку користење на ИКТ?

Дополнителни материјали

Ако е можно, може ли да споделите со нас какви било релевантни материјали што сте ги изработиле, вклучително и статистички податоци, соопштенија за медиуми и извештаи, кои се однесуваат на ТЛ преку користење на ИКТ.

Анекс 4 | Прашалник за технолошките компании

Овој прашалник се обидува да го разбере влијанието на технологијата врз трговијата со луѓе (ТЛ) врз основа на докази од вашата работа на терен. Под технологија, подразбираме широк збир на информатички и комуникациски технологии (ИКТ) кои им овозможуваат на корисниците да разменуваат дигитални информации. Примери за тоа се Интернет, онлајн социјални медиуми и апликации за мобилни телефони.

Дел 1. Влијанието на ИКТ врз ТЛ

1. Врз основа на доказите од вашата компанија/сектор, може ли да ги опишете начините на кои ИКТ се злоупотребуваат од страна на престапниците во контекст на ТЛ (за сексуална, трудова или други видови на експлоатација)?

2. Дали идентификувавте нови онлајн практики кои може да го зголемат ризикот од станување на жртва на ТЛ?

3. Кои механизми се развиени од вашата компанија или вашиот сектор поопшто, за спречување на злоупотребата на ИКТ за цели на ТЛ?

Дел 2. Соработка со органите на прогонот и граѓанското општество

4. На кој начин, доколку ги има, вашата компанија соработува со органите на прогонот за да ја олесни идентификацијата на жртвите и истрагите за ТЛ преку користење на ИКТ?

5. Кои се главните пречки за соработка со органите на прогонот во контекст на ТЛ преку користење на ИКТ?

6. Дали има примери на добри практики за унапредување на соработката со органите на прогонот?

7. Кои се законските барања на кои подлежи вашата компанија во контекст на борбата против ТЛ?

8. Кои алатки – правни и оперативни – би можеле да помогнат во зајакнувањето на соработката со органите на прогонот?

9. На кои начини, доколку постојат, вашата компанија соработува со граѓанското општество за да ја олесни идентификацијата и помошта на жртвите на трговија со луѓе?

Дел 3. Искористување на технологијата

10. Кои технолошки алатки, доколку ги има, моментално и се достапни на вашата компанија за идентификување на жртвите на ТЛ? Дали се користат вештачка интелигенција, препознавање лица и/или аналитика на големи податоци за да се идентификуваат жртвите? Дали имате збир на индикатори („црвени знаменца“)?

11. Кои иницијативи кои се потпираат на технологија постојат во вашиот сектор за поддршка на истрагите и зајакнување на прогонот?

12. Кои мерки се во сила за заштита на човековите и граѓанските права на поединците, вклучувајќи ги податоците и правата на приватност, кога се борат против ТЛ преку користење на ИКТ? Ако се користат технолошки алатки, на пример за чешлање на Интернет, кои протоколи се поставени за да се гарантира дека таквите алатки ги штитат чувствителните податоци, вклучително и за сексуалната ориентација, религијата и политичките ставови? Дали имате воспоставено возрасно-сензитивни протоколи?

13. Каков вид на обука, доколку има, му обезбедувате на персоналот во врска со влијанието на технологијата врз ТЛ? Која дополнителна обука може да помогне да се зголеми ефикасноста на стратегиите за борба против трговијата со луѓе?

На крај, дали има нешто друго што не е опфатено во овој прашалник што го сметате за релевантно во контекст на борбата против трговијата со луѓе, преку користење на ИКТ?

Дополнителни материјали

Доколку е можно, ве молиме споделете ги со нас сите релевантни недоверливи материјали, вклучително и статистички податоци, соопштенија за медиуми и извештаи, кои се однесуваат на ТЛ преку користење на ИКТ.

Овој превод е направен со финансиска поддршка на Европската Унија и на Советот на Европа. Наведената содржина е единствена одговорност на Советот на Европа и не значи дека секогаш ги одразува ставовите на Европската унија

МКД

Земјите членки на Европската Унија одлучија да ги поврзат своите знаења, ресурси и судбини. Заедно тие изградија зона на стабилност, демократија и одржлив развој, истовремено одржувајќи ја културната разновидност, толеранцијата и индивидуалните слободи. Европската Унија се залага за споделување на своите постигнувања и вредности со држави и народи и надвор од нејзините граници.

www.europa.eu

Советот на Европа е водечка организација за човековите права на континентот. Таа се состои од 46 држави членки, вклучувајќи ги сите држави членки на Европската унија. Сите држави членки на Советот на Европа ја потпишаа Европската конвенција за човекови права, која претставува меѓународен договор за заштита на човековите права, демократијата и владеењето на правото. Европскиот суд за човекови права ја следи примената на оваа конвенцијата од страна на државите членки.

www.coe.int

Превод кофинансиран од Европската Унија

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE